COMMISSION
EUROPÉENNE

Bruxelles, le 18.10.2017
COM(2017) 608 final

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

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

I. INTRODUCTION

Le présent rapport est le onzième rapport mensuel sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective; il fait état de l'évolution de la situation en ce qui concerne deux piliers principaux: d'une part, lutter contre le terrorisme et la criminalité organisée et contre les moyens sur lesquels ils s'appuient, et, d'autre part, renforcer nos défenses et notre résilience face à ces menaces.

Le président Juncker a souligné dans son discours sur l'État de l'Union[1] que l'Union européenne devait être plus forte en matière de lutte contre le terrorisme, en s'appuyant sur les progrès réels accomplis ces trois dernières années. Comme annoncé dans la lettre d'intention[2] adressée au Parlement européen et à la présidence du Conseil et dans la feuille de route pour une Europe plus unie, plus forte et plus démocratique, qui l'accompagnait, la Commission expose, dans le présent rapport, un **train de mesures en matière de lutte contre le terrorisme** à prendre au cours des seize prochains mois. Ces mesures opérationnelles aideront les États membres à remédier aux vulnérabilités importantes mises en évidence par les récents attentats terroristes et permettront de faire une réelle différence en ce qui concerne le renforcement de la sécurité. Cette initiative viendra compléter une union de la sécurité dans laquelle les terroristes ne puissent plus exploiter les failles pour commettre leurs atrocités. Au-delà de ces mesures pratiques à court terme, la Commission étudie actuellement la possibilité de créer une cellule européenne de renseignement, comme annoncé par le président Juncker dans le cadre de sa vision de l'Union européenne à l'horizon 2025.

Ce train de mesures en matière de lutte contre le terrorisme comprend:

- des mesures destinées à aider les États membres à **protéger les espaces publics** (chapitre II), notamment un plan d'action visant à améliorer la protection des espaces publics et un plan d'action visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire;
- des mesures destinées à **couper l'accès aux moyens utilisés par les terroristes** pour préparer et commettre des attentats, tels que des **substances dangereuses** ou des **sources de financement** (chapitre III), notamment une recommandation concernant les mesures à prendre immédiatement pour prévenir l'utilisation détournée des précurseurs d'explosifs, ainsi que des mesures destinées à aider les services répressifs et les autorités judiciaires lorsqu'ils sont confrontés à l'**utilisation du chiffrement** dans le cadre des enquêtes pénales;
- les prochaines mesures destinées à **lutter contre la radicalisation** (chapitre IV);
- les prochaines mesures destinées à renforcer la **dimension extérieure** de la lutte contre le terrorisme (chapitre V), notamment des propositions de décisions du Conseil relatives à la conclusion, au nom de l'UE, de la convention du Conseil de l'Europe pour la prévention du terrorisme et du protocole additionnel à cette convention, ainsi qu'une recommandation du Conseil visant à autoriser l'ouverture des négociations avec le Canada en vue de la révision de l'accord sur les dossiers passagers (PNR).

---

1 http://europa.eu/rapid/press-release_SPEECH-17-3165_fr.htm.
2 https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_fr.pdf.

II. MESURES DESTINÉES À AMÉLIORER LA PROTECTION ET LA RÉSILIENCE CONTRE LE TERRORISME

1. Protection accrue des espaces publics

Dans leur propagande et dans le choix de leurs cibles, les terroristes privilégient de plus en plus les espaces publics tels que les zones piétonnes, les sites touristiques, les nœuds de communication, les centres commerciaux, les salles de concert et les places publiques, comme l'ont montré les attentats perpétrés, par exemple, à Barcelone, Berlin, Bruxelles, Londres, Manchester, Nice, Paris et Stockholm. Ce que toutes ces «cibles faciles» (ou «soft targets») ont en commun est leur nature ouverte et leur caractère public, ainsi qu'une forte concentration de personnes, ce qui les rend intrinsèquement vulnérables.

