COMMISSION
EUROPÉENNE

Bruxelles, le 30.10.2019
COM(2019) 552 final

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

## Vingtième 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 vingtième 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 des principaux piliers de cette union: 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.

Dès le début de son mandat, la Commission Juncker a fait de la sécurité une priorité absolue. Se fondant sur le programme européen en matière de sécurité d'avril 2015[1] et sur la communication d'avril 2016 ouvrant la voie à une union de la sécurité réelle et effective[2], l'Union a adopté une approche coordonnée en réaction à une série d'attentats terroristes et d'autres défis grandissants en matière de sécurité, accomplissant d'importants progrès dans le renforcement de notre sécurité collective[3]. Il apparaît de plus en plus clairement que les défis actuels en matière de sécurité – qu'il s'agisse de terrorisme, de crime organisé, de cyberattaques, de désinformation ou d'autres menaces en constante évolution liées au cyberespace – sont des menaces communes. Ce n'est, en effet, qu'en travaillant ensemble que nous pourrons atteindre le niveau de sécurité collective que nos concitoyens réclament et attendent à raison. Cette vision commune constitue la base des progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective. Guidé par les besoins des autorités nationales qui s'efforcent d'assurer la sécurité de leurs citoyens, le soutien de l'Union se concentre sur des mesures législatives et opérationnelles dans le cadre desquelles une action conjointe peut avoir une incidence sur la sécurité des États membres. Ce travail est mené en étroite collaboration avec le Parlement européen et le Conseil, en totale transparence vis-à-vis du grand public. Le plein respect des droits fondamentaux est au cœur de ce travail, car la sécurité de l'Union ne peut être assurée que lorsque les citoyens sont convaincus que leurs droits fondamentaux sont pleinement respectés.

L'Union œuvre pour **lutter contre le terrorisme** en restreignant le périmètre d'action des terroristes, appliquant de nouvelles règles rendant plus difficile leur accès aux explosifs et aux armes à feu ainsi qu'aux financements, et limitant leur circulation. Elle a intensifié les **échanges d'informations** afin de fournir aux acteurs de première ligne, les agents de police et garde-frontières, un accès aisé à des données précises et complètes, mettant pleinement à profit les informations existantes et comblant les lacunes et les angles morts en matière d'information. Une protection forte des frontières extérieures est une condition sine qua non de la sécurité dans l'espace de libre circulation sans contrôles aux frontières intérieures. En mars 2019, le Parlement européen et le Conseil sont parvenus à un accord sur un **corps européen de garde-frontières et de garde-côte**s renforcé et parfaitement équipé, le nouveau règlement devant entrer en vigueur début décembre 2019. L'Union a doté les personnes travaillant dans les communautés locales d'une plateforme et de financements en vue de l'échange de bonnes pratiques en matière de **lutte contre la radicalisation et de prévention de l'extrémisme violent**, proposant également de nouvelles règles afin de supprimer efficacement les contenus à caractère terroriste en ligne. Le soutien de l'Union a contribué à

[1] COM(2015) 185 final du 28.4.2015.
[2] COM(2016) 230 final du 20.4.2016.
[3] Pour les précédents rapports sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, voir: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

**rendre les villes plus résistantes** aux attentats, grâce à des plans d'action renforçant la protection des espaces publics et améliorant la capacité des villes à faire face aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire. L'Union s'est penchée sur les **menaces liées au cyberespace et à la cybersécurité**, mettant en place une nouvelle stratégie européenne en matière de cybersécurité et adoptant une législation pertinente à cet égard, tout en s'attaquant à la **désinformation** afin de mieux protéger nos élections. Elle continue de renforcer la sécurité de nos **infrastructures numériques critiques**, notamment en développant la coopération en matière de **cybersécurité des réseaux 5G** en Europe.

Néanmoins, beaucoup reste à faire. En effet, la diffusion en direct de l'attaque d'une synagogue et du meurtre de deux citoyens à Halle, en Allemagne, le 9 octobre 2019, est venue rappeler brutalement la menace de l'extrémisme violent de droite et de l'antisémitisme. Cette retransmission a également mis en exergue l'utilisation abusive de l'internet par les terroristes à des fins de propagande, et donc la **nécessité de règles communes à l'échelle de l'Union pour la suppression des contenus à caractère terroriste en ligne**. Les 7 et 8 octobre 2019, le Conseil «Justice et affaires intérieures» a débattu de l'extrémisme violent et du terrorisme de la mouvance de droite, soulignant le besoin d'intensifier le travail de lutte contre la propagation des contenus illicites d'extrême droite en ligne et hors ligne. En parallèle, le meurtre de trois agents de police et d'un agent administratif dans l'enceinte de la préfecture de police de Paris le 3 octobre 2019 démontre que la menace du terrorisme inspiré du djihad demeure réelle et que les efforts actuels de l'Union en soutien aux États membres dans la lutte contre cette menace doivent se poursuivre. La récente évasion de djihadistes détenus dans une prison au nord de la Syrie pourrait également nuire gravement à la sécurité en Europe. Il est important que les États membres utilisent pleinement les systèmes d'information existants pour détecter et identifier les combattants terroristes étrangers lorsqu'ils traversent les frontières extérieures. De plus, des travaux sont actuellement menés sur l'utilisation des informations collectées sur le théâtre des opérations afin de traduire en justice les combattants terroristes étrangers.

Le présent rapport fait état des récents progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, mettant en évidence les domaines nécessitant de plus amples actions. Il fait le point sur la mise en œuvre des mesures convenues en matière de **cybersécurité des réseaux 5G**, en particulier sur le **rapport d'évaluation des risques de l'UE**, publié le 9 octobre 2019, et sur la **lutte contre la désinformation**.

Le présent rapport se concentre en particulier sur la **dimension extérieure** de la coopération dans l'union de la sécurité, avec la signature de deux accords bilatéraux de **lutte contre le terrorisme** avec l'Albanie et la Macédoine du Nord et l'accomplissement de progrès dans le cadre de la coopération avec des partenaires tiers en ce qui concerne l'échange des **données des dossiers passagers**. Par ailleurs, en parallèle du présent rapport, la Commission a adopté une demande d'autorisation en vue du lancement de négociations sur un accord entre l'Union et la **Nouvelle-Zélande** concernant l'échange de données à caractère personnel pour lutter contre les formes graves de criminalité et le terrorisme.

## 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 une pierre angulaire de la réponse de l'Union aux menaces du terrorisme. À cet égard, il est important de noter que les terroristes du 21e siècle

utilisent l'internet comme principal théâtre d'opérations. Les espaces où des individus radicalisés peuvent communiquer et partager du contenu favorisent le développement de réseaux de djihadistes et de d'extrémistes violents de droite, en expansion à l'échelle mondiale. C'est pourquoi la Commission continue d'appliquer son approche à deux voies contre la radicalisation en ligne, dans le cadre de laquelle les propositions législatives en matière de suppression des contenus à caractère terroriste illicite en ligne devraient permettre de renforcer le partenariat volontaire avec les plateformes en ligne.

La **proposition législative visant à prévenir la diffusion de contenus à caractère terroriste en ligne** est essentielle dans ce contexte, car elle inclut des règles et garanties claires qui obligeraient les plateformes internet à supprimer les contenus à caractère terroriste dans l'heure suivant la réception d'une demande motivée de la part des autorités compétentes, et à adopter des mesures proactives proportionnées au niveau d'exposition aux contenus à caractère terroriste[4]. Des négociations interinstitutionnelles sont en cours entre le Parlement européen et le Conseil, et une première réunion en trilogue s'est tenue le 17 octobre 2019. Compte tenu de la menace que représentent les contenus à caractère terroriste en ligne, la Commission appelle les colégislateurs à s'accorder sur la législation proposée avant la fin de l'année 2019.

