COMMISSION
EUROPÉENNE

Bruxelles, le 20.3.2019
COM(2019) 145 final

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

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

{SWD(2019) 140 final}

## I. INTRODUCTION

Le présent document constitue le dix-huitième 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.

Dans la perspective des élections du Parlement européen de mai 2019, le présent rapport souligne les efforts importants déployés à différents niveaux pour combattre et prévenir les cybermenaces et la désinformation dans le contexte électoral. En réponse à la demande du Conseil européen de prendre des mesures pour protéger les systèmes démocratiques de l'Union et lutter contre la désinformation à l'approche des prochaines élections, l'Union a accompli des progrès considérables vers une action davantage coordonnée en matière de résilience des processus électoraux. Néanmoins, eu égard au peu de temps dont elle dispose pour garantir son bon état de préparation avant que les électeurs européens ne se rendent aux urnes en mai 2019, la Commission invite tous les acteurs concernés — pouvoirs publics, partis politiques et notamment plateformes en ligne — à redoubler d'efforts pour renforcer la résilience des processus électoraux et lutter contre la désinformation. Dans la perspective du prochain Conseil européen des 21 et 22 mars 2019, qui examinera les progrès réalisés dans ce domaine, la Commission invite les États membres à renforcer leur coordination pour lutter contre la désinformation et garantir la protection des élections du Parlement européen.

L'UE a accompli des progrès considérables dans la mise en place d'une union de la sécurité réelle et effective, plusieurs initiatives législatives prioritaires qui renforceront la sécurité de tous les citoyens ayant été approuvées. Au cours des derniers mois[1], le Parlement européen et le Conseil sont parvenus à un accord sur l'interopérabilité des systèmes d'information de l'UE aux fins de la gestion de la sécurité, des frontières et des flux migratoires, ainsi que sur les nouvelles règles de l'UE visant à restreindre le périmètre d'action des terroristes et des criminels, de sorte qu'il leur soit plus difficile d'accéder aux précurseurs d'explosifs, de financer leurs activités et de se déplacer sans se faire repérer. Les accords conclus sur 15 des 22 initiatives législatives présentées par la Commission dans le domaine de l'union de la sécurité (la liste desdites initiatives figure à l'*annexe I*) permettent à l'UE de mener à bien ce qui constitue un objectif prioritaire commun pour le Parlement européen, le Conseil et la Commission[2].

Des efforts supplémentaires sont toutefois nécessaires. En particulier, il est nécessaire que les colégislateurs répondent, au cours de leur mandat législatif actuel, à la menace imminente que posent les contenus à caractère terroriste en ligne, en approuvant la proposition de la Commission en la matière. Le Parlement européen et le Conseil doivent également conclure un accord sur la proposition de la Commission visant à renforcer le corps européen de garde-frontières et de garde-côtes afin d'augmenter la sécurité en protégeant davantage les frontières extérieures de l'Union.

---

[1] Cela s'inscrit dans le prolongement des progrès accomplis précédemment sur la voie d'une union de la sécurité réelle et effective. Pour un aperçu complet, voir les précédents rapports sur l'état d'avancement de l'union de la sécurité: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Voir la déclaration commune sur les priorités législatives de l'UE pour 2018-2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

Les événements tragiques qui se sont déroulés à Christchurch, en Nouvelle-Zélande, le 15 mars 2019 montrent que la menace terroriste, qu'elle soit nourrie par l'extrême droite ou par d'autres idéologies extrémistes, est toujours bien présente. Les difficultés rencontrées pour tenter de supprimer les contenus diffusés en direct sur les plateformes en ligne et éviter qu'ils ne refassent surface mettent davantage encore en lumière l'importance capitale que revêt la proposition de la Commission relative aux contenus à caractère terroriste en ligne. Il est essentiel que les colégislateurs parviennent d'urgence à un accord sur les règles proposées en vue de supprimer les contenus à caractère terroriste en ligne. Afin de lutter contre le terrorisme sous toutes ses formes, il importe également que tous les États membres mettent pleinement en œuvre la législation adoptée par l'UE en réponse notamment aux attentats terroristes perpétrés en Europe afin de restreindre le périmètre d'action des terroristes, et en particulier la directive relative à la lutte contre le terrorisme et la directive relative au contrôle de l'acquisition et de la détention d'armes. En outre, dans le cadre de la lutte contre l'extrémisme, la Commission s'est employée activement à lutter contre les discours de haine illégaux en ligne, l'islamophobie et l'antisémitisme, et a pris des mesures appropriées à cet égard.

Le présent rapport expose en outre les progrès accomplis dans la mise en œuvre d'autres dossiers prioritaires en matière de sécurité, notamment en ce qui concerne les mesures visant à améliorer la protection des espaces publics. La mise en œuvre intégrale et correcte des mesures sur lesquelles un accord est intervenu est la priorité absolue pour tirer pleinement parti des avantages d'une union de la sécurité réelle et effective. La Commission aide activement les États membres en ce sens, notamment au moyen de financements et en facilitant l'échange des meilleures pratiques. Au besoin, 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 présent rapport s'inscrit dans le contexte de la 15e Journée européenne de commémoration des victimes du terrorisme, qui s'est tenue le 11 mars 2019, soit quinze ans après les attentats perpétrés à Madrid le 11 mars 2004 et trois ans après les attentats meurtriers de Bruxelles et de Zaventem du 22 mars 2016. Le soutien apporté aux victimes d'attentats terroristes constitue un volet important des efforts déployés en vue de mettre en place une union de la sécurité réelle et effective. Afin d'intensifier encore ce soutien, la Commission a adopté, le 31 janvier 2019, une décision relative au financement du projet pilote «Mise en place d'un centre d'expertise de l'UE pour les victimes du terrorisme[3]». Le centre d'expertise de l'UE fera office de pôle d'expertise et de plateforme pour les professionnels assurant la prise en charge de victimes du terrorisme.

La Commission salue la précieuse contribution que constitue le rapport du Parlement européen sur les observations et les recommandations de la commission spéciale sur le terrorisme[4], pour les travaux communs en vue de mettre en place une union de la sécurité réelle et effective.

## II. PROGRÈS RÉALISÉS DANS LA CONCRÉTISATION DES PRIORITÉS LÉGISLATIVES

[3] C(2019) 636 du 31.1.2019.

[4] Résolution du Parlement européen du 12 décembre 2018 sur les observations et les recommandations de la commission spéciale sur le terrorisme [2018/2044(INI)].

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

L'échange d'informations est un élément essentiel du soutien que l'UE apporte aux autorités nationales dans la lutte contre le terrorisme et les formes graves de criminalité. À cet égard, l'interopérabilité des systèmes d'information de l'UE marque un changement radical dans la manière de communiquer les données aux autorités nationales, car elle permet de garantir que ces données sont exactes et complètes. Les colégislateurs sont parvenus à un accord politique sur les propositions législatives prioritaires présentées dans ce domaine en vue d'assurer l'**interopérabilité des systèmes d'information de l'UE** aux fins de la gestion de la sécurité, des frontières et des flux migratoires[5]. Les mesures proposées permettront de faire collaborer les systèmes d'information de l'UE de manière plus intelligente et plus ciblée, tout en respectant pleinement les droits fondamentaux. En permettant l'utilisation optimale des données existantes, l'interopérabilité contribuera à combler les lacunes et les angles morts en matière d'informations en contribuant à détecter les identités multiples et à lutter contre la fraude à l'identité. Lorsque les nouvelles règles auront été adoptées formellement par les colégislateurs, la Commission sera disposée à aider les États membres à mettre en œuvre ces règles. Il est nécessaire de coopérer étroitement avec les agences de l'UE et avec tous les États membres et les pays associés à l'espace Schengen pour atteindre l'objectif ambitieux consistant à réaliser 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. Dans cette perspective, un premier atelier a eu lieu le 5 mars 2019 avec des experts des États membres afin de lancer un processus de coordination efficace.

