COMMISSION
EUROPÉENNE

Bruxelles, le 24.7.2019
COM(2019) 353 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL EUROPÉEN ET AU CONSEIL

Dix-neuvième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective

I. INTRODUCTION

Le présent document constitue le dix-neuvième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective; il rend compte de l'évolution de la situation en ce qui concerne deux piliers principaux: d'une part, la lutte contre le terrorisme et la criminalité organisée et contre les moyens sur lesquels ils s'appuient, et, d'autre part, le renforcement de nos défenses et de notre résilience face à ces menaces.

Les citoyens européens s'attendent à juste titre à ce que l'Union assure leur sécurité. Dès le début de son mandat, la Commission Juncker a fait de la sécurité une priorité absolue. Dans le cadre du «nouveau programme stratégique 2019-2024» du Conseil européen, l'objectif consistant à «protéger les citoyens et les libertés» constitue la première des quatre grandes priorités fixées pour l'Union[1]. Le Conseil européen a également annoncé qu'il poursuivrait et intensifierait les efforts déployés par l'Union en matière de lutte contre le terrorisme et la criminalité transfrontière, notamment en améliorant la coopération et l'échange d'informations et en continuant à développer des instruments communs.

Grâce à une coopération étroite entre le Parlement européen, le Conseil et la Commission, l'UE a accompli des progrès importants dans les travaux conjoints visant à établir une union de la sécurité réelle et effective, en mettant en place plusieurs initiatives législatives prioritaires et en appliquant un large éventail de mesures non législatives destinées à soutenir les États membres et à renforcer la sécurité de tous les citoyens[2]. L'Union a pris des mesures décisives pour restreindre le périmètre d'action des terroristes et des criminels, en privant les terroristes des moyens de commettre des attentats par l'interdiction d'acquérir et d'utiliser certains explosifs et armes à feu et en limitant l'accès au financement. L'UE a également renforcé l'échange d'informations entre les États membres et comblé les lacunes et les angles morts en matière d'information, tout en luttant contre la radicalisation, en protégeant les Européens en ligne, en s'attaquant aux cybermenaces et aux menaces liées au cyberespace, en renforçant la gestion des frontières extérieures de l'Union et en consolidant la coopération internationale dans le domaine de la sécurité.

Parallèlement, plusieurs initiatives prioritaires dans le cadre de l'union de la sécurité doivent encore être adoptées par les colégislateurs. À la suite de la constitution de la 9e législature du Parlement européen le 2 juillet 2019, le présent rapport:

- définit les cas dans lesquels une action des colégislateurs est nécessaire pour faire face à des menaces immédiates. Il est particulièrement urgent d'agir pour **lutter contre la propagande terroriste et la radicalisation en ligne**;
- expose les initiatives prioritaires pendantes dans l'union de la sécurité qui nécessitent une nouvelle action des colégislateurs pour renforcer la **cybersécurité**, faciliter l'accès aux **preuves électroniques** et achever les travaux sur des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires;
- informe des derniers développements concernant les travaux conjoints et urgents lancés en mars 2019 afin d'évaluer et de renforcer **la sécurité des réseaux 5G**, en s'appuyant sur les évaluations nationales des risques que les États membres ont présentées avant le 15 juillet 2019;
- examine un ensemble de quatre rapports relatifs à la **lutte contre le blanchiment de capitaux**, adoptés par la Commission le 24 juillet 2019, qui analysent les risques et les vulnérabilités actuels en matière de blanchiment de capitaux et évaluent la manière dont le

[1] https://www.consilium.europa.eu/media/39916/a-new-strategic-agenda-2019-2024-fr.pdf.

[2] Pour une vue d'ensemble, voir la fiche d'information intitulée «Union de la sécurité: une Europe qui protège» (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) et le dix-huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2019) 145 final du 20 mars 2019].

cadre réglementaire pertinent de l'UE est appliqué dans les secteurs privé et public;

- fournit des informations actualisées sur les progrès accomplis depuis mars 2019[3] en ce qui concerne l'application des mesures législatives dans l'union de la sécurité, la mise en œuvre rapide et complète de l'interopérabilité des systèmes d'information par les États membres constituant l'une des principales priorités;
- fait le point sur les travaux en cours visant à lutter contre la désinformation et à protéger les élections contre les menaces liées au cyberespace, sur les efforts déployés en vue d'améliorer la préparation et la protection contre les menaces pesant sur la sécurité, et sur la coopération avec des partenaires internationaux en matière de sécurité.

II. PROGRÈS RÉALISÉS DANS LA CONCRÉTISATION DES PRIORITÉS LÉGISLATIVES

1. Prévenir la radicalisation en ligne et dans les communautés

La prévention de la radicalisation est au cœur de la réponse de l'UE au terrorisme, tant en ligne qu'au sein de nos communautés.

L'effroyable attentat perpétré à Christchurch (Nouvelle-Zélande) le 15 mars 2019 a constitué un terrible rappel de l'usage qui peut être fait de l'internet à des fins terroristes, que celles-ci soient motivées par le djihadisme, l'extrême droite ou toute autre idéologie extrémiste. La rapidité et l'ampleur de la diffusion en direct de la vidéo de l'attentat de Christchurch sur l'ensemble des plateformes internet ont mis en évidence l'importance vitale pour ces plateformes de pouvoir utiliser des mesures adéquates pour endiguer la propagation rapide de tels contenus.

Les chefs d'État ou de gouvernement de certains États membres et de pays tiers, le président Juncker et les plateformes en ligne ont réagi en soutenant, le 15 mai 2019, l'«**appel à l'action de Christchurch**»[4], qui définit des actions collectives visant à éliminer les contenus à caractère terroriste ou extrémiste violent en ligne. D'autres engagements ont été pris à cet égard par le G7[5] et par le G20[6].

La Commission s'est déjà penchée sur le danger manifeste et actuel que représentent les contenus à caractère terroriste en ligne avec la **proposition législative** que le président Juncker a annoncée dans son discours sur l'état de l'Union de 2018, qui offre un cadre juridique clair et harmonisé afin d'empêcher l'utilisation abusive des services d'hébergement pour la diffusion en ligne de contenus à caractère terroriste[7]. Les mesures proposées obligent les plateformes internet à retirer les contenus à caractère terroriste dans un délai d'une heure après la réception d'une injonction de suppression émise par les autorités compétentes de tout État membre. En outre, si une plateforme fait l'objet d'une utilisation abusive aux fins de la diffusion de contenus à caractère terroriste, elle aura l'obligation de prendre des mesures proactives pour détecter ces contenus et les empêcher de réapparaître, des règles et des garanties précises étant prévues à cet égard. Les autorités des États membres devraient disposer d'un service répressif spécialisé doté des moyens nécessaires pour détecter efficacement les contenus à caractère terroriste et émettre des injonctions de suppression.

---

3 Voir le dix-huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2019) 145 final du 20 mars 2019].

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/appel-de-christchurch-pour-agir-contre-le-terrorisme-et-lextremisme-violent-en-ligne. Le président français, Emmanuel Macron, et la Première ministre néo-zélandaise, Jacinda Ardern, ont invité les dirigeants et les plateformes en ligne à Paris le 15 mai 2019 pour lancer cette initiative.

5 https://www.elysee.fr/en/g7/2019/04/06/quel-bilan-pour-la-reunion-des-ministres-de-linterieur-du-g7.fr

6 Lors de la réunion du G20 qui s'est tenue les 28 et 29 juin 2019 à Osaka, les dirigeants ont réaffirmé leur détermination à agir pour protéger les citoyens contre l'exploitation de l'internet par le terrorisme et l'extrémisme violent propice au terrorisme (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final du 12 septembre 2018.

Cela permettra de disposer, à l'échelle de l'Union, d'un système rapide et efficace, doté de solides garanties, y compris des dispositifs de réclamation effectifs et des voies de recours juridictionnel. Les mesures proposées contribueront à garantir le bon fonctionnement du marché unique numérique, tout en améliorant la sécurité, en renforçant la confiance dans l'environnement en ligne et en consolidant les garanties en matière de liberté d'expression et d'information.

Au sein du Conseil, les ministres de la justice et des affaires intérieures ont approuvé une orientation générale sur cette proposition en décembre 2018. Le Parlement européen a arrêté sa position en première lecture en avril 2019. **La Commission invite les deux colégislateurs à engager le plus rapidement possible des négociations interinstitutionnelles sur cette initiative prioritaire visant à supprimer les contenus à caractère terroriste en ligne**, en vue de parvenir rapidement à un accord sur un cadre réglementaire de l'UE comportant des règles et des garanties claires.