Nous pouvons faire davantage pour réduire la vulnérabilité de ces lieux, détecter les menaces plus précocement et accroître notre résilience. C'est la raison pour laquelle la Commission, sur la base d'un **plan d'action visant à améliorer la protection des espaces publics**[3], soumis parallèlement au présent rapport, définit des mesures destinées à soutenir les États membres, aux niveaux national, régional et local, dans leurs efforts de renforcement de la protection physique contre les menaces terroristes. Bien que le «risque zéro» n'existe pas, ce plan d'action vise à aider les États membres à détecter les risques, à réduire la vulnérabilité des espaces publics, à atténuer les conséquences d'un attentat terroriste et à améliorer la coopération.

Le soutien que l'UE peut apporter à la protection des espaces publics est double. Premièrement, elle peut favoriser l'**échange des meilleures pratiques par-delà les frontières, y compris au moyen de financements**. Il peut s'agir, par exemple, de mesures destinées à promouvoir et à soutenir la mise au point de barrières de protection innovantes et discrètes afin d'assurer la sécurité des villes sans porter atteinte à leur caractère ouvert («protection dès la conception»). Apportant son concours financier aux mesures prévues dans le plan d'action, la Commission a lancé aujourd'hui un appel à propositions pour un montant total de 18,5 millions d'EUR au titre du volet «police» du Fonds pour la sécurité intérieure. Ce financement à court terme sera complété, en 2018, par un financement au titre des «Actions innovatrices urbaines» (AIU) dans le cadre du Fonds européen de développement régional, pour lesquelles la sécurité constituera un thème clé et l'enveloppe totale pourra atteindre 100 millions d'EUR. Une consultation publique a été lancée le 15 septembre 2017 afin de recueillir auprès des villes des idées en matière de solutions de sécurité innovantes. Cette consultation permettra à la Commission d'élaborer les futurs appels à propositions dans ce domaine.

Deuxièmement, l'Union européenne peut favoriser la **coopération avec un large éventail de parties prenantes**, laquelle est considérée comme capitale pour améliorer la protection des espaces publics. Il conviendrait de mieux structurer le partage d'expériences et la mise en commun des ressources. La Commission créera un forum afin de dialoguer avec des opérateurs privés, tels que des centres commerciaux, des organisateurs de concerts, des installations sportives, des hôtels et des sociétés de location de voitures. Ce dialogue facilitera une prise de conscience commune des défis actuels en matière de sécurité et favorisera les partenariats public-privé destinés à améliorer la protection. Les autorités locales et régionales

[3] COM(2017) 612 final du 18.10.2017.

ont également un rôle fondamental à jouer dans la protection des espaces publics et doivent être associées aux activités connexes menées au niveau de l'UE. La Commission renforcera la participation de ces parties prenantes et entamera un dialogue avec les autorités régionales et locales, telles que les maires de grandes villes, en vue de partager des informations et les meilleures pratiques en matière de protection des espaces publics. Dans le cadre du suivi de la déclaration de Nice[4] du 29 septembre 2017, au début de l'année prochaine, la Commission organisera, en collaboration avec le Comité des régions, une réunion à haut niveau avec les maires signataires de cette déclaration et d'autres représentants intéressés des niveaux local et régional en vue de poursuivre l'échange des meilleures pratiques relatives à la protection des espaces publics.

La Commission poursuivra également ses travaux concernant la protection et la résilience des **infrastructures critiques**. L'évaluation globale de la politique de sécurité de l'UE[5] a également mis en évidence la nécessité d'adapter le programme européen de protection des infrastructures critiques[6] aux nouvelles menaces. La Commission a lancé une évaluation de la directive[7] concernant le recensement et la désignation des infrastructures critiques européennes. Cette évaluation tiendra compte des enseignements tirés de l'expérience acquise et de l'évolution de la situation au cours des dernières années, telles que l'adoption de la directive sur la sécurité des réseaux et de l'information[8]. Dans l'intervalle, le programme européen de protection des infrastructures critiques a été renforcé de manière à prendre en compte les nouveaux défis, tels que les menaces internes et les menaces hybrides, et à élargir son volet externe grâce à une coopération avec les pays du voisinage oriental et les pays voisins des Balkans occidentaux.