À ce stade, la future architecture des systèmes d'information de l'UE interopérables comprendra le **système d'information Schengen**[6] renforcé, le **système d'information sur les visas**[7] existant, l'extension récemment approuvée du **système européen d'information sur les casiers judiciaires**[8] aux ressortissants de pays tiers, et les nouveaux **système d'entrée/de sortie**[9] et **système européen d'information et d'autorisation concernant les voyages (ETIAS)**[10].

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, une proposition visant à apporter des modifications techniques au règlement y afférent[11]. Les modifications proposées concernent les actes juridiques régissant les systèmes d'information de l'UE qui seront interrogés par le système européen d'information et d'autorisation

---

5 COM(2017) 793 final du 12.12.2017, COM(2017) 794 final du 12.12.2017, COM(2018) 478 final du 13.6.2018, COM(2018) 480 final du 13.6.2018. L'accord politique conclu le 5 février 2019 a été approuvé par le Comité des représentants permanents du Conseil (Coreper) le 13 février 2019 et par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen le 19 février 2019.

6 Règlement (UE) 2018/1860 du 28.11.2018, règlement (UE) 2018/1861 du 28.11.2018 et règlement (UE) 2018/1862 du 28.11.2018.

7 Règlement (CE) n° 767/2008 du 9.7.2008.

8 Les colégislateurs sont parvenus à un accord politique sur cette proposition prioritaire le 11 décembre 2018 [COM(2017) 344 final du 29.6.2017]. L'accord a été approuvé par le Comité des représentants permanents du Conseil le 19 décembre 2018. Le Parlement européen a confirmé l'accord lors de sa session plénière du 11 mars 2019.

9 Règlement (UE) 2017/2226 du 30.11.2017.

10 Règlement (UE) 2018/1240 du 12.9.2018 et règlement (UE) 2018/1241 du 12.9.2018.

11 COM(2019) 4 final du 7.1.2019.

concernant les voyages dans le cadre de l'évaluation des risques posés en matière de sécurité ou d'immigration irrégulière par les ressortissants de pays tiers exemptés de l'obligation de visa préalablement à leur voyage vers l'espace Schengen. Les modifications proposées sont nécessaires pour mettre pleinement en place le système européen d'information et d'autorisation concernant les voyages. La Commission invite les colégislateurs à progresser dans leurs travaux sur les 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**[12], dans l'objectif de permettre une vérification 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 réuni en plénière a approuvé son rapport sur la proposition le 13 mars 2019, terminant ainsi la première lecture de cette proposition. La Commission invite les colégislateurs à démarrer rapidement les négociations lors de la prochaine législature du Parlement européen.

En mai 2016, la Commission proposait d'étendre la portée d'**Eurodac**[13] de manière à 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[14] 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[15], la Commission invite les colégislateurs à procéder sans tarder à l'adoption de la proposition. L'adoption de cette proposition législative permettra d'intégrer le système Eurodac à la future architecture des systèmes d'information de l'UE interopérables, 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, avant les élections européennes, la proposition législative relative à **Eurodac**, pour laquelle un accord est à portée de main (*priorité de la déclaration commune*);
- à faire avancer les travaux visant à 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**.

*2. Renforcer la sécurité par une meilleure gestion des frontières extérieures*

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. Cette mission

[12] COM(2018) 302 final du 16.5.2018.
[13] COM(2016) 272 final du 4.5.2016.
[14] https://www.consilium.europa.eu/fr/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.
[15] COM(2019) 126 final du 6.3.2019.

incombe aux États membres, qui doivent assurer la gestion de leurs frontières extérieures à la fois dans leur propre intérêt et dans l'intérêt commun de tous, avec l'aide du **corps européen de garde-frontières et de garde-côtes**. En réponse aux conclusions du Conseil européen de juin 2018[16], la Commission proposait en septembre 2018 de renforcer les capacités du corps européen de garde-frontières et de garde-côtes[17], permettant ainsi à l'Agence d'atteindre un nouveau niveau opérationnel, avec un corps permanent de 10 000 garde-frontières doté de pouvoirs exécutifs et de ses équipements propres, tout en respectant pleinement autant les droits fondamentaux que la souveraineté des États membres.

Les travaux législatifs sur la proposition progressent de manière satisfaisante et les négociations entre les colégislateurs sont entrées dans leur phase décisive. Le Parlement européen a adopté son mandat de négociation le 11 février 2019, tandis que le Conseil a reçu son mandat le 20 février 2019. Deux réunions en trilogue ont eu lieu le 27 février 2019 et le 12 mars 2019. La Commission salue et soutient l'avancement des travaux sur ce dossier prioritaire, qui témoigne de la volonté de toutes les institutions d'adopter cette proposition avant les élections du Parlement européen de 2019.

**Afin de renforcer la sécurité en optimisant la gestion des frontières extérieures, la Commission invite le Parlement européen et le Conseil:**

- à adopter la proposition législative visant à renforcer le **corps européen de garde-frontières et de garde-côtes** au cours de la législature actuelle du Parlement européen (*initiative annoncée dans le discours sur l'état de l'Union en 2018*).

*3. Prévenir la radicalisation*

Le traitement des contenus à caractère terroriste en ligne demeure un défi majeur dans la lutte contre le terrorisme et la prévention de la radicalisation. Ce type de contenus a joué un rôle dans la plupart des attentats perpétrés sur le sol européen ces deux dernières années, que ce soit en incitant à commettre une attaque, en fournissant des instructions sur le mode opératoire ou en glorifiant les issues fatales. Afin de lutter contre le danger manifeste et imminent que représente ce type de contenus, la Commission a présenté, à l'occasion du discours sur l'état de l'Union en 2018 du président Juncker, une proposition[18] de règlement sur les **contenus à caractère terroriste en ligne**, qui visait à établir un cadre juridique afin d'empêcher l'utilisation abusive des services d'hébergement pour la diffusion en ligne de contenus à caractère terroriste. Tout en garantissant pleinement le respect de la liberté d'expression et d'autres droits fondamentaux, il est essentiel que les futures règles prévoient des mesures efficaces pour supprimer le plus rapidement possible les contenus à caractère terroriste en ligne, étant donné que le risque de dommage causé par la publication en ligne de ces contenus augmente à chaque heure qui passe.

Alors que le Conseil a adopté son mandat de négociation en décembre 2018, les travaux au Parlement européen sont toujours en cours et devraient permettre à ce dernier d'adopter son mandat de négociation au cours du mois de mars 2019[19]. La Commission invite les deux

[16] https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.
[17] COM(2018) 631 final du 12.9.2018.
[18] COM(2018) 640 final du 12.9.2018.
[19] La commission du marché intérieur et de la protection des consommateurs du Parlement européen a adopté son avis le 4 mars 2019. La commission de la culture et de l'éducation du Parlement européen a

colégislateurs à parvenir à un accord sur la proposition législative au cours de la législature actuelle du Parlement européen, vu l'importance capitale d'établir un cadre réglementaire de l'UE prévoyant des règles et des garanties précises pour la suppression des contenus à caractère terroriste en ligne.