La législation proposée complète le partenariat volontaire engagé avec le secteur de l'internet et d'autres parties prenantes dans le cadre du **forum de l'UE sur l'internet**. Depuis sa création en 2015, ce forum incite les entreprises de l'internet à se montrer proactives dans la détection et la suppression des contenus à caractère terroriste en ligne, ouvrant la voie à l'initiative menée par le secteur d'une «base de données commune d'empreintes numériques» (*shared database of hashes*)[5] et à la création du Forum mondial de l'internet contre le terrorisme. L'unité de l'UE chargée du signalement des contenus sur l'internet, qui fait partie de l'agence de l'UE pour la coopération de services répressifs (Europol), joue un rôle important dans le renforcement de la coopération avec les entreprises de l'internet et la réalisation des objectifs globaux du forum de l'UE sur l'internet. Lors de la dernière réunion ministérielle du forum de l'UE sur l'internet, le 7 octobre 2019, les États membres et les représentants de haut niveau des entreprises de l'internet se sont engagés à collaborer dans le cadre du «**protocole européen de crise**». Le protocole européen de crise définit des seuils de coopération renforcée et établit de nouvelles façons d'améliorer la réaction aux crises. Ce protocole s'inscrit dans le cadre des efforts déployés à l'échelon international pour mettre en œuvre l'«appel à l'action de Christchurch»[6], cherchant à garantir une réaction rapide et coordonnée afin de contenir la diffusion en ligne de contenus viraux à caractère terroriste ou extrémiste violent.

Au-delà de ces mesures de lutte contre la radicalisation en ligne, la Commission continue de soutenir les efforts déployés aux échelons national et local pour **prévenir et lutter contre la radicalisation sur le terrain**. S'appuyant sur la vaste expérience et l'expertise solide acquises dans le cadre du réseau de sensibilisation à la radicalisation, l'Union offre un soutien ciblé

4 COM(2018) 640 final du 12.9.2018.

5 Un outil mis au point par un consortium d'entreprises afin de faciliter la coopération dans le but de prévenir la diffusion de contenus à caractère terroriste sur des plateformes internet.

6 En réponse aux attentats de Christchurch commis le 15 mars 2019 en Nouvelle-Zélande, le président français Emmanuel Macron et la première ministre néo-zélandaise Jacinda Ardern ont invité des chefs d'État ou de gouvernement ainsi que des dirigeants de plateformes en ligne à Paris, le 15 mai 2019, afin de lancer l'«appel à l'action de Christchurch». Le président Juncker a appuyé cet appel et a annoncé la création d'un protocole européen de crise.

aux acteurs locaux, comme les municipalités[7], et donne aux praticiens, chercheurs et décideurs politiques l'occasion de participer à des échanges. À titre d'exemple, le réseau a publié des orientations spécifiques et organisé des ateliers pour soutenir les autorités compétentes dans la prise en charge des enfants provenant de zones de conflit[8]. Afin de garantir la continuité des activités menées dans le cadre du réseau de sensibilisation à la radicalisation, la Commission a lancé la procédure relative à un nouveau contrat-cadre, d'une valeur estimée de 61 000 000 EUR sur une période de quatre ans, à compter de 2020[9].

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

- à conclure avant la fin de l'année les négociations sur la proposition législative visant à prévenir la diffusion de **contenus à caractère terroriste en ligne**.

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

L'Union a intensifié les échanges d'informations, facilitant la lutte contre la fraude à l'identité[10], renforçant les contrôles aux frontières[11], modernisant les bases de données des services répressifs à l'échelle de l'Europe[12], palliant les déficits d'information[13] et renforçant

---

7 S'agissant de la coopération avec les municipalités dans le domaine de la sécurité, voir également la section V.2 relative à la préparation et à la protection, et notamment la protection des espaces publics.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_fr.pdf.

9 Le contrat-cadre est divisé en deux lots: 29 000 000 EUR pour soutenir les activités du réseau de sensibilisation à la radicalisation durant les quatre prochaines années, et 32 000 000 EUR pour renforcer les capacités des États membres, des autorités nationales, régionales et locales et des pays tiers prioritaires afin de lutter efficacement contre la radicalisation, en particulier en donnant des occasions de nouer des contacts, en proposant des services ciblés et axés sur les besoins et en effectuant des recherches et des analyses.

10 Règlement (UE) 2019/1157 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.

11 Mise en place de vérifications systématiques réalisées aux frontières extérieures pour tous les citoyens, à l'aide du système d'information Schengen. Tous les États Schengen, ainsi que la Roumanie, la Bulgarie, la Croatie et Chypre, appliquent à leurs frontières extérieures les règles relatives aux vérifications systématiques dans les bases de données pertinentes, telles qu'elles ont été instaurées en avril 2017. Conformément à ces règles, des dérogations temporaires peuvent être adoptées aux frontières maritimes ou terrestres, mais uniquement pour les citoyens de l'UE, compte tenu de l'effet disproportionné sur la fluidité du trafic. Actuellement, de telles dérogations ont été notifiées par six États membres ou pays associés à Schengen (la Croatie, la Finlande, la Hongrie, la Lettonie, la Norvège et la Slovénie). S'agissant des frontières terrestres, la possibilité de déroger aux règles relatives aux vérifications systématiques a expiré en avril 2019.

12 Le système d'information Schengen renforcé [règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862 du 28 novembre 2018] et le système européen d'information sur les casiers judiciaires étendu aux ressortissants de pays tiers [règlement (UE) 2019/816 du 17 avril 2019]. Le renforcement du système d'information Schengen comprend l'obligation générale d'introduire les signalements liés au terrorisme dans le système.

l'agence de l'UE pour la coopération de services répressifs (Europol)[14]. Cette stratégie repose avant tout sur l'**interopérabilité des systèmes d'information de l'UE**[15], qui requiert d'utiliser au mieux les informations existantes et de combler les angles morts en matière d'information. Répondant aux besoins des acteurs de première ligne, cette interopérabilité donnera aux agents des services répressifs, aux garde-frontières et aux agents chargés des services de migration un accès plus rapide et plus systématique aux informations, contribuant ainsi à améliorer la sécurité intérieure et la gestion des frontières.

Néanmoins, l'interopérabilité et toute l'innovation que cela implique n'auront des effets réels sur la gestion de la sécurité, des frontières et des flux migratoires sur le terrain que si chaque État membre met pleinement en œuvre la législation correspondante. Pour cette raison, la **mise en œuvre** de l'interopérabilité est une priorité absolue pour l'union de la sécurité, à la fois sur le plan politique et technique. La Commission et l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) soutiennent les États membres en mettant leur expertise à leur disposition et en assurant l'échange de bonnes pratiques au moyen d'un réseau de coordinateurs nationaux et d'un tableau de bord qui permettront l'application de modalités de suivi et de coordination efficaces. 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.