Les transports sont, depuis de nombreuses années, à la fois la cible d'actes terroristes et un moyen de perpétrer des attentats (par exemple, détournement d'avions ou camions-béliers). En réponse, il est nécessaire d'évaluer la mesure dans laquelle les règles de **sécurité des transports** garantissent effectivement la sécurité, tout en assurant la fluidité des réseaux de transport. Alors que le secteur de l'aviation est considérablement mieux protégé, les attentats terroristes sont devenus plus opportunistes en visant davantage les espaces publics. Parmi ceux-ci, le **transport ferroviaire** est une cible à haut risque puisque son infrastructure est, par nature, ouverte. Il n'existe actuellement pas de cadre législatif de l'Union destiné à protéger le transport ferroviaire de voyageurs contre le terrorisme et les formes graves de criminalité. Le

---

4 La déclaration de Nice a été adoptée lors d'une conférence des maires de la région euro-méditerranéenne à Nice le 29 septembre 2017, organisée à l'initiative du maire de la ville de Nice, et avec la participation de la Commission, afin d'échanger entre les villes, les niveaux local et régional les meilleures pratiques en matière de prévention de la radicalisation et de protection des espaces publics: http://www.nice.fr/uploads/media/default/0001/15/ https://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf.

5 Voir le neuvième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 407 final du 26.7.2017] et le document de travail des services de la Commission joint en annexe [SWD(2017) 278 final].

6 Le programme européen de protection des infrastructures critiques (EPCIP) fixe le cadre des actions de l'UE visant à améliorer la protection des infrastructures critiques en Europe – dans tous les États membres et dans tous les secteurs d'activité économique pertinents. L'un des fondements essentiels de ces actions est la directive de 2008 concernant les infrastructures critiques européennes (directive 2008/114/CE du 8.12.2008).

7 Directive (UE) 114/680 du 8.12.2008.

8 Directive (UE) 2016/1148 du 6.7.2016.

15 juin 2017, la Commission a lancé, avec les États membres, une évaluation des risques communs dans le transport ferroviaire et elle travaille actuellement à l'élaboration de nouvelles mesures visant à améliorer la sécurité du transport ferroviaire de voyageurs. La Commission travaille à l'élaboration d'une boîte à outils d'orientations relatives aux meilleures pratiques en matière de sécurité pour le secteur du **transport** commercial **par route**, l'objectif étant d'améliorer la sécurité des poids lourds en atténuant le risque d'intrusion non autorisée, y compris de détournement ou de vol, dans le but de commettre un attentat terroriste au camion-bélier. La boîte à outils sera disponible avant la fin de l'année 2017 et fournira des orientations pour les secteurs des transports routiers nationaux. La Commission poursuivra également ses travaux sur l'amélioration de la **sûreté des transports maritimes**, notamment en vue de renforcer la protection des infrastructures, y compris les ports et les installations portuaires, des navires porte-conteneurs et des navires de transport de passagers tels que les bateaux de croisière et les ferries.

2. Une meilleure préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire

Bien que le risque d'attentats utilisant des substances chimiques, biologiques, radiologiques et nucléaires (CBRN) reste faible dans l'UE, le niveau général de la menace CBRN évolue. Il y a en effet des raisons de penser que certains groupes criminels ou terroristes pourraient avoir l'intention de se procurer des matières CBRN ainsi que les connaissances et les moyens nécessaires pour les utiliser à des fins terroristes. Le potentiel des attentats CBRN figure en bonne place dans la propagande terroriste. L'évaluation exhaustive de la politique de sécurité de l'UE[9] a mis en évidence la nécessité d'intensifier la préparation à ces menaces.