Parallèlement, la Commission continue de soutenir les efforts des États membres visant à **prévenir la radicalisation**. Un mécanisme de coopération spécifique de l'UE, qui réunit des représentants nationaux, contribue à garantir que le soutien de l'UE réponde aux besoins des États membres[20]. Parmi les exemples récents figurent une conférence sur le thème «Les villes de l'Union européenne contre la radicalisation», organisée en coopération avec le Comité des régions le 26 février 2019. Le 13 mars 2019, la Commission a organisé une réunion d'experts avec des responsables politiques nationaux afin de recenser les mesures pratiques à prendre pour continuer à soutenir les services pénitentiaires et de probation. Les résultats de ces travaux seront intégrés dans un manuel qu'est en train d'élaborer le réseau européen de sensibilisation à la radicalisation concernant la réhabilitation et la réinsertion des terroristes, le retour des combattants terroristes étrangers et la radicalisation des individus en prison (voir également la section IV, point 4 «À l'extérieur»).

| **Afin de prévenir la radicalisation, la Commission invite le Parlement européen:** |
|---|
| • à adopter prioritairement son mandat de négociation sur la proposition législative visant à prévenir la diffusion de **contenus en ligne à caractère terroriste**, afin de permettre aux colégislateurs de parvenir à un accord sur cette proposition au cours de sa législature actuelle (*initiative annoncée dans le discours sur l'état de l'Union en 2018*). |

*4. Renforcement de la cybersécurité*

Les cybermenaces ordinaires, qui visent les systèmes et les données, continuent d'augmenter, les activités des acteurs malveillants à l'encontre de cibles et de victimes diverses ayant connu une hausse en 2018. La lutte contre la cybercriminalité et le renforcement de la cybersécurité demeurent donc une priorité de l'action de l'Union européenne. L'UE a accompli des progrès tangibles pour renforcer sa cybersécurité, en mettant en œuvre les actions prévues dans la communication conjointe de septembre 2017[21] intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide».

Le 12 mars 2019, le Parlement européen réuni en plénière a confirmé l'accord politique auquel sont parvenus les colégislateurs en ce qui concerne **le règlement sur la cybersécurité**. Ce règlement, dont l'entrée en vigueur est prévue en mai 2019, permettra d'accroître les capacités en matière de cybersécurité et de renforcer la préparation des États membres et des entreprises. Il instaurera un cadre européen de certification de cybersécurité pour les produits, systèmes et services des technologies de l'information et de la communication. Il permettra également d'améliorer la coopération et la coordination entre les États membres et les

procédé à un vote sur son rapport le 11 mars 2019. La commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen devrait procéder au vote sur son rapport le 21 mars 2019.

[20] Les besoins des États membres en matière de prévention de la radicalisation ont été recensés, pour la première fois, dans les orientations stratégiques pour des actions de prévention au niveau de l'UE pour 2019. Les orientations stratégiques sont disponibles à l'adresse suivante: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

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

institutions, organes et organismes de l'UE, et notamment l'instance rebaptisée Agence de l'Union européenne pour la cybersécurité.

Les efforts doivent toutefois se poursuivre sur la proposition présentée par la Commission en septembre 2018 en vue d'établir le **Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination**[22]. 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. Le Parlement européen et le Conseil ont adopté leurs mandats de négociation le 13 mars 2019. La première réunion en trilogue a également eu lieu le 13 mars 2019. La Commission invite les colégislateurs à trouver rapidement un accord sur la proposition législative.

L'UE a considérablement progressé dans la poursuite de la mise en œuvre de la **réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance** (la «boîte à outils cyberdiplomatique»), répondant ainsi à l'appel du Conseil européen[23] à faire avancer les travaux relatifs à la capacité à décourager les cyberattaques et à y réagir au moyen de mesures restrictives de l'Union. Le 8 mars 2019, la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et la Commission ont présenté une proposition conjointe de règlement du Conseil concernant des mesures restrictives visant à contrer les cyberattaques qui menacent l'Union ou ses États membres. La Commission et la haute représentante demandent l'adoption rapide de cette proposition afin de renforcer la résilience de l'Union aux cyberattaques.

**Afin d'améliorer la cybersécurité, la Commission et la haute représentante invitent le Conseil:**

- à adopter le règlement du Conseil concernant des **mesures restrictives visant à contrer les cyberattaques** qui menacent l'Union ou ses États membres.

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

L'UE a pris des mesures supplémentaires visant à priver les terroristes et les criminels de leurs moyens d'action, de sorte qu'il leur soit plus difficile d'accéder aux précurseurs d'explosifs, de financer leurs activités et de se déplacer sans se faire repérer.

Le 14 février 2019, le Parlement européen et le Conseil sont parvenus à un accord politique sur la proposition de règlement relatif aux **mesures restreignant la commercialisation et l'utilisation des précurseurs d'explosifs**[24]. Une fois applicable, le règlement se traduira par des améliorations significatives du cadre législatif actuel et réduira l'accès aux précurseurs d'explosifs dangereux susceptibles d'être détournés pour la fabrication de bombes artisanales. Il permettra de remédier aux lacunes en matière de sécurité par des mesures telles que l'interdiction d'un certain nombre de substances chimiques supplémentaires, le contrôle obligatoire du casier judiciaire des personnes qui demandent une licence pour acquérir des substances faisant l'objet de restrictions, et l'indication explicite du fait que les règles applicables aux opérateurs économiques s'appliquent également aux sociétés exerçant leurs activités en ligne.

22 COM(2018) 630 final du 12.9.2018.
23 Voir les conclusions du Conseil européen de juin 2018 et d'octobre 2018.
24 COM(2018) 209 final du 17.4.2018.

En outre, dans le cadre des efforts déployés pour lutter contre le financement du terrorisme, les colégislateurs sont parvenus à un accord sur la proposition de directive visant à **faciliter l'utilisation d'informations financières et d'autre nature** à des fins de prévention et de détection d'infractions pénales graves, et d'enquêtes et de poursuites en la matière[25]. Une fois formellement adoptée et mise en œuvre, cette directive permettra aux autorités répressives et aux bureaux de recouvrement des avoirs de disposer d'un accès direct aux informations sur les comptes bancaires qui figurent dans les registres nationaux centralisés des comptes bancaires. La directive renforcera également la coopération entre les cellules de renseignement financier nationales et les autorités répressives et facilitera l'accès d'Europol aux informations financières.

Sur cette base, la Commission poursuivra sa réflexion sur la coopération entre les cellules de renseignement financier de différents États membres, dont elle fera notamment état dans le prochain rapport sur la coopération entre les cellules de renseignement financier, comme le prévoit la 5e directive anti-blanchiment[26]. De plus, donnant suite à ladite 5e directive, la Commission évalue actuellement les aspects liés à l'interconnexion potentielle des registres nationaux centralisés des comptes bancaires et des systèmes de recherche de données dans l'UE. La Commission examine également les mesures de confiscation non fondée sur une condamnation prises dans l'Union. Enfin, répondant également à un appel du Parlement européen[27], elle continuera à évaluer la nécessité, la faisabilité technique et la proportionnalité de mesures supplémentaires visant à surveiller le financement du terrorisme au sein de l'UE.

Le 19 février 2019, dans le cadre des travaux visant à lutter contre la fraude documentaire, les colégislateurs sont parvenus à un accord provisoire sur la proposition de règlement relatif au renforcement de la **sécurité des cartes d'identité des citoyens de l'Union et des titres de séjour**[28] afin que ces documents ne puissent pas être utilisés de manière frauduleuse par les criminels et les terroristes. La commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a confirmé l'accord le 11 mars 2019. Une fois adopté, le règlement introduira des éléments de sécurité minimaux pour les cartes d'identité, y compris des identifiants biométriques (une image faciale et deux empreintes digitales) sur une puce sans contact. Cela permettra d'améliorer sensiblement la sécurité des cartes nationales d'identité et des titres de séjour, et donc de rendre plus difficile l'utilisation abusive ou la falsification de ces documents par les terroristes et autres criminels aux fins d'entrer sur le territoire de l'Union européenne ou de s'y déplacer. La sécurisation accrue des documents d'identité contribuera à renforcer la gestion des frontières extérieures de l'UE, tandis que les citoyens de l'UE, grâce à des documents plus sûrs et plus fiables, pourront exercer plus facilement leurs droits de libre circulation.

---

25 Les colégislateurs sont parvenus à un accord politique sur la proposition de la Commission le 12 février 2019 [COM(2018) 213 final du 17.4.2018]. Cet accord a été approuvé par le Comité des représentants permanents du Conseil (Coreper) le 20 février 2019 et par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen le 26 février 2019.