Entre-temps, le Parlement européen et le Conseil doivent encore **achever le travail législatif** à cet égard. Il est essentiel de parvenir rapidement à un accord sur toutes les propositions législatives en attente pour assurer le déploiement complet et en temps voulu de l'interopérabilité. Premièrement, dans le cadre de la mise en œuvre technique du **système européen d'information et d'autorisation concernant les voyages**, il est nécessaire d'apporter des modifications techniques aux règlements correspondants[16] afin de configurer pleinement le système. La Commission invite le Parlement européen à accélérer son travail de modification technique afin de démarrer les négociations interinstitutionnelles le plus rapidement possible. Deuxièmement, les négociations interinstitutionnelles concernant la proposition de mai 2018 visant à renforcer et à améliorer le **système d'information sur les visas**[17] actuel sont toujours en cours. Sur la base de la première réunion en trilogue, qui s'est tenue le 22 octobre 2019, la Commission invite les deux colégislateurs à conclure rapidement les négociations. Troisièmement, la proposition de la Commission de mai 2016 visant l'extension du champ d'application d'**Eurodac**[18] est toujours dans l'attente d'un accord. Cette

---

13 Le système d'entrée/de sortie de l'UE [règlement (UE) 2017/2226 du 30 novembre 2017] et le système européen d'information et d'autorisation concernant les voyages [règlements (UE) 2018/1240 et (UE) 2018/1241 du 12 septembre 2018].

14 Ces dernières années, le rôle d'Europol a été considérablement élargi et approfondi. L'agence a vu son rôle renforcé avec l'adoption du règlement relatif à Europol en 2016 [règlement (UE) 2016/794 du 11 mai 2016]. Depuis lors, les États membres ont échangé beaucoup plus d'informations avec et via Europol. L'établissement du Centre européen de lutte contre le terrorisme d'Europol (ECTC) a renforcé les capacités analytiques d'Europol dans les affaires de terrorisme. Le budget d'Europol a constamment augmenté ces dernières années, passant de 82 000 000 EUR en 2014 à 138 000 000 EUR en 2019. Les négociations pour le budget 2020 sont en cours.

15 Règlements (UE) 2019/817 et (UE) 2019/818 du 20 mai 2019.

16 Règlements (UE) 2018/1240 et (UE) 2018/1241 du 12 septembre 2018.

17 COM(2018) 302 final du 16.5.2018.

18 COM(2016) 272 final du 4.5.2016.

proposition comprend d'étendre la conservation des empreintes digitales et données pertinentes des ressortissants de pays tiers en séjour irrégulier, en plus de la conservation actuelle des empreintes digitales et données pertinentes des demandeurs d'asile et des personnes appréhendées en lien avec le franchissement irrégulier d'une frontière extérieure. Les modifications proposées allongeraient également la durée de conservation des empreintes digitales et données pertinentes des ressortissants entrés de manière illégale dans l'UE. La Commission invite les colégislateurs à adopter la proposition.

**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 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**;
- à conduire et à conclure rapidement les négociations sur la proposition de renforcement du **système d'information sur les visas** actuel;
- à adopter la proposition législative relative à **Eurodac** (*priorité de la déclaration commune*).

*3. Restreindre le périmètre d'action des terroristes*

L'Union a pris des mesures fermes pour restreindre le périmètre d'action des terroristes, appliquant de nouvelles règles rendant plus difficile l'accès des terroristes et autres criminels aux explosifs[19], aux armes à feu et aux financements[20] , et limitant leur circulation[21].

Afin de renforcer la réponse judiciaire face au terrorisme, l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) a mis sur pied le 1er septembre 2019 un **registre judiciaire antiterroriste européen**. Le registre collectera des informations judiciaires afin d'établir des liens entre différentes procédures engagées contre des personnes suspectées d'avoir commis une infraction terroriste, renforçant partant la coordination entre les procureurs dans les enquêtes antiterroristes ayant de potentielles implications transfrontalières et transfrontières.

De plus amples efforts sont néanmoins nécessaires pour appuyer et faciliter les enquêtes dans les affaires transfrontalières et transfrontières, notamment en ce qui concerne l'**accès des services répressifs aux preuves électroniques**. En ce qui concerne les propositions législatives d'avril 2018 visant à améliorer l'accès transfrontière aux preuves électroniques dans les enquêtes judiciaires[22], le Parlement européen doit encore adopter sa position de négociation pour que les colégislateurs puissent entamer les négociations. 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. Sur la base de sa

[19] Règlement (UE) 2019/1148 du 20 juin 2019 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs. Le règlement est entré en vigueur le 31 juillet 2019 et s'appliquera 18 mois après son entrée en vigueur.

[20] Directive (UE) 2019/1153 du 11 juillet 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.

[21] Mise en place de vérifications systématiques réalisées aux frontières extérieures pour tous les citoyens, à l'aide du système d'information Schengen.

[22] COM(2018) 225 final du 17.4.2018 et COM(2018) 226 final du 17.4.2018.

proposition de réglementation interne de l'UE, la Commission entame également des **négociations internationales** visant à améliorer l'accès transfrontière aux preuves électroniques. Le 25 septembre 2019, la Commission et les autorités américaines ont organisé la première session formelle de négociation relative à un **accord entre l'UE et les États-Unis sur l'accès transfrontière aux preuves électroniques**. Une autre session est prévue le 6 novembre 2019. Dans le contexte des négociations en cours sur un **deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité du Conseil de l'Europe**, la Commission a participé à trois sessions de négociation au nom de l'Union en juillet, septembre et octobre 2019. Bien que ces négociations aient bien avancé, plusieurs grands thèmes revêtant un intérêt particulier pour l'Union doivent encore être abordés, notamment les garanties en matière de protection des données. La négociation d'un deuxième protocole additionnel se poursuivra en novembre 2019 et tout au long de l'année 2020. Il importe de poursuivre rapidement ces deux négociations afin de faire progresser la coopération internationale en matière de partage des preuves électroniques, tout en garantissant la compatibilité avec le droit de l'Union et avec les obligations des États membres qui en découlent, en tenant également compte de l'évolution future du droit de l'Union.

Du fait des préoccupations actuelles soulevées par le blanchiment de capitaux, le Parlement européen a adopté le 19 septembre 2019 une **résolution sur l'état d'avancement de la mise en œuvre de la législation de l'Union relative à la lutte contre le blanchiment de capitaux**[23], en réponse aux quatre rapports sur le blanchiment de capitaux adoptés par la Commission le 24 juillet 2019[24]. Le Parlement européen a invité les États membres à garantir la mise en œuvre rapide et en bonne et due forme des directives anti-blanchiment. Il a également invité la Commission à déterminer si un règlement anti-blanchiment serait plus adéquat qu'une directive et à étudier la nécessité d'un mécanisme de coordination et d'appui pour les cellules de renseignement financier.

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

- à parvenir rapidement à un accord sur les propositions législatives relatives aux **preuves électroniques** (*priorité de la déclaration commune*).

### *4. Renforcer la cybersécurité*

Le renforcement de la cybersécurité reste un aspect essentiel de l'établissement d'une union de la sécurité réelle et effective. Mettant en œuvre la stratégie européenne de 2017 en matière de cybersécurité[25], l'Union a amélioré sa résilience en devenant plus résistante aux attaques et plus apte à les surmonter rapidement. Par ailleurs, elle a renforcé sa force de dissuasion en augmentant les chances que les assaillants soient appréhendés et sanctionnés, notamment grâce à l'application d'un cadre pour une réponse diplomatique conjointe de l'UE face aux

[23] https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_FR.html.

[24] 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 du 24.7.2019]; 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 24.7.2019]; 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 24.7.2019]; rapport évaluant le cadre de coopération entre les cellules de renseignement financier [COM(2019) 371 final du 24.7.2019].