Afin d'être mieux préparé à faire face aux menaces CBRN au cours des prochaines années, la Commission soumet, avec le présent rapport, un **plan d'action visant à améliorer la préparation aux risques en matière de sécurité chimique, biologique, radiologique et nucléaire[10]**. Ce plan prévoit un large éventail de mesures visant à améliorer la préparation, la résilience et la coordination au niveau de l'UE, par exemple par la création d'un réseau de l'UE pour la sécurité CBRN afin de regrouper l'ensemble des acteurs du secteur. Ce réseau bénéficiera notamment du soutien d'un pôle de connaissances CBRN qui relèvera du Centre européen de la lutte contre le terrorisme (ECTC) au sein d'Europol. Comme il importe également de mieux exploiter les ressources disponibles, le plan d'action propose de renforcer la préparation et la réaction dans le domaine CBRN par des formations et des exercices associant l'ensemble des différents premiers intervenants (services répressifs, protection civile et santé) et, selon le cas, des partenaires militaires et privés. Il s'appuiera également sur les instruments existants au niveau de l'UE, notamment le mécanisme de protection civile de l'Union (MPCU)[11] et l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL). Afin d'être en mesure de mieux réagir en cas d'incident CBRN majeur, les États membres devraient continuer à renforcer l'actuelle capacité européenne de réaction d'urgence (EERC) du MPCU. Dans ce contexte, les États membres sont invités à continuer d'engager de nouveaux moyens dans l'EERC.

---

[9] Voir le neuvième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 407 final du 26.7.2017] et le document de travail des services de la Commission joint en annexe [SWD(2017) 278 final].

[10] COM(2017) 610 final du 18.10.2017.

[11] Décision 1313/2013 du 17.12.2013.

La législation de l'UE relative aux **menaces transfrontières graves pour la santé**[12] prévoit la préparation, la surveillance et la coordination des réponses aux urgences sanitaires dans l'ensemble de l'UE. Dans ce contexte, le système d'alerte précoce et de réaction de l'UE sera mieux relié aux autres systèmes d'alerte de l'UE concernant les menaces biologiques, chimiques, environnementales et encore inconnues. Le programme de santé permet également de financer des exercices à l'échelle de l'UE sur la préparation et la réaction aux urgences, ainsi que des actions communes destinées à aider les États membres à renforcer les laboratoires, la vaccination et les principales capacités en application du règlement sanitaire international.

Toutes ces initiatives seront soutenues par des activités de recherche spécifiques, des financements et une coopération avec les partenaires internationaux pertinents.

III. S'ATTAQUER AUX MOYENS D'ACTION DES TERRORISTES

1. Financement du terrorisme: accès transfrontière aux informations financières

Les informations sur les activités financières de terroristes présumés peuvent fournir des pistes cruciales dans le cadre des enquêtes antiterroristes. En raison de leur fiabilité et de leur précision, les données financières (y compris les données relatives aux transactions financières) peuvent permettre d'identifier des terroristes, de découvrir des liens avec des complices, d'établir les activités, les moyens logistiques et les déplacements des suspects, et de cartographier les réseaux terroristes. L'obtention rapide d'un aperçu des activités financières de suspects et de leurs complices peut fournir aux services répressifs des informations capitales pour empêcher des attentats ou réagir à la suite d'un attentat. Le phénomène croissant des attentats de moindre ampleur perpétrés à l'aide de moyens rudimentaires pose de nouveaux défis; les projets d'attentats peuvent être plus difficiles à déceler lorsque ceux-ci sont planifiés à court terme. Les transactions financières liées à des projets d'attentats de moindre ampleur ont plus de chances de passer inaperçues, de sorte que ces informations ne sont portées à l'attention des autorités compétentes qu'après les attentats.

Comme annoncé dans le plan d'action de 2016 destiné à renforcer la lutte contre le financement du terrorisme[13], la **Commission analyse actuellement la nécessité de prendre des mesures supplémentaires** pour faciliter l'accès aux informations financières détenues dans d'autres juridictions au sein de l'UE à des fins d'enquêtes antiterroristes. Dans le troisième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, de décembre 2016[14], la Commission exposait son analyse initiale et indiquait qu'elle poursuivrait son évaluation, compte tenu notamment des incidences possibles sur les droits fondamentaux, et en particulier le droit à la protection des données à caractère personnel. Depuis lors, la Commission a consulté les parties prenantes et analysé les mécanismes par lesquels les autorités compétentes peuvent actuellement accéder aux informations pertinentes, notamment des données financières stockées dans d'autres États membres; les obstacles qui les empêchent de le faire rapidement et efficacement; et les mesures qui permettraient de remédier à ces obstacles.