Parallèlement, la Commission poursuit la coopération avec les plateformes en ligne dans le cadre du **forum de l'UE sur l'internet**[8]. Ainsi que le président Juncker l'a annoncé lors de la réunion tenue à Paris le 15 mai 2019 sur l'«appel à l'action de Christchurch», la Commission, en collaboration avec Europol, a commencé à élaborer un **protocole européen de crise** afin de permettre aux gouvernements et aux plateformes internet de réagir rapidement et de manière coordonnée à la diffusion de contenus à caractère terroriste en ligne, par exemple au lendemain d'une attaque terroriste. Ces travaux s'inscrivent dans le cadre des efforts déployés au niveau international pour mettre en œuvre l'«appel à l'action de Christchurch». En plus des nouvelles discussions avec les États membres et les entreprises et d'un exercice de simulation d'une situation d'urgence prévu pour septembre 2019, la Commission organisera une réunion ministérielle du forum de l'UE sur l'internet le 7 octobre 2019 en vue d'approuver le protocole européen de crise.

En outre, la Commission poursuit ses efforts pour **aider les États membres et les acteurs locaux à prévenir et à combattre la radicalisation** sur le terrain dans les communautés locales de toute l'Europe. Cela nécessite des efforts durables et à long terme de la part de tous les acteurs concernés aux niveaux local, national et de l'UE. Le **comité directeur pour les actions de l'Union en matière de prévention de la radicalisation et de lutte contre celle-ci**, créé en août 2018 pour conseiller la Commission sur la manière de renforcer la stratégie adoptée par l'UE dans ce domaine, a tenu sa deuxième réunion le 17 juin 2019 afin d'examiner de nouvelles mesures dans des domaines prioritaires tels que la radicalisation dans les prisons et la lutte contre les idéologies extrémistes. Les professionnels de première ligne et de terrain étant souvent les mieux placés pour détecter les signes avant-coureurs de la radicalisation et déterminer les moyens d'y remédier, le **réseau de sensibilisation à la radicalisation**[9], financé par l'UE, continue de les soutenir en reliant quelque 5 000 professionnels de la société civile, des écoles et de la police, ainsi que des coordinateurs nationaux et des responsables politiques.

La collaboration récente des professionnels de première ligne au sein du réseau a permis de mieux comprendre les défis de l'extrémisme de droite. Cette année, le réseau de sensibilisation à la radicalisation publiera des fiches d'information destinées à aider les responsables politiques et les professionnels à identifier les principales formes et manifestations de l'extrémisme de droite et de

---

[8] Lancé en 2015, le **forum de l'UE sur l'internet** réunit les ministres de l'intérieur de l'UE, des représentants du secteur de l'internet et d'autres parties prenantes souhaitant collaborer dans le cadre d'un partenariat volontaire pour lutter contre l'utilisation abusive de l'internet par des groupes terroristes et pour protéger les citoyens.

[9] En 2011, la Commission a mis en place le **réseau de sensibilisation à la radicalisation** pour réunir des professionnels de première ligne et de terrain. En 2015, la Commission a renforcé ce réseau en créant le centre d'excellence du réseau de sensibilisation à la radicalisation afin de concevoir des services d'orientation, de soutien et de conseil mieux ciblés à l'intention des parties prenantes dans les États membres et de renforcer l'expertise et les compétences des différents acteurs. Pour de plus amples informations sur les activités du réseau de sensibilisation à la radicalisation, voir: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

l'extrémisme islamiste, notamment les principaux discours, éléments de langage, formes, symboles, typologies et stratégies. Enfin, étant donné que les acteurs locaux et les **villes** sont en première ligne pour prévenir et combattre la radicalisation, la Commission soutient les initiatives lancées par des villes dans le domaine de la lutte contre la radicalisation. Dans le prolongement d'une conférence qui a eu lieu le 26 février 2019 sur «Les villes de l'UE contre la radicalisation», la première réunion d'un groupe pilote d'environ 20 villes, organisée par le maire de Strasbourg, s'est tenue le 8 juillet 2019 afin de renforcer l'échange de bonnes pratiques et de consolider les efforts des villes dans ce domaine.

Parallèlement, des travaux sont en cours pour aider les pays partenaires à lutter contre la radicalisation qui peut mener au terrorisme, y compris dans les prisons.

Afin de combattre la menace que représentent les contenus à caractère terroriste en ligne, la Commission invite le Parlement européen et le Conseil:

- à engager des négociations sur la proposition législative visant à prévenir la diffusion de **contenus à caractère terroriste en ligne**, en vue de parvenir rapidement à un accord sur un cadre réglementaire de l'UE comportant des règles et des garanties claires.

2. Renforcer la cybersécurité

La cybersécurité reste un défi majeur en matière de sécurité. L'UE a réalisé des progrès importants[10] en ce qui concerne la lutte contre les cybermenaces «classiques» ciblant les systèmes et les données, en mettant en œuvre les mesures définies dans la communication conjointe de septembre 2017[11] intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide». Il s'agit notamment du règlement de l'UE sur la cybersécurité[12], qui confère un mandat permanent à l'Agence de l'Union européenne pour la cybersécurité, en renforçant le rôle de celle-ci, et établit un cadre de l'UE pour la certification de cybersécurité. La Commission a également tenu compte des exigences sectorielles, par exemple dans sa recommandation relative à la cybersécurité dans le secteur de l'énergie, adoptée le 3 avril 2019[13]. Toutefois, du fait de la progression constante des agissements d'acteurs malveillants à l'encontre de toute une série d'objectifs et de victimes, les efforts visant à lutter contre la cybercriminalité et à renforcer la cybersécurité demeurent un domaine d'action prioritaire de l'UE.

Le Parlement européen et le Conseil doivent encore parvenir à un accord sur l'initiative prioritaire de la Commission en vue de la création d'un **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et d'un Réseau de centres nationaux de coordination**[14]. Cette proposition vise à renforcer les capacités industrielles et technologiques en matière de cybersécurité et à accroître la compétitivité du secteur de la cybersécurité dans l'Union. Les deux colégislateurs ont adopté leurs mandats de négociation en mars 2019. Comme il n'a pas été possible de conclure les négociations interinstitutionnelles avant la fin de la précédente législature du Parlement européen, ce dernier a formellement adopté sa position en première lecture. Dans l'intervalle, les discussions entre les États membres se poursuivent au sein du Conseil, l'accent étant

[10] Pour de plus amples informations, voir la brochure intitulée «Renforcer la cybersécurité dans l'Union européenne: résilience, dissuasion et défense»: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final du 13 septembre 2017.

[12] Le règlement de l'UE sur la cybersécurité [règlement (UE) 2019/881 du 17 avril 2019] introduit, pour la première fois, des règles à l'échelle de l'UE pour la certification de cybersécurité des produits, processus et services. En outre, il confie à l'Agence de l'Union européenne pour la cybersécurité un nouveau mandat permanent et lui alloue des ressources accrues pour lui permettre d'atteindre ses objectifs. Pour de plus amples informations sur l'appel à propositions, voir: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final du 3 avril 2019 et SWD(2019) 1240 final du 3 avril 2019.

[14] COM(2018) 630 final du 12 septembre 2018.

mis en particulier sur l'interaction entre, d'une part, le règlement proposé établissant le centre de compétences en matière de sécurité et le réseau et, d'autre part, le programme «Horizon Europe» et le programme pour une Europe numérique. **La Commission invite les deux colégislateurs à reprendre et à conclure rapidement les négociations interinstitutionnelles sur cette initiative prioritaire visant à renforcer la cybersécurité.**

Parallèlement, la Commission continue de **soutenir la recherche et l'innovation** en matière de cybersécurité, en mettant à disposition 135 millions d'EUR au titre du cadre financier pluriannuel actuel pour des projets dans des domaines tels que la cybersécurité dans les infrastructures critiques, la gestion intelligente de la sécurité et de la vie privée, et des outils spécifiquement destinés aux citoyens et aux petites et moyennes entreprises[15]. En juillet 2019, la Commission a publié un nouvel appel à propositions au titre du mécanisme pour l'interconnexion en Europe, en prévoyant un financement de l'UE de 10 millions d'euros en faveur des principaux acteurs identifiés par la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI)[16], tels que les centres européens de réponse aux incidents de sécurité informatique, les opérateurs de services essentiels (par exemple, les banques, les hôpitaux, les prestataires de services essentiels, les chemins de fer, les compagnies aériennes, les fournisseurs de noms de domaine) et diverses autorités publiques. Pour la première fois, les autorités européennes de certification de cybersécurité sont également autorisées à présenter une demande au titre de ce programme afin de leur permettre de mettre en œuvre le règlement de l'UE sur la cybersécurité.

Le 17 mai 2019, le Conseil a adopté un **régime de sanctions** qui permet à l'UE d'imposer des mesures restrictives ciblées pour décourager et contrer les cyberattaques qui représentent une menace extérieure pour l'UE et ses États. Le nouveau régime de sanctions fait partie de la **boîte à outils cyberdiplomatique de l'UE**[17], un cadre pour une réponse diplomatique conjointe de l'UE aux actes de cybermalveillance[18] qui permet à l'UE de tirer pleinement parti des mesures relevant de la politique étrangère et de sécurité commune pour décourager et contrer de tels actes.