[25] JOIN(2017) 450 final du 13.9.2017.

actes de cybermalveillance. L'Union soutient également les États membres en matière de cyberdéfense, avec la mise en œuvre du cadre stratégique de cyberdéfense de l'UE.[26]

Avec l'entrée en vigueur du règlement sur la cybersécurité[27] en juin 2019, le **cadre européen de certification de cybersécurité** est en train de prendre forme. La certification joue un rôle clé dans le renforcement de la confiance et de la sécurité à l'égard des produits et services qui revêtent une importance majeure pour le marché unique numérique. Le cadre de certification fournira des systèmes de certification à l'échelle européenne, prenant la forme d'un ensemble complet de règles, d'exigences techniques, de normes et de procédures. Il réunit deux groupes d'experts, à savoir le groupe européen de certification de cybersécurité, représentant les autorités des États membres, et le groupe de parties prenantes pour la certification de cybersécurité, représentant l'industrie. Ce dernier réunit des parties prenantes du côté tant de la demande que de l'offre de produits TIC et services TIC, y compris les petites et moyennes entreprises, les fournisseurs de services numériques, les organismes européens et internationaux de normalisation, les organismes d'accréditation nationaux, les autorités de contrôle de la protection des données, les organismes d'évaluation de la conformité.

Parallèlement, le Parlement européen et le Conseil doivent encore parvenir à un accord sur l'initiative législative[28] pour un **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et d'un Réseau de centres nationaux de coordination**. La proposition vise à renforcer les capacités de l'Union en matière de cybersécurité en stimulant l'écosystème technologique et industriel européen de la cybersécurité ainsi qu'en coordonnant et en mettant en commun les ressources correspondantes. La Commission invite les deux colégislateurs à reprendre et à conclure rapidement les négociations interinstitutionnelles sur cette initiative prioritaire visant à renforcer la cybersécurité.

Les travaux d'amélioration de la cybersécurité comprennent l'appui à l'échelon national et à l'échelon régional[29].

Au-delà des cybermenaces ciblant les systèmes et les données, l'UE continue de faire face aux défis complexes et multiformes que posent les **menaces hybrides**. Au Conseil, un groupe de travail horizontal consacré à la lutte contre les menaces hybrides a été mis sur pied en vue d'améliorer la résilience de l'Union et de ses États membres aux menaces hybrides et de soutenir les actions de renforcement de la résilience des sociétés aux crises. La Commission européenne et le Service européen pour l'action extérieure appuient les efforts accomplis au titre du cadre commun de 2016 en matière de lutte contre les menaces hybrides[30] et de la communication conjointe de 2018[31] intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides». En outre, le Centre commun de recherche élabore un cadre conceptuel pour caractériser les menaces hybrides, dans l'objectif d'aider les États membres et leurs autorités compétentes à recenser les types d'attaques hybrides auxquels ils peuvent

---

26 Cadre stratégique de cyberdéfense de l'UE (mise à jour de 2018) tel qu'il a été adopté par le Conseil le 19 novembre 2018 (14413/18).

27 Règlement (UE) 2019/881 du 17 avril 2019.

28 COM(2018) 630 final du 12.9.2018.

29 Par exemple, la Commission soutient un partenariat interrégional pour l'innovation dans le domaine de la cybersécurité réunissant la Bretagne, la Castille-et-León, la Rhénanie-du-Nord-Westphalie, la Finlande-Centrale et l'Estonie. Ce partenariat entend créer une chaîne de valeur de la cybersécurité européenne, axée sur la commercialisation et l'intensification des innovations.

30 JOIN(2016) 18 final du 6.4.2016.

31 JOIN(2018) 16 final du 13.6.2018.

être confrontés. Le modèle examine la façon dont un acteur (public ou non) emploie un ensemble d'outils (allant de la désinformation à l'espionnage ou à des opérations physiques) dans différents domaines (économiques, militaires, sociaux, politiques) pour toucher une cible et, ainsi, atteindre une série d'objectifs.

**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**.

## III. RENFORCER LA SÉCURITÉ DES INFRASTRUCTURES NUMÉRIQUES

Les réseaux de cinquième génération (5G) s'apprêtent à devenir l'épine dorsale d'économies et de sociétés de plus en plus numérisées. Des milliards d'objets et de systèmes connectés sont concernés, y compris dans des secteurs critiques tels que l'énergie, les transports, la banque et la santé, ainsi que des systèmes de contrôle industriel qui véhiculent des informations sensibles et étayent des dispositifs de sécurité. Il est donc essentiel de garantir la cybersécurité et la résilience des réseaux 5G.

Dans le cadre d'une approche coordonnée, les États membres ont publié le 9 octobre 2019 un rapport sur l'**évaluation coordonnée des risques au niveau de l'UE pour la cybersécurité des réseaux 5G**, avec le soutien de la Commission européenne et de l'Agence de l'Union européenne pour la cybersécurité[32]. Cette étape majeure s'inscrit dans la mise en œuvre de la recommandation de la Commission européenne adoptée en mars 2019 en vue d'assurer un niveau élevé de cybersécurité des réseaux 5G dans toute l'UE[33]. Le rapport est fondé sur les résultats des évaluations nationales des risques en matière de cybersécurité effectuées par tous les États membres. Il recense les principales menaces et les principaux acteurs malveillants, les actifs les plus sensibles, les principales vulnérabilités (techniques et autres) et plusieurs risques stratégiques. Cette évaluation sert de base pour définir des mesures d'atténuation pouvant être appliquées aux niveaux national et européen.

Le rapport recense plusieurs **difficultés majeures en matière de cybersécurité**, qui risquent fortement d'apparaître ou de prendre de l'ampleur avec les réseaux 5G. Ces défis en matière de sécurité sont principalement liés aux *innovations* clés permises par la technologie 5G, en particulier en ce qui concerne l'importance des logiciels et la large palette de services et d'applications rendus possibles par la 5G, ainsi qu'au rôle des *fournisseurs* dans la construction et l'exploitation des réseaux 5G et au degré de dépendance envers certains fournisseurs. Cela signifie que les produits, services et opérations des fournisseurs font de plus en plus partie de la «surface d'attaque» des réseaux 5G. De plus, le profil de risque de chaque fournisseur prendra une importance particulière, notamment la probabilité que le fournisseur subisse des ingérences d'un pays tiers.

---

[32] L'évaluation coordonnée des risques au niveau de l'UE pour la cybersécurité des réseaux 5G a été réalisée par le groupe de coopération des autorités compétentes tel qu'il a été institué par la directive sur la sécurité des réseaux et des systèmes d'information [directive (UE) 2016/1148 du 6 juillet 2016], avec l'aide de la Commission européenne et de l'Agence de l'Union européenne pour la cybersécurité: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019) 2355 final du 26.3.2019.

Conformément au processus fixé dans la recommandation de mars 2019 de la Commission, les États membres devraient convenir avant le 31 décembre 2019 d'une boîte à outils de **mesures d'atténuation** pour parer aux risques en matière de cybersécurité recensés à l'échelon national et de l'Union. La Commission européenne et le Service européen pour l'action extérieure continueront également d'échanger avec des partenaires partageant les mêmes idées sur la cybersécurité et la résilience des réseaux 5G. À cet égard, la Commission est en contact avec l'OTAN au sujet de l'évaluation coordonnée des risques au niveau de l'UE pour la cybersécurité des réseaux 5G.