26 L'article 65, paragraphe 2, de la directive (UE) 2018/843 (JO L 156 du 19.6.2018) prévoit que, au plus tard le 1er juin 2019, la Commission évalue le cadre pour la coopération des cellules de renseignement financier avec les pays tiers ainsi que les obstacles à surmonter et les possibilités de renforcer la coopération entre les cellules de renseignement financier au sein de l'Union, y compris la possibilité de créer un mécanisme de coordination et de soutien.

27 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 (TFTS) pour les transactions réalisées par des personnes ayant des liens avec le terrorisme et son financement dans l'espace unique de paiement en euros.

28 COM(2018) 212 final du 17.4.2018.

Les efforts doivent toutefois se poursuivre sur les propositions présentées par la Commission en avril 2018 et relatives à l'**accès aux preuves électroniques**, étant donné qu'aujourd'hui, dans plus de la moitié de l'ensemble des enquêtes pénales, une demande transfrontière d'accès à des preuves électroniques est présentée[29]. Le Conseil a adopté son mandat de négociation portant sur une proposition de règlement[30] visant à améliorer l'accès transfrontière aux preuves électroniques dans les enquêtes pénales et sur la proposition de directive[31] établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale. Toutefois, au sein du Parlement européen, les progrès sur ces propositions n'ont été que très limités depuis qu'elles ont été adoptées par la Commission en avril 2018. Eu égard à l'importance cruciale que revêt un accès efficace aux preuves électroniques pour les poursuites contre les formes de criminalité transfrontière, telles que le terrorisme ou la cybercriminalité, la Commission invite instamment le Parlement européen à avancer sur cette proposition.

Parallèlement, la Commission travaille sur deux **initiatives internationales sur l'accès aux preuves électroniques**, l'une étant menée dans le cadre des négociations en cours concernant un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest), et l'autre avec les États-Unis. La Commission a dès lors adopté, le 5 février 2019, des recommandations[32] pour les mandats de négociation relatifs à ces deux initiatives internationales. Le Conseil examine ces projets de mandat à l'heure actuelle et notamment lors de la session du Conseil «Justice et affaires intérieures» des 7 et 8 mars 2019. La Commission invite le Conseil à adopter la décision autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe, ainsi que la décision autorisant l'ouverture de négociations avec les États-Unis sur l'accès transfrontière aux preuves électroniques. Il importe de poursuivre rapidement les 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.

**Afin de restreindre le périmètre d'action des terroristes, la Commission invite:**

- le **Parlement européen** à adopter d'urgence son mandat de négociation sur les propositions législatives relatives aux **preuves électroniques** afin d'entamer sans retard les discussions en trilogue avec le Conseil (*priorité de la déclaration commune*);
- le **Conseil** à adopter la décision autorisant la participation aux négociations sur un **deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe**, ainsi que la décision autorisant l'ouverture de **négociations avec les États-Unis** sur l'accès transfrontière aux preuves électroniques.

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

[29] Les preuves électroniques sont nécessaires dans près de 85 % des enquêtes pénales et, dans les deux tiers de celles-ci, il est nécessaire de demander les preuves auprès de prestataires de services en ligne établis dans une autre juridiction. Voir l'analyse d'impact accompagnant la proposition législative [SWD(2018) 118 final du 17.4.2018].

[30] COM(2018) 225 final du 17.4.2018. 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.

[31] COM(2018) 226 final du 17.4.2018. Le Conseil a adopté son mandat de négociation sur la proposition de directive de la session du Conseil «Justice et affaires intérieures» du 8 mars 2019.

[32] COM(2019) 70 final du 5.2.2019 et COM(2019) 71 final du 5.2.2019.

La capacité des parties internes et externes à s'ingérer dans les débats publics et à manipuler les élections est plus réelle que jamais et pourrait encore s'accentuer avec les prochaines élections européennes. Les conséquences possibles, à savoir l'affaiblissement ou la délégitimation des institutions démocratiques, constituent une menace grave, stratégique et croissante. Au centre des défis en matière de sécurité auxquels l'UE est aujourd'hui confrontée par-delà les frontières nationales, cette menace nécessite la mise en place d'une réponse transfrontière commune.

Les campagnes électorales en amont des élections européennes commenceront réellement au mois de mars. Dans la perspective du Conseil européen des 21 et 22 mars 2019, la Commission invite les États membres à intensifier leur coordination et leurs échanges d'informations pour lutter contre la désinformation et protéger les élections contre les menaces liées au cyberespace. Les États membres devraient recourir à tous les outils et canaux d'information mis à leur disposition par l'UE, et notamment au nouveau système d'alerte rapide[33]. Par ailleurs, préoccupée par la situation actuelle, la Commission invite instamment les plateformes en ligne à accélérer leurs efforts dans tous les États membres afin de contribuer à garantir l'intégrité des élections européennes de mai 2019.

Afin de soutenir et d'encourager ces efforts, la Commission et la haute représentante continuent de prendre des mesures qui s'articulent autour de deux axes complémentaires pour lutter contre les menaces liées au cyberespace, à savoir la lutte contre la désinformation et l'amélioration de la résilience des processus électoraux.

*1. Lutter contre la désinformation*

L'exposition des citoyens à la désinformation à grande échelle, y compris à des informations trompeuses ou absolument fausses, peut constituer un type grave de menace liée au cyberespace, ainsi qu'un défi majeur dans la perspective des prochaines élections européennes. La Commission suit de près la mise en œuvre des mesures énoncées dans sa **communication d'avril 2018 sur la lutte contre la désinformation en ligne**[34].

En outre, les progrès réalisés au titre du **code de bonnes pratiques contre la désinformation** signé en octobre 2018 par des représentants de plateformes en ligne, des principaux réseaux sociaux, des annonceurs et du secteur de la publicité, font l'objet d'un suivi minutieux de la part de la Commission (voir ci-dessous). La Commission procédera à une évaluation globale du code au terme de sa première période d'application de 12 mois. Si la mise en œuvre et l'incidence du code de bonnes pratiques devaient ne pas être satisfaisantes, la Commission pourrait proposer de nouvelles mesures, notamment de nature législative.

Se fondant sur ces travaux et répondant à l'appel lancé par les dirigeants lors du Conseil européen de juin 2018 afin de protéger les systèmes démocratiques de l'Union, la Commission et la haute représentante ont présenté, en décembre 2018, un **plan d'action**

[33] Partie intégrante du plan d'action contre la désinformation que la Commission et la haute représentante ont présenté en décembre 2018 (voir ci-dessous), le système d'alerte rapide est une plateforme qui permettra aux États membres, aux institutions de l'UE et aux partenaires de partager des informations sur les campagnes de désinformation en cours et de coordonner leurs réponses. Le système reposera uniquement sur des informations de source ouverte, gratuites et non classifiées.

[34] COM(2018) 236 final du 26.4.2018, suivi d'un rapport de mise en œuvre [COM(2018) 794 final du 5.12.2018].

**conjoint de lutte contre la désinformation**[35]. Celui-ci souligne que, selon la **cellule de fusion de l'Union européenne contre les menaces hybrides**, ce sont les campagnes de désinformation émanant de la Fédération de Russie qui constituent la plus grande menace pour l'UE. Elles sont systématiques, bénéficient d'importantes ressources et se distinguent, par leur ampleur, des activités menées par d'autres pays. Pour contrer les risques posés par la désinformation, le plan d'action prévoit une augmentation des ressources allouées à la lutte contre ce phénomène, et en particulier à **la task force de l'Union sur la communication stratégique** du Service européen pour l'action extérieure (SEAE), y compris la task-force East Stratcom [36]. Le plan d'action prévoit également une hausse des ressources consacrées à ce problème et préconise leur renforcement au cours des deux années à venir.