Au-delà des cybermenaces ciblant les systèmes et les données, l'UE prend également des mesures pour faire face aux défis complexes et multiformes que posent les **menaces hybrides**[19]. Dans ses conclusions du 21 juin 2019[20], le Conseil européen a souligné que «[l]*'UE doit assurer une réponse coordonnée aux menaces hybrides et cyber et renforcer sa coopération avec les acteurs internationaux concernés*». La Commission se félicite que la lutte contre les menaces hybrides soit également une priorité de la présidence finlandaise du Conseil et qu'un débat d'orientation sur les menaces hybrides, fondé sur des scénarios, ait eu lieu lors de la réunion informelle des ministres de la justice et des affaires intérieures qui s'est tenue les 18 et 19 juillet 2019 à Helsinki. Un débat sur les menaces hybrides, également fondé sur des scénarios, s'est déroulé entre les directeurs chargés de la politique de défense de l'UE les 7 et 8 juillet 2019 et entre les directeurs politiques de l'UE les 9 et 10 juillet 2019; les résultats en seront communiqués aux ministres des affaires étrangères et de la défense lors d'une session informelle commune les 29 et 30 août 2019.

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Directive (UE) 2016/1148 du 6 juillet 2016.

17 https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/fr/pdf

18 Il s'agit notamment des cyberattaques ainsi que des tentatives de cyberattaques ayant un effet potentiellement important, qui impliquent par exemple l'accès à des systèmes d'information ou l'interception de données au moyen d'infrastructures numériques telles que les réseaux 5G (voir également la section III sur le renforcement de la sécurité des infrastructures numériques).

19 Voir le rapport sur la mise en œuvre du cadre commun de 2016 en matière de lutte contre les menaces hybrides et la communication conjointe de 2018 intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides» [SWD(2019) 200 final du 28 mai 2019]. Voir aussi la proposition législative de septembre 2016 relative à un règlement instituant un régime de l'Union de contrôle des exportations, des transferts, du courtage, de l'assistance technique et du transit en ce qui concerne les biens à double usage (refonte) [COM(2016) 616 final du 28 septembre 2016].

20 https://data.consilium.europa.eu/doc/document/ST-9-2019-INIT/fr/pdf

Pour renforcer la cybersécurité, la Commission invite le Parlement européen et le Conseil:

- à parvenir rapidement à un accord sur la proposition législative relative à la création d'un **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et à un Réseau de centres nationaux de coordination**.

3. Améliorer l'accès transfrontière aux preuves électroniques

L'UE a pris des mesures supplémentaires pour restreindre les moyens d'action des terroristes et des criminels, et rendre plus difficile leur accès aux précurseurs d'explosifs[21],le financement de leurs activités[22] et leurs déplacements clandestins[23].

Les négociations sur les propositions présentées par la Commission en avril 2018 afin d'améliorer **l'accès** des services répressifs **aux preuves électroniques** devraient être menées à bien dans les meilleurs délais, plus de la moitié de l'ensemble des enquêtes pénales donnant aujourd'hui lieu à une demande transfrontière d'accès à des preuves électroniques[24]. Le Conseil a adopté sa position de négociation portant sur la proposition de règlement[25] visant à améliorer l'accès transfrontière aux preuves électroniques dans les enquêtes pénales et sur la proposition de directive[26] établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale. Eu égard à l'importance cruciale que revêt un accès efficace aux preuves électroniques pour les enquêtes et les poursuites concernant la criminalité transfrontière telle que le terrorisme ou la cybercriminalité, la Commission invite instamment le Parlement européen à faire avancer les travaux sur cette proposition, de sorte que les colégislateurs puissent procéder à son adoption rapide.

Parallèlement, la Commission s'emploie à améliorer et à assurer les garanties nécessaires en matière d'**échange international de preuves électroniques** dans le cadre des négociations en cours d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité du Conseil de l'Europe, ainsi que des négociations avec les États-Unis, conformément aux mandats de négociation adoptés par le Conseil lors de la session du Conseil «Justice et affaires intérieures» des 6 et 7 juin 2019[27]. La Commission a participé au dernier cycle des négociations portant sur un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité du Conseil de l'Europe, du 9 au 11 juillet 2019. La Commission et les autorités des États-Unis se préparent actuellement au niveau technique pour le lancement officiel des négociations en vue d'un accord entre l'UE et les États-Unis sur l'accès transfrontière aux preuves électroniques.

---

21 Règlement (UE) 2019/1148 du Parlement européen et du Conseil du 20 juin 2019 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs.

22 Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière.

23 Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.

24 Des preuves électroniques sont nécessaires dans près de 85 % des enquêtes pénales et, dans les deux tiers de celles-ci, il faut demander les preuves auprès de prestataires de services en ligne établis dans un autre pays. Voir l'analyse d'impact accompagnant la proposition législative [SWD(2018) 118 final du 17 avril 2018].

25 COM(2018) 225 final du 17 avril 2018. Le Conseil a adopté son mandat de négociation sur la proposition de règlement lors de la session du Conseil «Justice et affaires intérieures» du 7 décembre 2018.

26 COM(2018) 226 final du 17 avril 2018. Le Conseil a adopté sa position de négociation sur la proposition de directive lors de la session du Conseil «Justice et affaires intérieures» du 8 mars 2019.

27 https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

Afin d'améliorer l'accès des services répressifs aux preuves électroniques, la Commission invite le Parlement européen:

- à adopter son mandat de négociation sur les propositions législatives relatives aux **preuves électroniques** pour entamer rapidement des discussions en trilogue avec le Conseil *(priorité de la déclaration commune).*

4. Des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires

À la suite de l'adoption de règles sur l'**interopérabilité des systèmes d'information**[28], qui combleront les lacunes et les angles morts en matière d'information en contribuant à la détection des identités multiples et à la lutte contre la fraude à l'identité, la Commission a rapidement lancé une série d'initiatives visant à aider les États membres à les mettre en œuvre, notamment financièrement lorsque cela est nécessaire, ainsi qu'au moyen d'ateliers destinés à faciliter l'échange d'expertise et de bonnes pratiques. Une coopération étroite entre les agences de l'UE, l'ensemble des États membres et les pays associés à l'espace Schengen sera primordiale pour atteindre l'objectif ambitieux consistant à parvenir à la pleine interopérabilité des systèmes d'information de l'UE aux fins de la gestion de la sécurité, des frontières et des flux migratoires d'ici à 2020.

Cet objectif suppose également la mise en œuvre rapide et complète de la législation qui a été récemment adoptée en vue de mettre en place de nouveaux systèmes d'information – le système d'entrée/de sortie de l'UE[29] et le système européen d'information et d'autorisation concernant les voyages[30] – ainsi que de renforcer le système d'information Schengen[31] et d'étendre le système européen d'information sur les casiers judiciaires[32] aux ressortissants de pays tiers. La nouvelle architecture visant à mettre en place des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires n'aura des effets réels sur le terrain que si tous les éléments en sont pleinement mis en œuvre au niveau de l'Union et par chaque État membre, conformément au calendrier convenu.

Parallèlement, les colégislateurs doivent prendre de nouvelles mesures pour terminer les travaux entrepris en ce qui concerne des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires. Dans le cadre de la mise en œuvre technique du **système européen d'information et d'autorisation concernant les voyages**, la Commission a présenté, le 7 janvier 2019, deux propositions visant à apporter au règlement y afférent[33] les modifications techniques nécessaires à la mise sur pied du système dans son intégralité. La Commission invite les colégislateurs à progresser dans leurs travaux sur ces modifications techniques afin de parvenir à un accord le plus rapidement possible et de permettre ainsi la mise en œuvre rapide et en temps utile du système européen d'information et d'autorisation concernant les voyages, afin qu'il soit opérationnel au début de l'année 2021.

En mai 2018, la Commission a présenté une proposition visant à **renforcer le système d'information sur les visas existant**[34], afin de permettre une vérification plus approfondie des antécédents des demandeurs de visas et de combler les lacunes en matière d'information par un meilleur échange de données entre les États membres. Le Conseil a adopté son mandat de négociation le 19 décembre 2018 et le Parlement européen a approuvé son rapport sur la proposition lors de sa séance plénière du 13 mars 2019, concluant ainsi la première lecture de cette proposition. La Commission invite les

28 Règlements (UE) 2019/817 et (UE) 2019/818 du 20 mai 2019.
29 Règlement (UE) 2017/2226 du 30 novembre 2017.
30 Règlements (UE) 2018/1240 et (UE) 2018/1241 du 12 septembre 2018.
31 Règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862 du 28 novembre 2018.
32 Règlement (UE) 2019/816 du 17 avril 2019.
33 COM(2019) 3 final et COM(2019) 4 final du 7 janvier 2019.
34 COM(2018) 302 final du 16 mai 2018.

colégislateurs à démarrer rapidement les négociations après la récente constitution de la législature du Parlement européen.

En mai 2016, la Commission a proposé d'élargir la portée d'**Eurodac**[35] de manière à y inclure non seulement l'identification des demandeurs d'asile mais aussi celle des ressortissants de pays tiers en séjour irrégulier et des personnes entrées irrégulièrement sur le territoire de l'Union. Conformément aux conclusions du Conseil européen de décembre 2018[36] et à la communication de la Commission du 6 mars 2019 sur les progrès réalisés dans la mise en œuvre de l'agenda européen en matière de migration[37], la Commission invite les colégislateurs à procéder à l'adoption de la proposition. Il est nécessaire d'adopter cette proposition législative pour permettre d'intégrer le système Eurodac à la future architecture des systèmes d'information interopérables de l'UE, qui comprendra ainsi les données cruciales relatives aux ressortissants de pays tiers en séjour irrégulier et aux personnes entrées irrégulièrement sur le territoire de l'Union.