## IV. LUTTE CONTRE LA DÉSINFORMATION ET PROTECTION DES ÉLECTIONS CONTRE LES MENACES LIÉES AU CYBERESPACE

L'Union a établi un **cadre pour une action coordonnée contre la désinformation**, qui respecte pleinement les valeurs et droits fondamentaux européens[34]. Au titre du plan d'action contre la désinformation[35], les travaux se poursuivent pour restreindre le périmètre d'action de la désinformation, notamment en vue de protéger l'intégrité des élections.

Cette stratégie repose avant tout sur le travail mené auprès de l'industrie au moyen du **code d'autorégulation relatif aux bonnes pratiques sur la désinformation** consacré aux plateformes en ligne et au secteur de la publicité, applicable depuis octobre 2018[36]. La Commission a évalué l'efficacité du code après sa première année d'utilisation, en se basant sur les rapports d'auto-évaluation annuels soumis par les plateformes en ligne et les autres signataires du code, publiés le 29 octobre 2019 avec une déclaration de la Commission[37]. Globalement, les rapports démontrent d'importants efforts de la part des signataires pour honorer leurs engagements.

Les mesures prises par les signataires des plateformes dans le cadre des cinq piliers d'engagement du code varient sur le plan de la rapidité et de la portée. De façon générale, de plus amples progrès ont été accomplis en ce qui concerne le respect des engagements pris en lien avec l'élection européenne de 2019, à savoir entraver les incitations à la publicité et à la monétisation de la désinformation (pilier 1), garantir la transparence de la publicité politique et engagée (pilier 2) et veiller à l'intégrité des services pour empêcher les comptes fictifs et comportements non authentiques (pilier 3). En revanche, les progrès sont moins importants voire inexistants pour ce qui est des engagements du pilier 4 (donner des moyens d'agir aux consommateurs) et du pilier 5 (donner des moyens d'agir à la communauté de la recherche, notamment moyennant la fourniture par les plateformes d'un accès pertinent et respectant la vie privée à des jeux de données à des fins de recherche). Des différences existent également

---

34 Voir le plan d'action contre la désinformation [JOIN(2018) 36 final du 5.12.2018].

35 JOIN(2019) 12 final du 14.6.2019.

36 En vertu du code, les plateformes en ligne Google, Facebook, Twitter, et Microsoft se sont engagées à prévenir l'utilisation de leurs services à des fins de manipulation par des acteurs malveillants, à garantir la transparence et à permettre l'identification de la publicité à caractère politique, et à prendre d'autres mesures pour améliorer la transparence, la responsabilité et la fiabilité de l'écosystème en ligne. Les associations professionnelles du secteur de la publicité se sont aussi engagées à coopérer avec ces plateformes pour améliorer la surveillance des placements de publicité et mettre au point des outils de sécurité des marques visant à limiter le placement de publicités sur les sites internet qui diffusent de fausses informations.

37 https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. Outre Google, Facebook, Twitter et Microsoft, les autres signataires du code comptent Mozilla, sept associations nationales ou européennes représentant le secteur de la publicité, et EDiMA, une association européenne représentant les plateformes et d'autres entreprises technologiques actives dans le secteur de l'internet.

en ce qui concerne l'envergure des actions entreprises par chaque plateforme pour garantir le respect de leurs engagements, et entre les États membres en ce qui concerne le déploiement de leurs mesures. La Commission continue de travailler avec les signataires du code et d'autres parties prenantes afin d'intensifier les mesures prises contre la désinformation.

Au titre du plan d'action contre la désinformation, la Commission et la haute représentante, en coopération avec les États membres, ont mis sur pied un **système d'alerte rapide** pour lutter contre les campagnes de désinformation. Le système d'alerte rapide a permis aux institutions de l'Union et aux États membres de partager des informations et des analyses en amont des élections de 2019 au Parlement européen, et de coordonner leurs actions. Ces travaux ont pris davantage d'ampleur après les élections, notamment grâce aux échanges quotidiens au niveau opérationnel et aux trois réunions entre les points de contact des systèmes d'alerte rapide organisées par différents États membres.

Une autre mesure pratique de détection des messages de désinformation a vu le jour dans le cadre des travaux de l'**équipe de communication stratégique** «StratComm», et en particulier du groupe de travail East Stratcom, qui dirige le projet «EUvsDisinfo», ayant pour mission de surveiller, analyser et combattre la désinformation «pro-Kremlin»[38]. Depuis le début de l'année 2019, le premier budget consacré à la lutte contre la désinformation, s'élevant à 3 000 000 EUR, a permis d'intensifier et d'élargir ces travaux afin d'inclure la surveillance et l'analyse de la désinformation pro-Kremlin sur le web, les plateformes de radiodiffusion et les réseaux sociaux dans 19 langues, dont l'anglais, le serbe et l'arabe. La quantité d'activités de désinformation détectées a plus que doublé, grâce au renforcement de la capacité de surveillance: en effet, près de 2 000 affaires de désinformation ont été recensées en 2019, contre 765 pendant la même période en 2018. Le groupe de travail East Stratcom a joué un rôle majeur dans la surveillance et la révélation d'activités de désinformation pro-Kremlin qui ont ciblé les élections 2019 au Parlement européen. Les travaux de recherche étaient associés à une campagne de sensibilisation aux tentatives d'ingérence dans les processus électoraux dans le monde. Le travail d'East Stratcom, mené en étroite collaboration avec le Parlement européen et la Commission, a donné lieu à plus de 20 interviews dans la presse, et la campagne a fait appel à plus de 300 journalistes.

La Commission a également pris des mesures pour **réduire la diffusion d'informations trompeuses et d'idées reçues sur les institutions et politiques européennes**. Elle a mis sur pied un réseau d'experts en communication au moyen d'un portail en ligne fournissant des supports d'information interactifs sur les politiques européennes et le défi que représente la désinformation, ainsi que son impact sur la société. Elle a également lancé une série de campagnes sur les réseaux sociaux visant à lutter contre la désinformation[39], en collaboration avec le Parlement européen et le Service européen pour l'action extérieure.

## 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*

Les mesures adoptées dans le cadre de l'union de la sécurité ne porteront véritablement leurs fruits en matière de sécurité que si tous les États membres garantissent leur mise en œuvre

[38] www.euvsdisinfo.eu.
[39] https://europa.eu/euprotects/.

rapide et complète. À cette fin, la Commission aide activement les États membres à mettre en œuvre la législation européenne, notamment au moyen de financements et en facilitant l'échange des meilleures pratiques. La Commission fait 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 transposition de la **directive de l'UE relative aux données des dossiers passagers**[40] a expiré le 25 mai 2018. À ce jour, vingt-cinq États membres ont notifié la transposition complète de la directive[41], ce qui représente un important progrès depuis juillet 2018, date à laquelle la Commission a engagé des procédures d'infraction à l'encontre de quatorze États membres[42]. Deux États membres doivent encore notifier la transposition complète de la directive, malgré les procédures d'infraction en cours lancées le 19 juillet 2018[43]. 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**[44] a expiré le 8 septembre 2018. À ce jour, vingt-deux États membres ont notifié la transposition complète de la directive, ce qui représente un important progrès depuis novembre 2018, date à laquelle la Commission a engagé des procédures d'infraction à l'encontre de seize États membres[45]. Trois États membres doivent encore notifier la transposition complète de la directive, en dépit des procédures d'infraction en cours[46]. Le 25 juillet 2019, la Commission a envoyé un avis motivé à deux États membres pour défaut de notification de la transposition complète de la directive[47]. En réponse à ces avis, les deux États membres ont annoncé que le travail législatif serait effectué avant la fin de cette année.