Le plan d'action énonce des mesures concrètes pour combattre la désinformation, y compris la création d'un **système d'alerte rapide**. Ce dernier a été mis en place en mars 2019 par les institutions de l'Union européenne et les États membres, dans la perspective des élections du Parlement européen, afin de faciliter l'échange de données et l'évaluation des campagnes de désinformation ainsi que de lancer des alertes sur les risques de désinformation.

Le plan d'action prévoit également un suivi étroit de la mise en œuvre du code de bonnes pratiques susmentionné, signé par les plateformes en ligne. Le 29 janvier 2019, la Commission a publié les **rapports présentés par les signataires du code de bonnes pratiques** – Google, Facebook, Twitter, Mozilla et les associations commerciales représentant le secteur de la publicité; si la Commission a salué les progrès accomplis, elle a également exhorté les signataires à intensifier leurs efforts à l'approche des élections du Parlement européen[37].

Le 28 février 2019, la Commission a publié les **rapports présentés par Facebook, Google et Twitter** sur les progrès accomplis en janvier 2019 dans le cadre de leur engagement à combattre la désinformation. Dans ces rapports, les plateformes n'ont toutefois pas suffisamment démontré que de nouvelles stratégies et de nouveaux outils étaient déployés en temps utile et dotés de ressources suffisantes dans tous les États membres. Des améliorations sont clairement possibles pour tous les signataires[38]. Plus précisément, la Commission invite les plateformes à garantir la transparence des publicités à caractère politique d'ici le début de la campagne des élections européennes dans tous les États membres de l'UE, à permettre un accès approprié aux données des plateformes à des fins de recherche et de vérification des faits et à assurer une bonne coopération entre ces plateformes et les différents États membres par l'intermédiaire des points de contact au sein du système d'alerte rapide.

Le 20 mars 2019, la Commission présentera un nouveau rapport sur la mise en œuvre du code de bonnes pratiques susmentionné.

*2. Améliorer la résilience des processus électoraux*

---

35 JOIN(2018) 36 final du 5.12.2018.

36 Depuis sa création en 2015, la task force East Stratcom a répertorié, analysé et mis en lumière près de 5 000 cas de désinformation imputables à la Fédération de Russie, en révélant de nombreux scénarios de désinformation, en sensibilisant aux instruments, techniques et aux intentions qui sous-tendent les campagnes de désinformation et en les exposant au grand jour.

37 Pour plus d'information, voir: http://europa.eu/rapid/press-release_IP-19-746_fr.htm.

38 Pour plus d'informations, voir: http://europa.eu/rapid/press-release_STATEMENT-19-1379_fr.htm.

Le 12 septembre 2018, la Commission a adopté un train de mesures visant à renforcer la résilience de nos systèmes électoraux, destiné aux États membres, ainsi qu'aux fondations et aux partis politiques nationaux et européens, y compris une recommandation sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et les campagnes de lutte contre la désinformation, des orientations relatives à l'application du droit de l'UE en matière de protection des données[39], et une modification législative rendant plus strictes les règles en matière de financement des partis politiques européens.

Le Parlement européen a accueilli favorablement ce train de mesures dans la résolution qu'il a adoptée le 28 octobre 2018. Le Conseil s'est félicité de ce train de mesures dans ses conclusions du 19 février 2019, intitulées «Garantir des élections européennes libres et équitables», qui exprime l'engagement pris par tous les États membres d'adopter une approche européenne coordonnée pour protéger l'intégrité des élections européennes à venir. Le Conseil justice et affaires intérieures a discuté de l'état de la situation le 7 mars 2019.

La modification du règlement relatif **au statut et au financement des partis politiques européens et des fondations politiques européennes**[40] **introduit la possibilité de sanctionner l'utilisation illégale de données à caractère personnel en cas d'impact délibéré sur les résultats des élections** du Parlement européen. Après avoir conclu un accord politique[41] en janvier 2019, l'assemblée plénière du Parlement européen a approuvé le texte de l'amendement le 12 mars 2019. Cet amendement devrait acquérir force de loi avant les élections européennes de 2019.

La recommandation **sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen**[42] s'adresse aux États membres et aux partis et fondations politiques nationaux et européens et présente des mesures concrètes pour les acteurs concernés dans ces domaines. Afin de mettre en œuvre la recommandation, les réseaux électoraux nationaux ont nommé des points de contact pour participer à un **réseau de coopération en matière d'élections au niveau européen**, qui permet de prévenir de menaces, d'échanger des bonnes pratiques entre réseaux nationaux, de rechercher des solutions communes à des problèmes détectés et d'encourager les projets et exercices communs à plusieurs réseaux nationaux. Lors de la première réunion du réseau, qui s'est tenue le 21 janvier 2019, les participants sont convenus qu'il était essentiel d'adopter une approche globale pour garantir l'intégrité des élections tout en assurant un débat démocratique ouvert et des conditions identiques pour tous sur le terrain politique. La deuxième réunion du réseau de coopération en matière d'élections au niveau européen qui a eu lieu le 27 février 2019 portait plus particulièrement sur la surveillance et le respect des règles dans le contexte électoral, y compris la protection des données, la réglementation des médias, l'application de la législation, la transparence et les médias sociaux, ainsi que l'engagement des différentes parties prenantes dans le suivi des activités. Cette réunion a préparé le terrain pour la participation de ses membres à un exercice de cyber-résilience immédiatement après la prochaine réunion du réseau prévue le 5 avril 2019.

---

39 COM(2018) 638 final du 12.9.2018.

40 COM(2018) 636 final du 12.9.2018.

41 Le 16 janvier 2018, les colégislateurs ont conclu un accord politique qui a été approuvé par le Comité des représentants permanents du Conseil (Coreper) le 25 janvier 2019 et par la commission des affaires constitutionnelles du Parlement européen le 29 janvier 2019.

42 C(2018) 5949 final du 12.9.2018.

Un **groupe de travail ayant pour thème «Renforcer la cyber-résilience des processus électoraux»**, organisé conjointement par le Parlement européen et la Commission, s'est réuni le 19 février 2019 afin d'améliorer la sécurité et la résilience des infrastructures et systèmes électoraux et de contrer les menaces liées au cyberespace qui sont en constante évolution. Les autorités compétentes en matière de cybersécurité des États membres, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information et les plateformes en ligne, ont examiné des mesures axées sur les actions urgentes et pertinentes pour garantir l'intégrité des élections européennes de 2019.

En outre, les institutions de l'UE collaborent étroitement avec les États membres afin de mener d'autres **activités de sensibilisation** visant à protéger l'intégrité du processus électoral et de faire participer les acteurs des secteurs privé et public, y compris les médias, les plateformes en ligne et la société civile.

**Afin de lutter contre la désinformation et de garantir la résilience des processus électoraux, la Commission et la haute représentante invitent les États membres:**

- à mettre en œuvre rapidement et résolument les actions du **plan d'action conjoint sur la désinformation** de décembre 2018.

## IV. MISE EN ŒUVRE DES AUTRES DOSSIERS PRIORITAIRES EN MATIÈRE DE SÉCURITÉ

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

La mise en œuvre complète et correcte des mesures approuvées est de la plus haute priorité afin de tirer le meilleur parti d'une union de la sécurité réelle et effective. La Commission aide activement les États membres en ce sens, notamment au moyen de financements et en facilitant l'échange des meilleures pratiques. Au besoin, 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.

En ce qui concerne la mise en œuvre de la **directive relative aux données des dossiers passagers**[43], la Commission a lancé le 19 juillet 2018 des procédures d'infraction à l'encontre de 14 États membres pour défaut de communication de l'adoption de la législation nationale destinée à transposer intégralement la directive[44] – un instrument crucial dans la lutte contre le terrorisme et les formes graves de criminalité. Neuf de ces États membres ont depuis lors notifié une transposition complète[45]. Les États membres qui n'ont toujours pas effectué une transposition complète se sont vu adresser des avis motivés (l'Espagne le 24 janvier 2019, les Pays-Bas et la Finlande le 7 mars 2019). Parallèlement, la Commission continue de soutenir les efforts consentis par les États membres pour achever le développement de leurs systèmes de dossiers passagers, notamment en facilitant l'échange d'informations et de meilleures pratiques.