Afin de renforcer les systèmes d'information de l'UE aux fins de la gestion de la sécurité, des frontières et des flux migratoires, la Commission invite le Parlement européen et le Conseil:

- à adopter la proposition législative relative à **Eurodac** *(priorité de la déclaration commune)*;
- à faire avancer les travaux en vue de parvenir rapidement à un accord sur les modifications techniques proposées qui sont nécessaires à la mise en place du **système européen d'information et d'autorisation concernant les voyages**.

III. RENFORCER LA SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES

La résilience de nos infrastructures numériques est fondamentale pour la conduite des affaires publiques, l'activité des entreprises, la sécurité de nos données à caractère personnel et le fonctionnement de nos institutions démocratiques. Les **réseaux de cinquième génération (5G)** qui seront déployés dans les prochaines années constitueront l'épine dorsale numérique de nos sociétés et de nos économies, reliant des milliards de citoyens, d'objets et de systèmes, y compris dans des secteurs critiques comme l'énergie, les transports, les banques et la santé, ainsi que des systèmes de contrôle industriel qui véhiculeront des informations sensibles et étayeront des dispositifs de sécurité.

La 5G, dont les recettes mondiales devraient atteindre 225 milliards d'euros en 2025, est un atout majeur de la compétitivité de l'Europe sur le marché mondial et **la sécurité du réseau 5G est essentielle pour garantir l'autonomie stratégique de l'Union**. Garantir un niveau élevé de cybersécurité nécessite des mesures concertées aux niveaux national et européen, puisque toute vulnérabilité des réseaux 5G dans un État membre affecte l'Union dans son ensemble.

Après que les chefs d'État ou de gouvernement ont exprimé leur soutien lors du Conseil européen de mars 2019[38], la Commission a présenté, le 26 mars 2019, une **recommandation sur la cybersécurité des réseaux 5G**[39], qui expose des mesures permettant d'évaluer les risques que présentent les réseaux 5G en matière de cybersécurité et de renforcer les mesures préventives. La recommandation repose sur des mesures coordonnées d'évaluation et de gestion des risques au niveau de l'UE, sur un cadre efficace de coopération et d'échange d'informations et sur une connaissance commune de la situation des réseaux de communication critiques au niveau de l'UE.

Conformément à la **première phase** du processus lancé par la recommandation, au 15 juillet 2019, tous les États membres avaient achevé leur **évaluation nationale des risques** et présenté leurs

35 COM(2016) 272 final du 4 mai 2016.
36 https://www.consilium.europa.eu/fr/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final du 6 mars 2019.
38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/fr/pdf
39 C(2019) 2335 final du 26 mars 2019.

conclusions à la Commission et à l'Agence de l'UE pour la cybersécurité, ou avaient annoncé qu'ils le feraient sous peu. Les évaluations nationales des risques ont suivi un ensemble d'orientations et un modèle commun de rapport convenus par les États membres et la Commission, afin de favoriser la cohérence et de faciliter l'échange d'informations sur les résultats nationaux au niveau de l'UE. Les paramètres évalués dans tous les États membres comprenaient:

- les principales menaces et les principaux auteurs d'actes malveillants qui ont une incidence sur les réseaux 5G;
- le degré de sensibilité des composantes, fonctions et autres ressources des réseaux 5G; et
- différents types de vulnérabilités, techniques et autres, telles que celles qui pourraient découler de la chaîne d'approvisionnement de la 5G.

De plus, un large éventail d'acteurs responsables dans les États membres ont été associés aux travaux d'évaluation des risques au niveau national, parmi lesquels, en fonction des responsabilités nationales, les autorités chargées de la cybersécurité, des télécommunications ou des services de sûreté et de renseignement, qui ont renforcé leur coopération et leur coordination. Parallèlement et compte tenu de leurs calendriers nationaux de déploiement de la 5G, plusieurs États membres ont déjà pris des mesures pour renforcer les exigences de sécurité applicables dans ce domaine, tandis que plusieurs autres ont indiqué leur intention d'examiner de nouvelles mesures dans un avenir proche.

En fonction des résultats de l'évaluation nationale des risques, les autorités des États membres chargées de la cybersécurité procèderont avant le 1er octobre 2019, au sein du groupe de coopération pour la sécurité des réseaux et des systèmes d'information[40], à un **examen conjoint des risques au niveau de l'UE**, ce qui constituera la deuxième phase du processus amorcé en vertu de la recommandation. Sur cette base, dans le cadre de la troisième phase, le groupe de coopération élaborera, avant le 31 décembre 2019, une **boîte à outils commune de mesures d'atténuation au niveau de l'Union**, afin de faire face aux risques recensés. La Commission et l'Agence de l'UE pour la cybersécurité continueront à soutenir la mise en œuvre de la recommandation.

Les travaux au sein du groupe de coopération pour la sécurité des réseaux et de l'information sont soutenus par plusieurs autres instances. L'Organe des régulateurs européens des communications électroniques prépare actuellement une enquête sur toutes les mesures de sécurité potentiellement pertinentes pour la 5G. Un nouveau groupe d'experts spécialisé au sein de l'Agence de l'UE pour la cybersécurité a lancé des travaux pour analyser l'inventaire des menaces propres aux réseaux 5G. En outre, à la suite de l'entrée en vigueur du règlement sur la cybersécurité le 27 juin 2019, la Commission et l'Agence de l'UE pour la cybersécurité prendront toutes les mesures nécessaires pour mettre en place le cadre de certification à l'échelle de l'UE. En juin 2019, les États membres se sont également réunis au sein du comité des normes pour débattre de la cybersécurité et de la normalisation en réponse à la recommandation invitant à étudier les futurs défis pour la normalisation en matière de cybersécurité, y compris les réseaux 5G, et à envisager des initiatives politiques appropriées au niveau de l'UE.

Enfin, la sécurité des réseaux 5G revêt une importance stratégique pour l'Union. Laisser dans des mains étrangères les investissements dans des secteurs stratégiques, l'acquisition d'actifs, de technologies et d'infrastructures critiques dans l'Union et la fourniture d'équipements critiques peut également présenter des risques pour la sécurité de l'Union.

[40] Le groupe de coopération pour la sécurité des réseaux et de l'information est institué par la directive (UE) 2016/1148 du 6 juillet 2016 sur la sécurité des réseaux et des systèmes d'information. Ainsi que cela est prévu dans la recommandation, un axe de travail spécifique, dirigé par plusieurs États membres, a été créé au sein du groupe de coopération pour la sécurité des réseaux et de l'information. Le groupe s'est déjà réuni trois fois (en avril, mai et juillet 2019) afin d'échanger des informations sur les approches nationales et de discuter de la manière de faciliter la préparation de l'évaluation coordonnée des risques au niveau de l'UE.

Le nouveau **cadre de l'UE pour le filtrage des investissements directs étrangers**[41] est entré en vigueur le 10 avril 2019. Au cours des 18 prochains mois, la Commission et les États membres prendront les mesures nécessaires pour que l'UE puisse pleinement appliquer le règlement relatif au filtrage des investissements à compter du 11 octobre 2020.

IV. LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX

La possibilité de déplacer des fonds entre comptes bancaires en quelques heures permet aux criminels et aux terroristes de préparer plus facilement des actes terroristes ou de blanchir illégalement les produits du crime dans différents États membres. Afin de faire face à ce défi, l'Union a élaboré un **cadre réglementaire solide pour prévenir le blanchiment de capitaux et le financement du terrorisme**, conformément aux normes internationales adoptées par le Groupe d'action financière.

Compte tenu de la nécessité de suivre de près l'évolution des tendances et des progrès technologiques et eu égard à l'ingéniosité dont font preuve les criminels pour exploiter toutes les failles ou lacunes du système, la Commission a adopté, le 24 juillet 2019, **un ensemble de quatre rapports** qui analysent les vulnérabilités et les risques actuels liés au blanchiment de capitaux et évaluent la manière dont le cadre est appliqué par les acteurs concernés, tant dans le secteur privé que dans le secteur public[42].