Le délai de transposition de la **directive relative au contrôle de l'acquisition et de la détention d'armes**[48] a expiré le 14 septembre 2018. À ce jour, treize États membres ont notifié la transposition complète de la directive. Quinze États membres doivent encore notifier la transposition complète de la directive, malgré les procédures d'infraction en cours lancées le 22 novembre 2018[49]. Le 25 juillet 2019, la Commission a envoyé des avis motivés à

---

40 Directive (UE) 2016/681 du 27 avril 2016. Le Danemark n'a pas participé à l'adoption de cette directive et n'est pas lié par celle-ci ni soumis à son application.

41 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 (situation au 17 octobre 2019).

42 Voir le seizième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2018) 690 final du 10.10.2018.

43 La Slovénie a notifié une transposition partielle. L'Espagne n'a notifié aucune mesure de transposition (situation au 17 octobre 2019).

44 Directive (UE) 2017/541 du 15 mars 2017. La directive n'est pas applicable au Royaume-Uni, en Irlande et au Danemark.

45 Voir le dix-septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2018) 845 final du 11.12.2018.

46 La Grèce et le Luxembourg n'ont pas notifié de mesures nationales de transposition. La Pologne a notifié des mesures nationales représentant une transposition partielle de la directive (situation au 17 octobre 2019).

47 La Grèce et le Luxembourg.

48 Directive (UE) 2017/853 du 17 octobre 2019.

49 La Belgique, l'Estonie, la Pologne, le Royaume-Uni, la Slovaquie, la Suède et la Tchéquie ont notifié des mesures de transposition pour une partie des nouvelles dispositions. L'Allemagne, Chypre, l'Espagne, le

20 États membres pour défaut de notification de la transposition complète de la directive. Cinq États membres ont répondu à cet avis en notifiant la transposition complète de la directive[50].

Le délai fixé pour la transposition de la **directive relative à la protection des données dans le domaine répressif**[51] a expiré le 6 mai 2018. À ce jour, vingt-cinq États membres ont notifié la transposition complète de la directive, ce qui représente un important progrès depuis juillet 2018, date à laquelle la Commission a engagé des procédures d'infraction à l'encontre de dix-neuf États membres[52]. Trois États membres doivent encore notifier la transposition complète de la directive, en dépit des procédures d'infraction en cours[53]. Le 25 juillet 2019, la Commission a décidé de saisir la Cour de justice de l'Union européenne de recours contre deux États membres[54] pour non-transposition de la directive et a adressé une lettre de mise en demeure à un État membre[55] pour avoir omis de transposer complètement la directive[56].

La Commission évalue actuellement la transposition de la **4e directive anti-blanchiment**[57], tout en vérifiant que ses dispositions sont mises en œuvre par les États membres. Ces derniers devaient transposer la directive dans leur droit national au plus tard le 26 juin 2018. La Commission maintient des procédures d'infraction à l'encontre de vingt-et-un États membres, car elle a estimé que les communications qu'ils lui avaient transmises ne constituaient pas une transposition complète de ladite directive[58].

La Commission a évalué la conformité de la transposition des **directives de lutte contre la cybercriminalité**. Elle a engagé en juillet et en octobre 2019 des procédures d'infraction à l'encontre de vingt-trois États membres[59], car elle a estimé que la législation d'application nationale notifiée par ces États membres ne constituait pas une transposition correcte de la **directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants**[60]. La Commission a également engagé en juillet et en octobre 2019 des procédures d'infraction à l'encontre de quatre États membres[61], car elle a estimé que la législation d'application nationale notifiée par ces États membres ne constituait pas une transposition correcte de la

---

Luxembourg, la Grèce, la Hongrie, la Roumanie et la Slovénie n'ont notifié aucune mesure de transposition (situation au 17 octobre 2019).

50 La Finlande, l'Irlande, la Lituanie, les Pays-Bas et le Portugal (situation au 17 octobre 2019).

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

52 Voir le seizième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2018) 690 final du 10.10.2018.

53 La Slovénie a notifié une transposition partielle. L'Espagne n'a 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 17 octobre 2019).

54 La Grèce et l'Espagne.

55 L'Allemagne.

56 La Grèce a notifié la transposition complète, que la Commission est en train d'évaluer.

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

58 L'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, le Danemark, l'Estonie, la Finlande, la France, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, les Pays-Bas, la Pologne, la Roumanie, le Royaume-Uni, la Slovaquie, la Suède et la Tchéquie (situation au 17 octobre 2019). Précédemment, sept procédures d'infraction en lien avec la directive ont été classées.

59 L'Allemagne, l'Autriche, la Belgique, la Bulgarie, la Croatie, l'Estonie, la Finlande, la France, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, la Suède et la Tchéquie.

60 Directive 2011/93/UE du 13 décembre 2011.

61 La Bulgarie, l'Italie, le Portugal et la Slovénie.

**directive relative aux attaques contre les systèmes d'information**[62].

**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 encore compléter la notification des mesures de transposition[63];
- 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 encore compléter la notification des mesures de transposition[64];
- la **directive relative au contrôle de l'acquisition et de la détention d'armes**, dont huit États membres doivent encore notifier la transposition en droit national et dont sept États membres doivent encore compléter la notification des mesures de transposition[65];
- la **directive relative à la protection des données dans le domaine répressif**, dont un État membre doit encore notifier la transposition en droit national et dont deux États membres doivent encore compléter la notification des mesures de transposition[66];
- la **4e directive anti-blanchiment**, dont 21 États membres doivent encore compléter la notification des mesures de transposition[67];
- la **directive relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants,** pour laquelle des procédures d'infraction pour transposition incorrecte ont été engagées à l'encontre de vingt-trois États membres[68];
- la **directive relative aux attaques contre les systèmes d'information,** pour laquelle des procédures d'infraction pour transposition incorrecte ont été engagées à l'encontre de quatre États membres[69].

*2. Préparation et protection*

Le renforcement de la résilience face aux menaces pesant sur la sécurité constitue un aspect essentiel des travaux visant à mettre en place une union de la sécurité réelle et effective. La Commission soutient les États membres et les autorités locales dans le renforcement de la protection des espaces publics, par la mise en œuvre du plan d'action d'octobre 2017 et du

62 Directive 2013/40/UE du 12 août 2013.

63 La Slovénie a notifié une transposition partielle. L'Espagne n'a notifié aucune mesure de transposition (situation au 17 octobre 2019).

64 La Grèce et le Luxembourg n'ont notifié aucune mesure de transposition. La Pologne a notifié une transposition partielle de la directive (situation au 17 octobre 2019).

65 La Belgique, l'Estonie, la Pologne, le Royaume-Uni, la Slovaquie, la Suède et la Tchéquie ont notifié des mesures de transposition pour une partie des nouvelles dispositions. L'Allemagne, Chypre, l'Espagne, le Luxembourg, la Grèce, la Hongrie, la Roumanie et la Slovénie n'ont notifié aucune mesure de transposition (situation au 17 octobre 2019).

66 La Slovénie a notifié une transposition partielle. L'Espagne n'a 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 17 octobre 2019).

67 L'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, le Danemark, l'Estonie, la Finlande, la France, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, les Pays-Bas, la Pologne, la Roumanie, le Royaume-Uni, la Slovaquie, la Suède et la Tchéquie (situation au 17 octobre 2019).