---

43 Directive (UE) 2016/681 du 27.4.2016.

44 Bulgarie, République tchèque, Estonie, Grèce, Espagne, France, Chypre, Luxembourg, Pays-Bas, Autriche, Portugal, Roumanie, Slovénie et Finlande.

45 Bulgarie, Estonie, Grèce, France, Chypre, Luxembourg, Autriche, Portugal et Roumanie (situation au 11 mars 2019).

Le délai de transposition de la **directive relative à la lutte contre le terrorisme**[46] a expiré le 8 septembre 2018. Le 22 novembre 2018, la Commission a lancé des procédures d'infraction à l'encontre de 16 États membres pour défaut de communication de l'adoption d'une législation nationale destinée à transposer intégralement la directive. Parmi eux, 9 États membres ont depuis lors notifié une transposition complète[47]. La Commission invite instamment les 7 autres États membres à prendre les mesures nécessaires le plus rapidement possible[48].

Le délai de transposition de la **directive relative au contrôle de l'acquisition et de la détention d'armes**[49] a expiré le 14 septembre 2018. À ce jour, 6 États membres ont notifié une transposition complète de la directive[50] et 5 États membres ont notifié une transposition partielle[51]. Le 22 novembre 2018, la Commission a adressé des lettres de mise en demeure à 22 États membres[52], y compris ceux qui ont notifié une transposition partielle.

En ce qui concerne la transposition en droit national de la **directive en matière de protection des données dans le domaine répressif**[53], le 19 juillet 2018, la Commission a lancé des procédures d'infraction à l'encontre de 19 États membres, pour défaut de communication de l'adoption d'une législation nationale garantissant la transposition complète de la directive[54]. À l'heure actuelle, 17 États membres ont notifié la transposition complète et 5 États membres ont notifié une transposition partielle de la directive[55]. À ce jour, les procédures à l'encontre de 6 États membres ont été closes[56], tandis que 9 États membres ont reçu un avis motivé le 25 janvier 2019[57].

La Commission devrait faire rapport sur la cohérence en ce qui concerne l'identification des opérateurs de services essentiels au plus tard le 9 mai 2019. Sur la base des notifications des États membres, il a été établi que 25 États membres ont intégralement transposé la **directive sur la sécurité des réseaux et des systèmes d'information**[58] et qu'un État membre l'a

---

46 Directive (UE) 2017/541 du 15.3.2017.

47 La Bulgarie, la République tchèque, l'Allemagne, l'Estonie, l'Espagne, la France, la Croatie, l'Italie, la Lettonie, la Lituanie, la Hongrie, Malte, les Pays-Bas, l'Autriche, le Portugal, la Slovaquie, la Finlande et la Suède ont notifié la transposition de la directive (situation au 11 mars 2019).

48 La Belgique, la Pologne, la Roumanie et la Slovénie ont notifié une transposition partielle. La Grèce, Chypre et le Luxembourg n'ont fait aucune notification (situation au 11 mars 2019).

49 Directive (UE) 2017/853 du 17.5.2017.

50 Danemark, France, Croatie, Italie, Malte et Autriche (situation au 11 mars 2019).

51 République tchèque, Estonie, Lituanie, Portugal et Royaume-Uni (situation au 11 mars 2019).

52 Belgique, Bulgarie, République tchèque, Allemagne, Estonie, Irlande, Grèce, Espagne, Chypre, Lettonie, Lituanie, Luxembourg, Hongrie, Pays-Bas, Pologne, Portugal, Roumanie, Slovénie, Slovaquie, Finlande, Suède et Royaume-Uni (situation au 11 mars 2019).

53 Directive (UE) 2016/680 du 27.4.2016.

54 Belgique, Bulgarie, République tchèque, Estonie, Grèce, Espagne, France, Croatie, Chypre, Lettonie, Lituanie, Luxembourg, Hongrie, Pays-Bas, Pologne, Portugal, Roumanie, Slovénie et Finlande. Les États membres transmettent des réponses à la Commission, y compris des notifications de la législation concernée, qui sont en cours d'analyse (situation au 11 mars 2019).

55 La Belgique, l'Allemagne, l'Estonie, l'Irlande, la France, la Croatie, l'Italie, la Lituanie, le Luxembourg, la Hongrie, Malte, l'Autriche, la Pologne, la Roumanie, la Slovaquie, la Suède et le Royaume-Uni ont notifié une transposition complète. La République tchèque, le Portugal, la Finlande, la Slovénie et les Pays-Bas ont notifié une transposition partielle. En outre, le Danemark a achevé la transposition de la directive (situation au 11 mars 2019).

56 Belgique, France, Croatie, Lituanie, Luxembourg et Hongrie (situation au 11 mars 2019).
Grèce, Chypre, Espagne, Slovénie, Portugal, République tchèque, Bulgarie, Lettonie et Pays-Bas (situation au 11 mars 2019).

58 Directive (UE) 2016/1148 du 27.4.2016.

transposée partiellement[59]. En janvier 2019, la Commission a clos les procédures d'infraction pour non-communication concernant 6 États membres[60]. Une procédure d'infraction pour non-communication de la transposition complète de la directive a été engagée à l'encontre de 9 États membres[61]. En ce qui concerne la transposition de la directive sur la sécurité des réseaux et des systèmes d'information, les États membres devaient communiquer à la Commission, au plus tard le 9 novembre 2018, des informations sur les opérateurs de services essentiels recensés sur leur territoire. La Commission procède actuellement à l'évaluation des informations transmises par les États membres[62].

En outre, la Commission évalue actuellement la transposition de la **4e directive anti-blanchiment**[63], tout en vérifiant la mise en œuvre de la règlementation par les États membres. La Commission a engagé des procédures d'infraction à l'encontre des 28 États membres car elle a estimé que les communications qu'ils lui avaient transmises ne constituaient pas une transposition complète de ladite directive[64]. Elle continuera à exercer ses pouvoirs toutes les fois où cela sera nécessaire pour garantir la mise en œuvre intégrale de ladite directive.

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

- la **directive relative aux données des dossiers passagers**, dont 3 États membres doivent encore notifier la transposition en droit national et dont 2 États membres doivent achever la notification des mesures de transposition[65];
- la **directive sur la sécurité des réseaux et des systèmes d'information**, dont 2 États membres doivent encore notifier la transposition en droit national et 1 État membre doit achever la notification des mesures de transposition[66];
- **la directive relative à la lutte contre le terrorisme**, dont 3 États membres doivent encore notifier la transposition en droit national et 4 États membres doivent achever la notification des mesures de transposition[67];

59 La Bulgarie, la République tchèque, le Danemark, l'Allemagne, la Grèce, l'Estonie, l'Irlande, l'Espagne, la France, la Croatie, l'Italie, Chypre, la Lettonie, la Lituanie, Malte, les Pays-Bas, l'Autriche, la Pologne, le Portugal, la Roumanie, la Slovénie, la Slovaquie, la Finlande, la Suède et le Royaume-Uni ont notifié une transposition complète. La Hongrie a notifié une transposition partielle. La Belgique et le Luxembourg n'ont notifié aucune mesure nationale de transposition à la Commission (situation au 11 mars 2019).

60 Irlande, Espagne, France, Croatie, Pays-Bas et Portugal (situation au 11 mars 2019).

61 Bulgarie, Belgique, Danemark, Lettonie, Lituanie, Luxembourg, Hongrie, Autriche et Roumanie (situation au 11 mars 2019).