Lesdits rapports sont également accompagnés d'une **évaluation de l'interconnexion potentielle des registres nationaux centralisés des comptes bancaires et des systèmes de recherche de données** dans l'UE. Ces systèmes nationaux centralisés permettent d'identifier toute personne physique ou morale titulaire ou gestionnaire de comptes de paiement, de comptes bancaires et de coffres forts, informations souvent précieuses pour aider les autorités compétentes à lutter contre le blanchiment de capitaux et le financement du terrorisme. La 5e directive anti-blanchiment[43] impose aux États membres de mettre en place de tels systèmes nationaux centralisés et de veiller à ce que leurs cellules nationales de renseignement financier disposent d'un accès direct à ceux-ci. À la suite de l'adoption récente des dispositions destinées à faciliter l'utilisation des informations financières afin de lutter contre les formes graves de criminalité[44], les services répressifs désignés et les bureaux de recouvrement des avoirs ont un accès direct aux registres centraux nationaux respectifs. Sur cette base, et conformément à la directive anti-blanchiment, le rapport évalue différentes solutions

41 Règlement (UE) 2019/452 du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union. Le nouveau cadre crée un mécanisme de coopération grâce auquel les États membres et la Commission seront en mesure d'échanger des informations et de faire état de leurs préoccupations concernant des investissements spécifiques. Il permettra également à la Commission d'émettre des avis lorsqu'un investissement constitue une menace pour la sécurité ou l'ordre public de plus d'un État membre, ou lorsqu'un investissement risque de porter atteinte à un projet ou à un programme présentant un intérêt pour l'ensemble de l'Union. L'État membre dans lequel l'investissement a lieu a le dernier mot sur la manière de traiter l'investissement.

42 Rapport sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontières [COM(2019) 370 final du 24 juillet 2019]; rapport sur l'interconnexion des mécanismes automatisés centralisés nationaux (registres centraux ou systèmes centraux électroniques d'extraction de données) des États membres concernant les comptes bancaires [COM(2019) 372 final du 24 juillet 2019]; rapport sur l'évaluation des récents cas présumés de blanchiment de capitaux impliquant des établissements de crédit de l'UE [COM(2019) 373 final du 24 juillet 2019]; rapport évaluant le cadre de coopération entre les cellules de renseignement financier [COM(2019) 371 final du 24 juillet 2019].

43 Directive (UE) 2015/849 du 20 mai 2015.

44 Directive (UE) 2019/1153 du 20 juin 2019.

informatiques à l'échelle de l'UE, déjà opérationnelles ou en cours de développement, qui peuvent servir de modèle pour une éventuelle interconnexion des systèmes nationaux centralisés. Étant donné qu'une future interconnexion, à l'échelle de l'UE, des mécanismes centralisés offrirait un accès plus rapide aux informations financières et faciliterait la coopération transfrontières entre les autorités compétentes, la Commission entend étendre sa consultation aux parties prenantes, aux gouvernements ainsi qu'aux cellules de renseignement financier, aux services répressifs et aux bureaux de recouvrement des avoirs, en tant qu'«utilisateurs finaux» potentiels d'un éventuel système d'interconnexion.

Dans le cadre de la réflexion de la Commission sur les travaux des cellules de renseignement financier, un rapport évaluant la **coopération entre les cellules de renseignement financier** examine la coopération tant au sein de l'Union qu'avec les pays tiers[45]. Il recense certaines lacunes susceptibles de perdurer jusqu'à ce que les missions et les obligations de coopération transfrontière des cellules de renseignement financier soient énoncées plus clairement dans le cadre juridique de l'UE en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. L'évaluation fait également apparaître la nécessité d'un mécanisme renforcé pour coordonner et soutenir la coopération transfrontière et l'analyse.

Outre les travaux en cours pour lutter contre le blanchiment de capitaux et le financement du terrorisme, et afin de donner suite à l'invitation du Parlement européen[46], la Commission continuera d'évaluer la nécessité, la faisabilité technique et la proportionnalité de mesures supplémentaires pour surveiller le financement du terrorisme au sein de l'UE[47].

V. MISE EN ŒUVRE DES AUTRES DOSSIERS PRIORITAIRES EN MATIÈRE DE SÉCURITÉ

1. Mise en œuvre des mesures législatives dans l'union de la sécurité

Le fait de parvenir à un accord sur des mesures dans le cadre de l'union de la sécurité ne constitue pas l'aboutissement du processus — encore est-il essentiel de veiller ensuite à ce que les États membres mettent en œuvre rapidement et intégralement ces mesures afin qu'elles puissent produire pleinement leurs effets. À cette fin, la Commission aide activement les États membres, notamment au moyen de financements et en facilitant l'échange des meilleures pratiques.
Au besoin, néanmoins, la Commission se tient prête à faire pleinement usage des pouvoirs que lui confèrent les traités pour faire respecter le droit de l'Union, dont la procédure d'infraction s'il y a lieu.

Le délai fixé pour la mise en œuvre **de la directive de l'UE relative aux données des dossiers passagers**[48] a expiré le 25 mai 2018. À ce jour, 25 États membres ont notifié une

[45] Cette évaluation est requise par l'article 65, paragraphe 2, de la 5e directive anti-blanchiment, c'est-à-dire la directive (UE) 2018/843 du 30 mai 2018.

[46] Dans son rapport final adopté en décembre 2018, la commission spéciale sur le terrorisme du Parlement européen a recommandé la mise en place d'un système européen de surveillance du financement du terrorisme à même de suivre les transactions réalisées par des personnes ayant des liens avec le terrorisme et son financement dans l'espace unique de paiement en euros.

[47] Voir le dix-huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2019) 145 final du 20 mars 2019.

[48] Directive (UE) 2016/681 du 27 avril 2016.

transposition complète à la Commission[49]. Deux États membres n'ont toujours pas procédé à sa transposition complète, malgré les procédures d'infraction lancées le 19 juillet 2018[50]. Parallèlement, la Commission continue de soutenir les efforts consentis par les États membres pour achever le développement de leurs systèmes de dossiers des données passagers, notamment en facilitant l'échange d'informations et des meilleures pratiques.

Le délai de transposition de la **directive relative à la lutte contre le terrorisme**[51] a expiré le 8 septembre 2018. À ce jour, 22 États membres ont notifié une transposition complète à la Commission. Trois États membres n'ont toujours pas communiqué l'adoption d'une législation nationale transposant intégralement la directive, malgré les procédures d'infraction lancées le 22 novembre 2018[52].

Le délai de transposition de la **directive relative au contrôle de l'acquisition et de la détention d'armes**[53] a expiré le 14 septembre 2018. À ce jour, huit États membres ont notifié une transposition complète à la Commission. 20 États membres n'ont toujours pas communiqué l'adoption de mesures nationales transposant intégralement la directive, malgré les procédures d'infraction lancées le 22 novembre 2018[54].

En ce qui concerne la transposition en droit national de la **directive relative à la protection des données dans le domaine répressif**[55], le délai de transposition a expiré le 6 mai 2018. À ce jour, 20 États membres ont notifié une transposition complète à la Commission[56]. Sept États membres n'ont toujours pas communiqué l'adoption de mesures nationales transposant pleinement la directive, malgré les procédures d'infraction lancées par la Commission le 19 juillet 2018[57].

Les États membres avaient jusqu'au 9 mai 2018 pour transposer **la directive relative à la sécurité des réseaux et des systèmes d'information**[58] dans leur droit national. À ce jour, 26 États membres ont notifié une transposition complète à la Commission et deux États membres ont partiellement transposé la directive[59]. En outre, conformément à la directive, les États membres étaient invités à identifier les opérateurs de services essentiels pour le 9 novembre 2018 au plus tard. La Commission devait présenter au Parlement européen et au Conseil, au plus tard le 9 mai 2019, un rapport évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels sur leur territoire.

---

49 Les mentions d'une notification de transposition complète tiennent compte des déclarations des États membres et sont sans préjudice du contrôle de la transposition par les services de la Commission.

50 La Slovénie a notifié une transposition partielle. L'Espagne n'a notifié aucune mesure de transposition (situation au 24 juillet 2019).

51 Directive (UE) 2017/541 du 15 mars 2017.

52 La Pologne a notifié une transposition partielle. La Grèce et le Luxembourg n'ont notifié aucune mesure de transposition (situation au 24 juillet 2019).

53 Directive (UE) 2017/853 du 17 mai 2017.

54 La Belgique, la Tchéquie, l'Estonie, la Lituanie, la Pologne, le Portugal, la Suède et le Royaume-Uni ont notifié une transposition partielle. L'Allemagne, l'Irlande, la Grèce, l'Espagne, Chypre, le Luxembourg, la Hongrie, les Pays-Bas, la Roumanie, la Slovénie, la Slovaquie et la Finlande n'ont notifié aucune mesure de transposition (situation au 24 juillet 2019).

55 Directive (UE) 2016/680 du 27 avril 2016.

56 20 États membres ont achevé la transposition de la directive (situation au 24 juillet 2019).

57 La Lettonie, le Portugal, la Slovénie et la Finlande ont notifié une transposition partielle. La Grèce et l'Espagne n'ont notifié aucune mesure de transposition. Bien que l'Allemagne ait notifié une transposition complète, la Commission considère que cette transposition n'est pas complète (situation au 24 juillet 2019).

58 Directive (UE) 2016/1148 du 27 avril 2016.

59 La Belgique et la Hongrie ont partiellement transposé la directive (situation au 24 juillet 2019).

Or, un certain nombre d'États membres n'ayant pas encore communiqué des informations complètes sur le processus d'identification, la Commission a dû différer son rapport.

La Commission évalue actuellement la transposition de la **4e directive anti-blanchiment**[60], tout en vérifiant que ses dispositions sont mises en œuvre par les États membres. La Commission a engagé des procédures d'infraction à l'encontre de 24 États membres car elle a estimé que les communications qu'ils lui avaient transmises ne constituaient pas une transposition complète de ladite directive[61].