68 L'Allemagne, l'Autriche, la Belgique, la Bulgarie, la Croatie, l'Estonie, la Finlande, la France, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, la Suède et la Tchéquie.

69 La Bulgarie, l'Italie, le Portugal et la Slovénie.

partenariat sur la sécurité dans les espaces publics de janvier 2019 au titre du programme urbain pour l'UE. Ces travaux concernent les villes ayant contacté la Commission en vue d'obtenir son aide pour faire face aux difficultés qu'elles rencontraient dans la protection des espaces publics.

Les échanges de bonnes pratiques entre les autorités locales et avec les opérateurs privés sont essentiels au renforcement de la sécurité des espaces publics. Ce point était au cœur de la **semaine européenne de la sécurité**, qui s'est tenue à Nice, en France, du 14 au 18 octobre 2019, et était organisée par le projet financé par l'Union européenne «Protéger les villes alliées contre le terrorisme en sécurisant les zones urbaines». Rassemblant 500 participants issus de villes de toute l'Europe, des autorités nationales et des instituts de recherche, l'événement a souligné l'importance d'une étroite collaboration entre toutes les parties prenantes concernées, autant publiques que privées, et le rôle des nouvelles technologies pour que les villes soient mieux protégées. La protection des espaces publics faisait également partie des thèmes abordés lors de la **semaine européenne des régions et des villes**, qui s'est tenue à Bruxelles du 7 au 10 octobre 2019, comprenant un atelier sur le partenariat sur la sécurité dans les espaces publics dans le cadre du programme urbain pour l'UE. Cet événement s'est concentré sur le rôle des autorités locales dans le domaine de la sécurité, sur la législation européenne et sur les financements pour relever les principaux défis en matière de sécurité dans les espaces publics urbains, ainsi que sur certains thèmes clés tels que l'innovation au moyen de solutions et technologies intelligentes, comme le concept de la sécurité dès la conception, la prévention et l'inclusion sociale. La Commission contribue également à encourager l'innovation apportée les villes dans ces domaines, par l'intermédiaire de son dernier appel à propositions dans le cadre de l'initiative «Actions innovatrices urbaines», dont les résultats ont été annoncés en août 2019. Parmi les projets sélectionnés, trois villes (Le Pirée en Grèce, Tampere en Finlande et Turin en Italie) expérimenteront de nouvelles solutions en réponse à des questions de sécurité urbaine[70].

Afin de mieux **protéger les lieux de culte** et de connaître les besoins des différents groupes religieux, la Commission a organisé une réunion le 7 octobre 2019 avec des représentants des communautés juive, musulmane, chrétienne et bouddhiste. S'inscrivant dans la mise en œuvre du plan d'action de l'Union européenne de 2017 en faveur de la protection des espaces publics, la réunion a révélé que la sensibilisation et la préparation à l'égard de la sécurité variaient significativement d'une communauté religieuse à une autre, soulignant l'importance de plus amples échanges de bonnes pratiques. La réunion a également démontré que l'instauration de mesures de sécurité élémentaires et une meilleure sensibilisation à la sécurité n'étaient pas incompatibles avec le maintien du caractère ouvert et accessible des lieux de culte. La Commission recensera les bonnes pratiques et les supports de sensibilisation sur sa plateforme électronique dédiée aux experts, et portera cette question à l'attention des autorités chargées de la sécurité des États membres dans le cadre du forum public-privé pour la protection des espaces publics.

La menace grandissante des **drones** pour la sécurité des infrastructures et espaces publics critiques est un domaine spécifique qui requiert une attention toute particulière. Pour

[70] L'initiative «Actions innovatrices urbaines» est un instrument cofinancé par le Fonds européen de développement régional. Pour en savoir plus: https://www.uia-initiative.eu/fr/call-proposals/4th-call-proposals.

compléter la récente législation européenne[71] concernant l'exploitation en toute sécurité des drones dans l'espace aérien, et sans contrecarrer les possibilités d'utilisation bénéfique des drones, la Commission encourage les États membres à suivre les tendances d'utilisation malveillante des drones, en finançant des recherches en la matière et en facilitant l'expérimentation de contre-mesures. Les échanges d'expériences et de bonnes pratiques sont essentiels, comme l'a démontré la conférence internationale de haut niveau relative à la lutte contre les menaces posées par les aéronefs sans équipage à bord, qui s'est tenue à Bruxelles le 17 octobre 2019. Organisé par la Commission, cet événement a réuni 250 participants des États membres, d'organisations internationales, de partenaires de pays tiers, de l'industrie, des milieux universitaires et de la société civile, en vue de discuter des enjeux pour la sécurité posés par les drones et de la façon d'y faire face. La conférence a mis en exergue la nécessité de procéder à des évaluations régulières des risques causés par les drones et d'établir une étroite coopération entre le secteur de l'aviation et les autorités répressives en vue de la consolidation de la législation européenne sur l'exploitation en toute sécurité des drones. Il est également nécessaire d'expérimenter de façon plus approfondie les contre-mesures concernant les drones au moyen d'une approche européenne coordonnée. Par ailleurs, les parties présentes ont convenu que, pour que les drones soient sûrs, sécurisés, fiables d'un point de vue opérationnel et difficiles à détourner à des fins malveillantes, une coopération étroite des autorités et de l'industrie était essentiel.

### *3. Dimension extérieure*

Étant donné que la majorité des risques de sécurité auxquels l'Union fait face dépassent les frontières européennes et représentent des menaces mondiales, il est essentiel de coopérer avec les pays partenaires, les organisations et les parties prenantes concernées pour bâtir une union de la sécurité réelle et effective.

L'échange d'informations est au cœur d'une telle coopération. En plus du présent rapport, la Commission a adopté une recommandation au Conseil en vue de l'autorisation de l'ouverture de négociations sur un **accord entre l'Union et la Nouvelle-Zélande concernant l'échange de données à caractère personnel pour lutter contre les formes graves de criminalité et le terrorisme**, entre Europol et les autorités néo-zélandaises compétentes. Un tel accord renforcera davantage les capacités d'Europol à nouer un dialogue avec la Nouvelle-Zélande afin de prévenir et de combattre les criminalités qui relèvent des objectifs d'Europol. L'accord de travail d'avril 2019 entre Europol et la police néo-zélandaise fournit certes un cadre pour une coopération stratégique structurée, mais il ne fournit pas de base juridique pour l'échange de données à caractère personnel. L'échange de données à caractère personnel dans le plein respect des droits fondamentaux et du droit de l'Union est essentiel à une coopération policière opérationnelle efficace. Précédemment, la Commission a recensé huit pays prioritaires au Moyen-Orient et en Afrique du Nord sous l'angle des enjeux relatifs à la migration et de la menace terroriste, et ainsi que les besoins opérationnels d'Europol pour entamer des négociations[72]. Tenant compte des besoins opérationnels des autorités répressives de l'Union, ainsi que des avantages potentiels d'une coopération renforcée dans ce domaine comme a pu le démontrer l'appel à l'action pris à la suite de l'attentat de Christchurch en

[71] 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.

[72] Voir le onzième rapport sur les progrès réalisés vers une union de la sécurité réelle et effective [COM(2017) 608 final du 18.10.2017]. Les pays prioritaires sont l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie.

mai 2019, la Commission estime nécessaire d'ajouter la Nouvelle-Zélande sur la liste des pays prioritaires avec lesquels des négociations doivent être entamées sous peu.