62 Bulgarie, Chypre, République tchèque, Allemagne, Danemark, Estonie, Espagne, Finlande, France, Croatie, Hongrie, Irlande, Italie, Lituanie, Malte, Pays-Bas, Pologne, Portugal, Slovaquie, Suède et Royaume-Uni (situation au 11 mars 2019).

63 Directive (UE) 2015/849 du 20.5.2015.

64 La Commission a lancé des procédures d'infraction à l'encontre de tous les États membres pour défaut de communication de la législation nationale destinée à transposer intégralement la directive, son évaluation lui permettant de conclure que certaines dispositions de la directive n'ont pas été transposées.

65 L'Espagne, les Pays-Bas et la Finlande doivent encore notifier les mesures de transposition. La République tchèque et la Slovénie ont communiqué une transposition partielle et doivent encore achever la notification des mesures de transposition (situation au 11 mars 2019). Les mentions des notifications 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.

66 La Belgique et le Luxembourg doivent encore notifier les mesures de transposition. La Hongrie a communiqué une transposition partielle et doit encore achever la notification des mesures de transposition (situation au 11 mars 2019).

- la **directive relative au contrôle de l'acquisition et de la détention d'armes**, dont 17 États membres doivent encore notifier la transposition en droit national et 5 États membres doivent achever la notification des mesures de transposition[68];
- la **directive en matière de protection des données dans le domaine répressif**, dont 5 États membres doivent encore notifier la transposition en droit national et 5 États membres doivent achever la notification des mesures de transposition[69]; et
- la **4e directive anti-blanchiment**, dont 1 État membre doit encore achever la notification des mesures de transposition[70].

*2. Protection des espaces publics: meilleures pratiques recommandées*

Pour ce qui est des mesures sur le terrain visant à améliorer la protection et la résilience face au terrorisme, la Commission continue de soutenir les États membres et leurs autorités locales en vue de **protéger les espaces publics.** En exécution du plan d'action d'octobre 2017 en faveur de la protection des espaces publics[71], les efforts se concentrent sur la mise au point et la collecte d'orientations et de meilleures pratiques. En collaboration avec les pouvoirs publics et les exploitants privés d'espaces publics, dans le cadre du Forum des exploitants d'espaces publics[72], la Commission a recensé les meilleures pratiques concernant plusieurs mesures que tous les exploitants et pouvoirs publics actifs dans la protection des espaces publics peuvent mettre en œuvre pour renforcer la sécurité[73]. Elles énoncent les étapes essentielles pour orienter les travaux futurs dans tous les secteurs pertinents pour la protection des espaces publics (voir encadré ci-dessous).

---

67 La Grèce, Chypre et le Luxembourg doivent encore notifier les mesures de transposition. La Belgique, la Pologne, la Roumanie et la Slovénie ont communiqué une transposition partielle et doivent encore achever la notification des mesures de transposition (situation au 11 mars 2019).

68 La Belgique, la Bulgarie, l'Allemagne, l'Irlande, la Grèce, l'Espagne, Chypre, la Lettonie, le Luxembourg, la Hongrie, les Pays-Bas, la Pologne, la Roumanie, la Slovénie, la Slovaquie, la Finlande et la Suède doivent encore notifier les mesures de transposition. La République tchèque, l'Estonie, la Lituanie, le Portugal et le Royaume-Uni ont communiqué une transposition partielle et doivent encore achever la notification des mesures de transposition (situation au 11 mars 2019). 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.

69 La Bulgarie, la Grèce, l'Espagne, Chypre et la Lettonie doivent encore notifier les mesures de transposition. La République tchèque, le Portugal, les Pays-Bas, la Finlande et la Slovénie ont communiqué une transposition partielle et doivent encore achever la notification des mesures de transposition (situation au 11 mars 2019).

70 La Roumanie n'a communiqué à ce jour qu'une transposition partielle et n'a pas encore achevé la notification des mesures de transposition. Tous les autres États membres ont notifié une transposition complète. Or, selon l'évaluation de la Commission, toutes les dispositions de la directive ne semblent pas encore avoir été pleinement transposées (situation au 11 mars 2019).

71 COM(2017) 612 final du 18.10.2017.

72 Le forum des exploitants privés d'espaces publics, créé dans le cadre du plan d'action d'octobre 2017 pour soutenir la protection des espaces publics, réunit les responsables politiques des États membres et les opérateurs de différents secteurs, les événements de masse et le divertissement, l'hébergement, les centres commerciaux, les complexes culturels et sportifs, les plateformes de transport et autres.

73 Pour de plus amples informations sur les meilleures pratiques, voir le document de travail des services de la Commission intitulé «Meilleures pratiques pour soutenir la protection des espaces publics» [SWD (2019) 140 du 20.3.2019].

**Meilleures pratiques à l'usage des autorités publiques et des opérateurs privés en vue de renforcer la sécurité des espaces publics**

***Évaluation et planification***

- Élaborer et entreprendre des évaluations de la vulnérabilité afin de recenser les vulnérabilités potentielles face aux attaques de tiers ou d'initiés;
- élaborer et mettre en œuvre un plan de sécurité concernant les installations ou les événements, y compris des mesures préparatoires, d'urgence et de remise en état, et recenser les mesures de sécurité appropriées pour protéger l'environnement de l'établissement ou de l'événement en question. Les mesures de sécurité doivent être effectives, discrètes, proportionnées et adaptées à différents environnements, mais aussi tenir compte du fonctionnement spécifique de ces derniers;
- désigner et former une personne chargée de la coordination et de la mise en œuvre des mesures de sécurité contenues dans le plan de sécurité; et
- élaborer et mettre en œuvre un plan de gestion de crise.

***Sensibilisation et formation***

- Lancer des campagnes visant à sensibiliser le public à la nécessité de signaler les comportements suspects et l'informer sur la conduite à tenir en cas d'attaque compromettant la sécurité d'une installation ou d'un événement;
- élaborer et mettre en œuvre un programme interne de sensibilisation à la sécurité à l'intention de tous les employés;
- élaborer et mettre en œuvre un programme de sensibilisation aux menaces intérieures qui contribuera à protéger les installations ou les événements contre différents types de menaces internes, telles que le sabotage, le vol commercial ou les attentats terroristes;
- élaborer des programmes de formation de base à la sécurité pour l'ensemble du personnel et dispenser des formations spécifiques en matière de sécurité, contribuant ainsi au développement d'une culture de la sécurité d'entreprise. Mettre au point des activités incitant les employés à mettre en œuvre des pratiques de sécurité saines et à maintenir un niveau élevé de vigilance en matière de sécurité; et
- entreprendre régulièrement des exercices de sécurité permettant d'évaluer le niveau de préparation à la dissuasion et à la réaction à une attaque.

***Protection physique***

- Évaluer les aspects liés à la sécurité et à la protection physique dès les premières étapes de la conception d'une nouvelle installation ou d'un nouvel événement;
- déterminer les contrôles et les barrières d'accès nécessaires, tout en évitant de créer de nouvelles vulnérabilités. Les contrôles et les barrières d'accès ne doivent pas déplacer les risques ni créer de nouvelles cibles;
- déterminer la technologie de détection la plus appropriée pour les explosifs, les armes à feu, les armes blanches, ainsi que les agents chimiques, biologiques, radiologiques et nucléaires.

***Coopération***

- Désigner des points de contact et clarifier les rôles et responsabilités respectifs dans le cadre de la coopération entre les secteurs public et privé dans le domaine de la sécurité (par exemple entre opérateurs, services de sécurité privés et services répressifs) et améliorer la communication et la coopération régulières;
- instaurer une communication et une coopération fiables et en temps utile en ce qui concerne les risques et les menaces, en vue d'un échange d'informations entre autorités publiques responsables, services répressifs locaux et secteur privé;

- coordonner les travaux relatifs à la protection des espaces publics aux niveaux local, régional et national et entreprendre une communication et des échanges de meilleures pratiques à tous les niveaux, y compris au niveau de l'UE; et
- les autorités publiques, en collaboration avec les exploitants, devraient élaborer et proposer des recommandations pratiques et des documents d'orientation aux fins de la détection, de l'atténuation ou de la réaction aux menaces pesant sur la sécurité.