La Commission invite les États membres à prendre d'urgence les mesures requises pour transposer intégralement dans leur droit national les directives suivantes et à les communiquer à la Commission:

- la **directive relative aux données des dossiers passagers**, dont un État membre doit encore notifier la transposition en droit national et dont un autre État membre doit compléter la notification des mesures de transposition[62];
- la **directive relative à la lutte contre le terrorisme**, dont deux États membres doivent encore notifier la transposition en droit national et dont un État membre doit compléter la notification des mesures de transposition[63];
- la **directive relative au contrôle de l'acquisition et de la détention d'armes**, dont 12 États membres doivent encore notifier la transposition en droit national et dont huit États membres doivent compléter la notification des mesures de transposition[64];
- la **directive relative à la protection des données dans le domaine répressif**, dont deux États membres doivent encore notifier la transposition en droit national et dont cinq États membres doivent compléter la notification des mesures de transposition[65];
- la **directive relative à la sécurité des réseaux et des systèmes d'information**, dont deux États membres doivent encore compléter la notification des mesures de transposition[66]; et
- la **4e directive anti-blanchiment**, dont 24 États membres doivent encore compléter la notification des mesures de transposition[67].

2. Lutte contre la désinformation et protections des élections contre les menaces liées au cyberespace

60 Directive (UE) 2015/849 du 20 mai 2015.

61 La Belgique, la Bulgarie, la Tchéquie, le Danemark, l'Allemagne, l'Estonie, l'Irlande, l'Espagne, la France, l'Italie, Chypre, la Lettonie, la Lituanie, la Hongrie, les Pays-Bas, l'Autriche, la Pologne, le Portugal, la Roumanie, la Slovénie, la Slovaquie, la Finlande, la Suède et le Royaume-Uni (situation au 24 juillet 2019).

62 La Slovénie a notifié une transposition partielle. L'Espagne n'a notifié aucune mesure de transposition (situation au 24 juillet 2019).

63 La Pologne a notifié une transposition partielle. La Grèce et le Luxembourg n'ont notifié aucune mesure de transposition (situation au 24 juillet 2019).

64 La Belgique, la Tchéquie, l'Estonie, la Lituanie, la Pologne, le Portugal, la Suède et le Royaume-Uni ont notifié une transposition partielle. L'Allemagne, l'Irlande, la Grèce, l'Espagne, Chypre, le Luxembourg, la Hongrie, les Pays-Bas, la Roumanie, la Slovénie, la Slovaquie et la Finlande n'ont notifié aucune mesure de transposition (situation au 24 juillet 2019).

65 La Lettonie, le Portugal, la Slovénie et la Finlande ont notifié une transposition partielle. La Grèce et l'Espagne n'ont notifié aucune mesure de transposition. Bien que l'Allemagne ait notifié une transposition complète, la Commission considère que cette transposition n'est pas complète (situation au 24 juillet 2019).

66 La Belgique et la Hongrie ont partiellement transposé la directive (situation au 24 juillet 2019).

67 La Belgique, la Bulgarie, la Tchéquie, le Danemark, l'Allemagne, l'Estonie, l'Irlande, l'Espagne, la France, l'Italie, Chypre, la Lettonie, la Lituanie, la Hongrie, les Pays-Bas, l'Autriche, la Pologne, le Portugal, la Roumanie, la Slovénie, la Slovaquie, la Finlande, la Suède et le Royaume-Uni (situation au 24 juillet 2019).

Protéger les processus et institutions démocratiques contre la désinformation et les ingérences qui y sont liées constitue un défi majeur pour les sociétés du monde entier. Pour le relever, l'Union a établi un **cadre solide pour une action coordonnée contre la désinformation**, qui respecte pleinement les valeurs et droits fondamentaux européens[68]. Comme indiqué dans la communication conjointe du 14 juin 2019 sur la mise en œuvre du plan d'action contre la désinformation[69], les travaux menés sur plusieurs volets complémentaires ont contribué à réduire le champ d'influence de la désinformation et à préserver l'intégrité des élections au Parlement européen.

Dans ses conclusions du 21 juin 2019[70], le Conseil européen a salué l'intention de la Commission de procéder à une évaluation approfondie de la mise en œuvre des engagements pris par les plateformes en ligne et d'autres signataires au titre du **code de bonnes pratiques contre la désinformation**[71] et a invité la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité à évaluer de manière continue «*le caractère évolutif des menaces et le risque croissant d'ingérence malveillante et de manipulation en ligne associés au développement de l'intelligence artificielle et des techniques de collecte de données*» et à y apporter une réponse appropriée.

La Commission et la haute représentante feront avancer les travaux dans ce domaine, conformément aux conclusions du Conseil européen. En mars 2019, la Commission et la haute représentante ont créé un **système d'alerte rapide** entre les institutions de l'UE et les États membres afin de faciliter le partage de données liées aux campagnes de désinformation et d'apporter des réponses coordonnées. La première réunion des points de contact des États membres à la suite des élections au Parlement européen a eu lieu à Tallinn, les 3 et 4 juin 2019. Afin de renforcer encore le système d'alerte rapide, la haute représentante et la Commission, en étroite coopération avec les États membres, en examineront le fonctionnement à l'automne 2019. Elles élaboreront également une méthodologie commune pour analyser et mettre en lumière les campagnes de désinformation ainsi que pour établir des partenariats renforcés avec des partenaires internationaux tels que le G7 et l'OTAN.

Les travaux se poursuivent également au sein du **réseau européen de coopération en matière d'élections**[72], qui a tenu une première réunion le 7 juin 2019 pour faire le point sur

---

68 Voir le plan d'action contre la désinformation [JOIN(2018) 36 final du 5 décembre 2018].

69 JOIN(2019) 12 final du 14 juin 2019.

70 https://www.consilium.europa.eu/media/39947/20-21-euco-final-conclusions-fr.pdf. L'invitation du Conseil européen fait suite aux contributions de la présidence roumaine du Conseil ainsi que de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité sur les enseignements tirés en ce qui concerne la désinformation et la garantie d'élections libres et régulières, y compris la communication conjointe sur la mise en œuvre du plan d'action contre la désinformation.

71 Le code de bonnes pratiques a été signé en octobre 2018 par les plateformes en ligne Facebook, Google et Twitter, par Mozilla ainsi que par les annonceurs et le secteur de la publicité; il fixe des normes d'autorégulation pour lutter contre la désinformation. Il vise à réaliser les objectifs fixés par la communication de la Commission d'avril 2018 sur la lutte contre la désinformation en ligne [COM(2018) 236 final du 26 avril 2018] en fixant une série d'engagements, consistant notamment à garantir la transparence de la publicité à caractère politique et la fermeture des faux comptes et à priver de leurs recettes les vecteurs de désinformation.

72 Le réseau européen de coopération en matière d'élections réunit les points de contact des réseaux nationaux de coopération en matière d'élections, composés des autorités nationales compétentes en matière électorale et des autorités chargées de contrôler et de faire appliquer les règles relatives aux activités en ligne ayant trait au contexte électoral. Le réseau européen de coopération en matière d'élections sert à prévenir de

les élections au Parlement européen. Ces réflexions et les contributions supplémentaires des autorités nationales compétentes, des partis politiques et des plateformes en ligne enrichiront le rapport global de la Commission sur les élections au Parlement européen, qui devrait être adopté en octobre 2019. Les États membres ont utilisé le réseau pour d'autres élections que celles du Parlement européen, ce qui témoigne de son utilité générale pour garantir l'intégrité de la démocratie dans l'UE.

La Commission continuera également à surveiller et à promouvoir la mise en œuvre des engagements pris par les plateformes dans le **code de bonnes pratiques contre la désinformation**. Les rapports fournis par Google, Twitter et Facebook dans le cadre du code de bonnes pratiques montrent que toutes les plateformes ont pris des mesures en amont des élections au Parlement européen en étiquetant les publicités à caractère politique et en les rendant accessibles au public au moyen de recherches dans des bibliothèques d'annonces. Parallèlement, les améliorations indiquées par le groupe des régulateurs européens pour les services de médias audiovisuels sont également possibles[73]. En particulier, l'accès aux données brutes détaillées nécessaires à une surveillance complète n'est toujours pas suffisant. Enfin, les plateformes devraient fournir à la communauté des chercheurs un véritable accès aux données, dans le respect des règles de protection des données à caractère personnel. Dans le courant de cette année, la Commission procédera à une évaluation complète de la mise en œuvre de tous les engagements pris au titre du code de bonnes pratiques pendant sa période initiale de 12 mois. Sur cette base, la Commission pourra envisager de nouvelles mesures, notamment de nature réglementaire, pour améliorer la réaction à long terme de l'UE face à la désinformation.