Le transfert des **données des dossiers passagers** constitue une autre pierre angulaire de la coopération de l'Union en matière de sécurité avec des pays tiers partenaires. Le 27 septembre 2019, la Commission a adopté une recommandation à l'intention du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Japon aux fins du transfert de données des dossiers passagers afin de prévenir et de combattre le terrorisme et d'autres formes graves de criminalité transnationale, dans le plein respect des garanties en matière de protection des données et des droits fondamentaux[73]. La recommandation est examinée actuellement par un groupe de travail du Conseil et la Commission invite le Conseil à adopter rapidement un mandat de négociation avec le Japon. La mise en œuvre de dispositions à temps pour les Jeux olympiques de 2020 serait véritablement bénéfique pour la sécurité.

Sur le plan international, la Commission soutient les travaux réalisés par l'**Organisation de l'aviation civile internationale**, qui visent à établir une norme pour le traitement des données des dossiers passagers. Ces travaux répondent à un appel de la résolution 2396 du Conseil de sécurité de l'Organisation des Nations unies, qui exhorte tous les États membres des Nations unies à renforcer leur capacité de collecter, de traiter et d'analyser les données des dossiers passagers. Le 13 septembre 2019, la Commission a présenté une proposition[74] de décision du Conseil relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale, en ce qui concerne les normes et pratiques recommandées en matière de données des dossiers passagers. La proposition est actuellement examinée par un groupe de travail du Conseil et la Commission appelle à une adoption rapide de la décision du Conseil. La position de l'Union et de ses États membres a également été établie dans un document d'information portant sur les normes et les pratiques recommandées pour la collecte, l'utilisation, le traitement et la protection des données PNR, présenté lors de la 40e session de l'assemblée de l'Organisation de l'aviation civile internationale.

En ce qui concerne les travaux menés en vue de la conclusion d'un nouvel accord avec le **Canada** sur les données des dossiers passagers, la Commission s'efforce d'obtenir la finalisation rapide de l'accord. Parallèlement, le réexamen conjoint combiné à l'évaluation commune de l'accord avec l'**Australie** sur les données des dossiers passagers ainsi que l'évaluation commune de l'accord avec les **États-Unis** sur les données des dossiers passagers ont été lancés cet été, commençant par des visites à Canberra et à Washington en août et en septembre 2019, respectivement. La Commission a informé la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen lors d'une séance à huis clos le 14 octobre 2019 de l'état d'avancement des travaux avec le Japon, l'Australie et le Canada en ce qui concerne les données des dossiers passagers.

Des progrès ont également été enregistrés dans le domaine de la coopération en matière de sécurité avec les partenaires des **Balkans occidentaux**, avec la mise en œuvre du plan d'action conjoint d'octobre 2018 sur la lutte contre le terrorisme dans cette région. Le 9 octobre, la Commission a signé deux accords bilatéraux non contraignants de lutte contre le

[73] COM(2019) 420 final du 27.9.2019.
[74] COM(2019) 416 final du 13.9.2019.

terrorisme avec l'Albanie et la République de Macédoine du Nord[75]. Ces accords définissent les actions prioritaires sur mesure devant être menées par les autorités du pays partenaire concerné, qui englobent les cinq objectifs du plan d'action conjoint[76] et indiquent le soutien que la Commission envisage d'offrir. Des accords similaires avec les autres partenaires des Balkans occidentaux devraient être signés au cours des prochaines semaines. De plus, le 7 octobre 2019, la Commission a signé avec le Monténégro un accord sur la coopération, dans le domaine de la gestion des frontières, entre ce pays et l'Agence européenne de garde-frontières et de garde-côtes (Frontex). Cet accord permet à Frontex d'aider le Monténégro dans le domaine de la gestion des frontières, dans l'objectif de lutter contre la migration irrégulière et la criminalité transfrontière, améliorant ainsi la sécurité de la frontière extérieure de l'Union.

**Afin de renforcer la coopération avec des pays partenaires dans la lutte contre des menaces communes pour la sécurité, la Commission invite le Conseil:**

- à autoriser le lancement de négociations sur un accord entre l'Union et la **Nouvelle-Zélande** concernant l'échange de données à caractère personnel pour lutter contre les formes graves de criminalité et le terrorisme;
- à autoriser le lancement de négociations sur un accord entre l'Union et le **Japon** concernant le transfert de données des dossiers passagers;
- à adopter la proposition de **décision du Conseil relative à la position à prendre, au nom de l'Union européenne, au sein du Conseil de l'Organisation de l'aviation civile internationale**, en ce qui concerne les normes et pratiques recommandées en matière de données des dossiers passagers.

## VI. CONCLUSIONS

Le présent rapport expose le large éventail de mesures prises par l'Union pour faire face aux menaces communes auxquelles l'Europe est confrontée et renforcer notre sécurité collective. Guidés par une vision commune selon laquelle la meilleure manière de résoudre les enjeux actuels en matière de sécurité consiste à travailler ensemble et avec des pays tiers, les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective sont le résultat d'une étroite coopération entre une large palette d'acteurs pour instaurer un climat de confiance tout en partageant les ressources et en affrontant ensemble les menaces. Ces acteurs se trouvent à tous les échelons des États, qu'il s'agisse de municipalités ou d'autres acteurs locaux, de régions ou d'autorités nationales, jusqu'au niveau de l'UE, avec le Parlement européen et le Conseil. Il s'agit autant de pouvoirs publics que d'agences européennes, d'acteurs du secteur privés que de la société civile, et ils mettent à profit l'expertise, les outils et les ressources dans différents domaines d'action, comme la politique des transports, le marché unique numérique ou la politique de cohésion. Ce faisant, l'action en faveur d'une union de la sécurité s'inscrit dans la protection des droits fondamentaux, préservant et promouvant nos valeurs.

Le travail accompli dans la mise en place d'une union de la sécurité réelle et effective doit

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en.

[76] Le plan d'action conjoint prévoit des actions axées sur les cinq objectifs suivants: mettre en place un cadre robuste pour lutter contre le terrorisme; prévenir et combattre avec efficacité l'extrémisme violent; assurer un échange d'informations et une coopération opérationnelle efficaces; renforcer les capacités de lutte contre le blanchiment de capitaux et le financement du terrorisme; renforcer la protection des citoyens et des infrastructures.

continuer. Un accord doit être rapidement obtenu sur les initiatives importantes en cours, notamment; 1) la proposition législative relative à la suppression des contenus à caractère terroriste en ligne, 2) la proposition législative visant à améliorer l'accès des services répressifs aux preuves électroniques, 3) la proposition législative concernant l'établissement du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et du Réseau de centres nationaux de coordination, et 4) les propositions législatives en cours concernant des systèmes d'information plus robustes et plus intelligents aux fins de la gestion de la sécurité, des frontières et des flux migratoires. Les mesures et instruments adoptés doivent être convertis en réalité opérationnelle sur le terrain, par une mise en œuvre rapide et intégrale de la législation européenne par tous les États membres afin d'en retirer tous les bénéfices pour la sécurité. En particulier, il est essentiel que tous les États membres appliquent la législation récemment adoptée sur l'interopérabilité des systèmes d'information de l'UE aux fins de la gestion de la sécurité, des frontières et des flux migratoires pour atteindre l'objectif ambitieux d'une pleine interopérabilité d'ici 2020. Enfin, l'Europe doit rester vigilante à l'égard des menaces émergentes et changeantes, et continuer sa collaboration pour améliorer la sécurité de tous les citoyens.