*3. Vulnérabilités des infrastructures numériques*

La résilience numérique est essentielle pour protéger au sens large les activités de nos gouvernements, la recherche industrielle, la propriété intellectuelle, les plans d'entreprise, nos élections, nos institutions démocratiques ainsi que nos propres données à caractère personnel. L'une des principales questions liées à la cybersécurité qui est au centre du débat public dans l'UE concerne les réseaux de 5e génération (5G). Lors du récent Conseil ministériel informel sur les télécommunications qui a eu lieu à Bucarest le 1er mars 2019, les ministres se sont montrés favorables à une approche européenne coordonnée pour renforcer la résilience numérique dans l'UE en lien avec les réseaux 5G. L'infrastructure des réseaux 5G constitue une base importante pour l'économie numérique. Au-delà des services aux consommateurs, la technologie 5G est conçue en vue de fournir des services essentiels aux secteurs verticaux, tels que la mobilité, l'énergie et la santé. Les normes applicables aux réseaux 5G étant mondiales, les équipements et les dispositifs seront proposés par un certain nombre de fournisseurs mondiaux.

Le déploiement des réseaux 5G ces prochaines années signe un changement radical par rapport aux réseaux antérieurs. Le stockage de données dans le nuage permettra la connexion de milliards de dispositifs de l'internet des objets et stimulera de nouvelles innovations dans la sphère de l'intelligence artificielle, ouvrant de nouveaux débouchés aux citoyens et aux entreprises. Par conséquent, la cybersécurité acquiert d'autant plus d'importance que le risque d'une exploitation des vulnérabilités est susceptible d'entraîner des dommages considérables. Les frontières n'existant pas pour l'internet, une faille de la sécurité dans un État membre pourrait se répercuter sur de nombreux autres États membres.

La prévention d'éventuelles conséquences graves en matière de sécurité pour les infrastructures numériques critiques passe donc par une approche commune de l'UE en ce qui concerne la sécurité des réseaux 5G. Dans cet ordre d'idées, la Commission publiera, à l'issue du Conseil européen des 21 et 22 mars 2019, une recommandation relative à une approche commune de l'UE en matière de risques pour la sécurité des réseaux 5G, fondée sur une évaluation coordonnée des risques au niveau de l'UE et des mesures de gestion des risques, sur un cadre efficace de coopération et d'échange d'informations ainsi que sur une appréciation commune de la situation au niveau de l'UE couvrant les réseaux de communication critiques. Parmi les mesures potentielles examinées, il conviendrait d'inclure le déploiement des technologies quantiques pour la sécurité des réseaux ainsi que pour la protection des données stockées[74].

[74] Voir également la communication intitulée «Initiative européenne sur l'informatique en nuage - Bâtir une économie compétitive des données et de la connaissance en Europe» [COM(2016) 178 final du 19.4.2016].

Le 12 mars 2019, le Parlement européen a adopté une résolution sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et les actions possibles à l'échelle de l'UE pour les réduire.

*4. À l'extérieur*

Les négociations menées par l'UE et le Canada relatives à un **accord révisé sur les données des dossiers passagers progressent de manière satisfaisante. Le prochain sommet entre l'UE et le Canada qui se tiendra à Montréal les 11 et 12 avril 2019 pourrait créer une dynamique positive pour les négociations.**

La Commission collabore avec les autorités américaines à la préparation de la prochaine évaluation conjointe de **l'accord entre l'UE et les États-Unis sur les données des dossiers passagers**[75], conformément aux dispositions de l'accord entre l'UE et les États-Unis sur les données des dossiers passagers. Des travaux sont déjà en cours dans le cadre du cinquième examen conjoint de **l'accord entre l'Union européenne et les États-Unis sur le programme de surveillance du financement du terrorisme**[76]. Cet examen conjoint, qui portera sur les dispositions de l'accord relatives aux garanties, aux contrôles et à la réciprocité, permettra également d'évaluer la valeur du programme en tant qu'instrument de lutte contre le terrorisme tant pour l'UE que pour les États-Unis.

Les évènements actuels sur le terrain en Syrie ont placé au centre des débats la question des **combattants terroristes étrangers** actuellement présents ou détenus dans des zones de conflit. L'Union est en mesure d'aider les États membres qui en font la demande, en ce qui concerne notamment l'échange d'informations et l'assistance dans les enquêtes pénales, et en particulier la coopération avec les partenaires internationaux et avec l'aide d'Europol, ainsi qu'en tirant parti de l'expertise et des meilleures pratiques en matière de réhabilitation et de réintégration mises au point dans le contexte du réseau de sensibilisation à la radicalisation. Elle peut également soutenir le renforcement des capacités des pays tiers particulièrement touchés par le phénomène du retour des combattants terroristes étrangers. C'est aux États membres concernés qu'il appartient de se prononcer en ce qui concerne le rapatriement des combattants terroristes étrangers et de leurs familles des zones de conflits.

L'UE et l'Égypte ont coprésidé la réunion plénière du groupe de travail du **Forum mondial de lutte contre le terrorisme** sur le renforcement des capacités en Afrique de l'Est, qui s'est tenue à Nairobi le 20 février 2019, avec un taux élevé de participation des services de la justice et de la police somaliens, kenyans, soudanais, ougandais, djiboutiens, éthiopiens, yéménites et tanzaniens.

## V. CONCLUSION

L'Union a accompli des progrès considérables dans le cadre des efforts conjoints en faveur d'une union de la sécurité réelle et effective, un certain nombre de ses initiatives législatives prioritaires ayant été adoptées par le Parlement européen et le Conseil au cours des derniers mois et semaines. Toutefois, il y a lieu, afin de répondre à des exigences prioritaires en matière de sécurité, de redoubler d'efforts avant les élections du Parlement européen en mai 2019. La Commission invite notamment les colégislateurs à engager des négociations sur les règles proposées pour la suppression des contenus à caractère terroriste en ligne, dès que le

[75] JO L 215 du 11.8.2012, p. 5.
[76] JO L 195 du 27.7.2010, p. 5.

Parlement européen aura adopté son mandat de négociation, afin qu'un accord puisse encore être dégagé au cours du présent mandat du Parlement européen. En ce qui concerne la proposition visant à renforcer le corps européen de garde-frontières et de garde-côtes, les négociations en sont déjà au stade du trilogue, ce qui témoigne de la détermination de l'ensemble des institutions à l'adopter avant les élections du Parlement européen. La Commission invite également les États membres à mettre en œuvre toutes les mesures approuvées dans le cadre de l'union de la sécurité afin de garantir qu'elles produisent pleinement leurs effets en ce qui concerne la sécurité de tous les citoyens.

En outre, étant donné que le temps presse pour préparer suffisamment l'Union avant que les électeurs européens ne se rendent aux urnes en mai 2019, la Commission invite tous les acteurs concernés à redoubler d'efforts pour renforcer la résilience du processus électoral en luttant contre la désinformation. Dans la perspective du Conseil européen des 21 et 22 mars 2019, il est nécessaire que les États membres intensifient leur coordination et leurs échanges d'informations afin de lutter contre la désinformation et de protéger les élections contre d'autres menaces liées au cyberespace, en tirant pleinement parti des instruments dont dispose l'UE à cet effet. Parallèlement, il appartient aux plateformes en ligne d'accélérer leurs efforts, et ce dans l'ensemble des États membres, en vue d'assurer l'intégrité des élections du Parlement européen en mai 2019. La Commission continuera de soutenir et d'encourager ces efforts dans les semaines et les mois à venir afin de protéger l'intégrité des élections du Parlement européen.