3. Préparation et protection

Le renforcement des moyens de se défendre et de la résilience face aux menaces pesant sur la sécurité constitue un aspect important des travaux visant à mettre en place une union de la sécurité réelle et effective. À cette fin, la Commission apporte son soutien aux États membres et à leurs collectivités locales pour renforcer la **protection des espaces publics**[74], de même qu'elle fournit une aide aux États membres pour améliorer leur niveau de préparation aux

---

menaces, à échanger des bonnes pratiques entre réseaux nationaux, à rechercher des solutions communes à des problèmes détectés et à encourager les projets et exercices communs à plusieurs réseaux nationaux.

73 Le groupe des régulateurs européens pour les services de médias audiovisuels réunit des responsables ou des représentants de haut niveau des organismes de régulation nationaux indépendants dans le domaine des services audiovisuels afin de conseiller la Commission sur la mise en œuvre de la directive de l'UE sur les services de médias audiovisuels (directive 2010/13/UE du 10 mars 2010). Lors de sa dernière réunion, qui s'est tenue les 20 et 21 juin 2019 à Bratislava, le groupe a présenté les résultats des travaux accomplis jusqu'à présent sur la désinformation, en mettant l'accent sur les élections au Parlement européen de 2019 et les domaines connexes de la publicité à caractère politique et de la publicité engagée.

74 Voir les «Meilleures pratiques à l'usage des autorités publiques et des opérateurs privés en vue de renforcer la sécurité des espaces publics», telles que décrites dans le dix-huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2019) 145 final du 20 mars 2019]. Ces mesures s'appuient sur le plan d'action visant à améliorer la protection des espaces publics, d'octobre 2017 [COM(2017) 612 final du 18 octobre 2017]. Le 5 juin 2019 s'est tenue la troisième réunion du Forum des exploitants de l'UE sur la protection des espaces publics. S'y sont rencontrés des représentants des États membres de l'UE et des exploitants privés d'espaces publics, représentés par 14 associations européennes, provenant des secteurs de l'hôtellerie, du spectacle, de la musique et du divertissement, des parcs d'attraction et de loisirs, de l'aviation, du transport ferroviaire, des centres commerciaux, des télécommunications, ainsi que des secteurs des services de sécurité privée et des fabricants d'équipements de sécurité.

risques en matière de sécurité chimique, biologique, radiologique et nucléaire[75]; elle met en œuvre les deux plans d'action dans ce domaine et analyse les besoins liés aux capacités de réaction nécessaires au titre de rescEU[76]. En ce qui concerne l'évolution des menaces chimiques[77], en coopération avec les États membres et en consultation avec les partenaires internationaux, la Commission a élaboré une liste des cas les plus préoccupants de produits chimiques détournés de leur utilisation initiale à des fins terroristes. La liste de l'UE sert de base à la poursuite des travaux visant à entraver l'accès à ces substances chimiques et à œuvrer avec les fabricants à l'amélioration des capacités de détection.

Les technologies des aéronefs sans équipage à bord rendent possible un large éventail d'exploitations. Connaissant une expansion rapide ces dernières années sur le marché des systèmes d'aéronefs sans équipage à des fins militaires, commerciales civiles et de loisirs, **les drones** ouvrent des perspectives mais représentent aussi une menace croissante pour la sécurité des infrastructures critiques (y compris l'aviation), des espaces et des événements publics, ainsi que des sites sensibles et des personnes. En Europe, les drones ont été utilisés pour perturber des opérations aériennes et répressives, pour surveiller des infrastructures critiques et pour faire de la contrebande dans les prisons et par-delà les frontières.

La Commission soutient la lutte des États membres contre la menace croissante que représentent les drones pour les citoyens et les fonctions sociétales critiques, sans exclure leur utilisation bénéfique, par exemple dans les opérations d'intervention d'urgence. La Commission a récemment adopté des **règles communes à l'échelle de l'UE concernant l'exploitation en toute sécurité des drones**[78] afin d'atténuer le risque de leur utilisation malveillante, qui prévoient notamment des dispositions exigeant l'enregistrement de l'opérateur et permettant l'identification à distance. De plus, la Commission soutient les États membres en observant les tendances de l'évolution de la menace que représentent les drones, en finançant des projets de recherche et des mesures de renforcement des capacités en la matière, et en facilitant les échanges entre les États membres et les autres parties prenantes. Soucieuse d'améliorer ce soutien, la Commission organisera, le 17 octobre 2019, une conférence internationale à haut niveau pour lutter contre les risques posés par les drones.

Eu égard à la nécessité de disposer d'une vue aussi large que possible de la politique de l'UE concernant la **protection des infrastructures critiques**[79], la Commission a présenté, le 23 juillet 2019, une évaluation de la directive relative aux infrastructures critiques européennes[80], dès lors que cette dernière constitue le cadre juridique pour le recensement et

---

75 Notamment par la mise en œuvre du plan d'action d'octobre 2017 visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire [COM(2017) 610 final du 18 octobre 2017].

76 Voir l'article 12, paragraphe 2, de la décision n° 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union, tel que modifié par la décision (UE) 2019/420 du 13 mars 2019.

77 Voir le renforcement des actions de lutte contre les menaces chimiques décrit dans le quinzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2018) 470 final du 13 juin 2018].

78 Règlement d'exécution (UE) 2019/947 de la Commission du 24 mai 2019 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord (JO L 152 du 11.6.2019, p. 45).

79 L'évaluation globale de la politique de sécurité de l'UE réalisée en 2017 [SWD(2017) 278 final du 26.7.2017] a souligné la nécessité d'adopter une position générale sur la politique de l'UE en matière de protection des infrastructures critiques.

80 La directive 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection a pour objet d'améliorer la protection des infrastructures critiques dans l'Union européenne.

la désignation des infrastructures critiques européennes ainsi que pour l'évaluation de la nécessité d'améliorer leur protection. L'évaluation a révélé que le contexte de l'exploitation des infrastructures critiques en Europe a considérablement changé depuis l'entrée en vigueur de la directive, notamment en raison de l'évolution de la législation dans certains secteurs particulièrement visés par la directive, tels que l'énergie[81]; en outre, du fait de la mutation du paysage dans ce domaine, les dispositions de la directive ne sont plus que partiellement pertinentes. Dans le même temps, les États membres continuent de soutenir, en matière de protection des infrastructures critiques, une politique de l'UE respectueuse de la subsidiarité et porteuse de valeur ajoutée.

4. Dimension extérieure

Compte tenu de la nature transfrontière et mondiale de la plupart des menaces auxquelles l'Union est confrontée en matière de sécurité, la coopération avec les organisations internationales et les pays partenaires en dehors de l'UE fait partie intégrante des travaux visant à mettre en place une union de la sécurité réelle et effective.

Tirer parti des avantages de la coopération multilatérale fait partie intégrante de cet effort et implique notamment la coopération entre l'UE et les Nations unies, récemment renforcée par la signature à New York, le 24 avril 2019, du **cadre de lutte contre le terrorisme entre l'ONU et l'UE**, à l'occasion du deuxième dialogue politique de haut niveau UE-ONU sur la lutte contre le terrorisme [82]. Ce cadre promeut la coopération en matière de renforcement des capacités pour lutter contre le terrorisme et prévenir et combattre l'extrémisme violent en Afrique, au Moyen-Orient et en Asie. Il définit des domaines de coopération entre l'ONU et l'UE et des priorités jusqu'en 2020.

La coopération en matière de **sécurité avec les Balkans occidentaux** représente une priorité régionale particulière, et se traduit par la mise en œuvre d'un certain nombre d'actions prioritaires en matière de sécurité définies dans la stratégie pour les Balkans occidentaux de 2018[83]. À cette fin, le 4 avril 2019, la Commission a organisé la première réunion de la task force interagences pour les Balkans occidentaux, lors de laquelle des représentants de sept agences de l'UE ont partagé leur expérience et renforcé leur coopération opérationnelle avec des partenaires de la région, notamment en matière de lutte contre la criminalité organisée, le terrorisme, les armes à feu, les stupéfiants, le trafic de migrants et la traite des êtres humains. Des enquêtes sur les menaces hybrides ont été lancées avec les six pays des Balkans occidentaux. Un autre exemple concret de coopération avec cette région est l'accord sur le statut du corps européen de garde-frontières et de garde-côtes entre l'UE et l'Albanie, entré en vigueur le 1 er mai 2019 et rapidement suivi du déploiement d'équipes de l'Agence européenne de garde-frontières et de garde-côtes à la frontière avec la Grèce. C'est la première fois qu'un tel accord est conclu avec un pays tiers et qu'un tel déploiement y est organisé. Des accords similaires devraient être signés prochainement avec d'autres pays de la région.

En outre, un officier de liaison Europol a été détaché en Albanie en juillet 2019 afin d'offrir une assistance supplémentaire aux autorités albanaises dans leurs efforts de prévention et de lutte contre la criminalité organisée. Afin de renforcer la lutte contre le trafic d'armes à feu, la

81 En particulier le règlement (UE) 2017/1938 du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et le règlement (UE) 2019/941 du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final du 6.2.2018.

Commission a présenté, le 27 juin 2019, une évaluation du plan d'action 2015-2019 sur le **trafic d'armes à feu** convenu entre l'UE et l'Europe du Sud-Est[84]. L'évaluation démontre la valeur ajoutée de la coopération, mais souligne la nécessité de déployer des efforts supplémentaires, par exemple en créant des centres nationaux de coordination efficaces sur les armes à feu ou en harmonisant la collecte d'informations et la communication d'informations sur les saisies d'armes à feu.

L'Union accorde la même priorité au développement de la **coopération avec les pays du Moyen-Orient et d'Afrique du Nord** dans le domaine de la sécurité. Elle a lancé un dialogue sur la sécurité avec la Tunisie et l'Algérie. Le 12 juin, à Tunis, l'Union et la Tunisie ont tenu la 3e session du dialogue en matière de sécurité et de lutte contre le terrorisme, tandis que la 2e session du dialogue entre l'Union et l'Algérie sur les questions sécuritaires et la lutte contre le terrorisme a eu lieu le 12 novembre 2018 à Alger. Des discussions sont en cours pour lancer un dialogue structuré sur la sécurité avec le Maroc, à la suite de la récente réunion du Conseil d'association du 27 juin, au cours de laquelle l'UE et le Maroc ont reconnu l'importance d'approfondir la coopération en matière de sécurité pour relever des défis communs. D'autres discussions ont lieu parallèlement afin de développer un dialogue structuré sur la sécurité avec l'Égypte, comme l'a également confirmé la dernière réunion à haut niveau entre l'UE et l'Egypte, qui s'est tenue le 10 juillet au Caire.

En vertu du mandat qui lui a été donné par le Conseil, la Commission a entamé des discussions informelles avec la plupart des **pays du Moyen-Orient et d'Afrique du Nord** pour lancer des négociations officielles en vue d'un accord international pour l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (**Europol**) et les autorités compétentes concernées des pays du **Moyen-Orient et d'Afrique du Nord** pour lutter contre les formes graves de criminalité et le terrorisme. Dans ce contexte, la Commission encourage également la conclusion directe d'arrangements de travail entre Europol et les autorités partenaires dans les pays du **Moyen-Orient et d'Afrique du Nord**, afin de fournir un cadre formel pour une coopération régulière au niveau stratégique.

L'UE et les **États-Unis** sont des partenaires stratégiques privilégiés lorsqu'il s'agit de faire face aux menaces communes et de renforcer la sécurité. Lors de la réunion des ministres de la justice et des affaires intérieures qui s'est tenue le 19 juin 2019, l'UE et les États-Unis ont confirmé que la lutte contre le terrorisme faisait partie de leurs principales priorités. En ce qui concerne l'accord entre l'UE et les États-Unis sur les données des dossiers passagers[85], les deux parties ont rappelé l'importance de l'accord et se sont engagées à entamer une évaluation conjointe en septembre 2019 afin d'apprécier sa mise en œuvre, conformément aux dispositions de l'accord. Les parties se sont également engagées à intensifier leurs efforts conjoints de lutte contre le terrorisme, notamment en développant les échanges d'informations recueillies dans des zones de combat en vue de leur utilisation dans le cadre d'enquêtes et de poursuites.

Afin de renforcer cette coopération, la Commission, conjointement avec le coordinateur de l'UE pour la lutte contre le terrorisme, a organisé, le 10 juillet 2019 à Bruxelles, un atelier de haut niveau sur les informations du champ de bataille. De hauts fonctionnaires des ministères

---

84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_fr.pdf

85 JO L 215 du 11.8.2012, p. 5.

de la défense, de l'intérieur et de la justice des États membres, des États-Unis, d'Europol et d'Eurojust et des représentants d'organisations internationales s'y sont rencontrés pour procéder à un échange de vues sur l'utilisation des informations du champ de bataille et examiner ensemble les problèmes procéduraux, juridiques et opérationnels qu'ils rencontrent lorsqu'il s'agit d'identifier les terroristes et de les traduire en justice. Les 14 et 15 mai, l'Union et les États-Unis ont également tenu à Bruxelles un dialogue sur le renforcement des capacités en matière de risques chimiques, biologiques, radiologiques et nucléaires (CBRN) afin de coordonner leurs efforts visant à réduire les menaces liées aux armes de destruction massive et à renforcer la sécurité en matière de risques CBRN à l'échelle mondiale.

L'accord sur le programme de surveillance du financement du terrorisme entre l'UE et les États-Unis[86] est en vigueur depuis 2010 et régit le transfert et le traitement de données aux fins d'identifier, de surveiller et de poursuivre les terroristes et leurs réseaux. Il prévoit des garanties qui assurent la protection des données des citoyens de l'UE ainsi qu'un réexamen régulier des «dispositions en matière de garanties, de contrôles et de réciprocité». Dans un rapport d'évaluation périodique[87] publié le 22 juillet 2019, la Commission a indiqué qu'elle était convaincue que l'accord, y compris ses garanties et contrôles essentiels, était correctement mis en œuvre. Elle se félicite de la transparence dont continuent de faire preuve les autorités américaines en matière d'échange d'informations, illustrant ainsi la valeur du programme de surveillance du financement du terrorisme dans le cadre des efforts conjoints en matière de lutte contre le terrorisme. Les informations fournies dans le cadre de l'accord ont été décisives pour l'avancement des enquêtes spécifiques concernant les attentats terroristes sur le sol européen, y compris les attentats de Stockholm, de Barcelone et de Turku en 2017. Les États membres et Europol ont recouru davantage au mécanisme et les données du programme de surveillance du financement du terrorisme ont généré sept fois plus d'enquêtes que lors de la période de référence précédente. Le prochain réexamen conjoint de l'accord est prévu pour 2021.

En ce qui concerne la coopération internationale en matière d'échange de **données des dossiers passagers aux fins de la lutte contre le terrorisme et les formes graves de criminalité**, lors du 17e sommet UE-Canada qui s'est tenu à Montréal les 17 et 18 juillet 2019, l'UE et le Canada se sont félicité de la conclusion des négociations en vue d'un nouvel accord sur les données des dossiers passagers. Tandis que le Canada a pris acte de son obligation de contrôle juridictionnel, les parties, conscientes que cet accord joue un rôle essentiel dans le renforcement de la sécurité tout en garantissant le respect de la vie privée et la protection des données à caractère personnel, s'engagent, sous réserve de la mise en œuvre dudit contrôle, à finaliser l'accord dès que possible. En ce qui concerne l'accord entre l'UE et l'Australie sur les données des dossiers passagers[88], une visite d'une équipe de l'UE à Canberra aura lieu en août 2019 dans le cadre du réexamen conjoint et de l'évaluation commune de l'accord.

La Commission travaille également avec les États membres au sein du Conseil sur une position de l'UE en vue de la 40e session de l'**assemblée de l'Organisation de l'aviation civile internationale**, qui se tiendra du 24 septembre au 4 octobre 2019. Ladite assemblée définira la direction politique et donnera des instructions au conseil de l'Organisation de l'aviation civile internationale (OACI) concernant les travaux techniques relatifs aux normes

86 JO L 195 du 27.7.2010, p. 5.
87 COM(2019) 342 final du 22 juillet 2019.
88 JO L 186 du 14.7.2012, p. 4.

de l'OACI en matière de traitement des données des dossiers passagers. Le Conseil a approuvé un document d'information élaboré par la Commission afin d'exposer le point de vue l'Union sur les principes fondamentaux qui devraient sous-tendre tout futur système mondial relatif aux données des dossiers passagers. Le document d'information sera présenté aux membres de ladite assemblée qui ne sont pas des États membres de l'UE.

VI. CONCLUSIONS

Grâce à une coopération étroite entre le Parlement européen, le Conseil, les États membres et la Commission, l'Union a accompli des progrès considérables ces dernières années dans le cadre des travaux communs en vue de mettre en place une union de la sécurité réelle et effective, en s'accordant sur un certain nombre d'initiatives législatives prioritaires. Les États membres, soutenus par la Commission, mettent également en œuvre un éventail de mesures opérationnelles non législatives visant à renforcer la sécurité de tous les citoyens. Parallèlement, il reste dans l'union de la sécurité un certain nombre d'initiatives prioritaires en suspens qui nécessitent des mesures supplémentaires de la part des colégislateurs pour faire face aux menaces immédiates. La Commission invite le Parlement européen et le Conseil à prendre les mesures nécessaires pour parvenir rapidement à un accord sur les propositions législatives visant à lutter contre la propagande terroriste et la radicalisation en ligne, à renforcer la cybersécurité, à faciliter l'accès aux preuves électroniques et à achever les travaux sur des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires.

La Commission invite les États membres à mettre en œuvre rapidement et intégralement l'ensemble de la législation adoptée dans l'union de la sécurité afin qu'elle produise pleinement ses effets. En outre, la Commission invite les États membres à poursuivre et à intensifier les travaux cruciaux menés sur des mesures concrètes visant à renforcer la sécurité des infrastructures numériques, à lutter contre la désinformation et d'autres menaces liées au cyberespace, à renforcer la préparation et la protection, et à intensifier la coopération avec des partenaires extérieurs à l'Union contre les menaces communes. Conjuguées, ces mesures renforcent collectivement la sécurité de tous les citoyens.