---

12 Décision 1082/2013/UE du 22.10.2013.
13 COM(2016) 50 final du 2.2.2016;
14 COM(2016) 831 final du 21.12.2016;

Outre l'évaluation en cours, la Commission continue à promouvoir l'**échange des meilleures pratiques** concernant les techniques d'enquête et l'analyse des modes de levée et de transfert de fonds utilisés par les terroristes, notamment en apportant son concours financier sur la base d'un appel à propositions d'un montant de 2,5 millions d'EUR lancé aujourd'hui.

Dans ce contexte, la Commission étudie également la manière d'**améliorer la coopération entre les cellules de renseignement financier**[15] mises en place afin de prévenir, de détecter et de combattre efficacement le blanchiment de capitaux et le financement du terrorisme. Un rapport de décembre 2016 établi par les cellules de renseignement financier ainsi que le document de travail connexe des services de la Commission sur l'amélioration de la coopération entre ces cellules[16] mettent en évidence un certain nombre de limites dans les compétences nationales des cellules de renseignement financier et définissent la voie à suivre pour y remédier au moyen des actions suivantes: (i) la mise en œuvre de la 4e directive anti-blanchiment[17] et les modifications qu'il est proposé d'y apporter[18], qui sont actuellement en cours de négociation; (ii) les autres initiatives menées par la plateforme des cellules de renseignement financier de l'UE afin de renforcer la coopération opérationnelle, en particulier au moyen d'orientations, de travaux de normalisation et de solutions entrepreneuriales à mettre en œuvre dans le cadre du CRF.NET; et (iii) les mesures réglementaires visant à s'attaquer aux autres problèmes découlant des différences de statut et de compétences des cellules de renseignement financier, notamment afin de faciliter la coordination et l'échange d'informations entre ces cellules, et entre elles et les services répressifs.

Des travaux sont également en cours pour faciliter l'**accès aux données financières au sein d'un État membre**. Les modifications qu'il est proposé d'apporter à la **4e directive anti-blanchiment**[19], qui sont actuellement en cours de négociation avec les colégislateurs, donneraient lieu à la création de registres centraux des comptes bancaires ou de systèmes centraux de recherche de données dans tous les États membres, accessibles aux cellules de renseignement financier et aux autres autorités compétentes chargées de lutter contre le blanchiment de capitaux et le financement du terrorisme. Ces registres, une fois établis dans tous les États membres, faciliteront l'obtention des données relatives aux comptes bancaires. Sur cette base, la Commission prépare une initiative visant à **élargir l'accès des services répressifs à ces registres des comptes bancaires**[20] afin de renforcer la capacité de ces services à découvrir l'existence d'un compte bancaire plus rapidement.

Dans le cadre de la consultation des parties prenantes, ces dernières ont également signalé les **obstacles à l'obtention des données relatives aux transactions financières détenues dans d'autres États membres**. Au besoin, les informations relatives aux comptes bancaires

---

15 Les cellules de renseignement financier ont été créées par la décision 2000/642/JAI du Conseil du 17 octobre 2000 et sont en outre régies par la directive (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme. Ce sont des cellules indépendantes et autonomes sur le plan opérationnel, chargées de recevoir et d'analyser les déclarations de transactions suspectes ainsi que d'autres informations ayant trait au blanchiment de capitaux, aux infractions sous-jacentes associées ou au financement du terrorisme provenant d'entités pertinentes, et de communiquer aux autorités compétentes les conclusions de leur analyse ainsi que toute autre information utile.

16 SWD(2017) 275 final du 26.6.2017.

17 Directive (UE) 2015/849 du 20.5.2015.

18 COM(2016) 450 final du 5.7.2016.

19 COM(2016) 450 final du 5.7.2016.

20 http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182.

peuvent être échangées entre les États membres par les canaux de la coopération policière dans un délai de huit heures[21]. L'accès aux données relatives aux transactions financières détenues par d'autres États membres peut également être facilité par les cellules de renseignement financier. Lorsque ces informations doivent servir de preuves dans une procédure pénale, il peut être nécessaire de les demander dans le cadre de l'entraide judiciaire. La décision d'enquête européenne[22] offre de nouvelles possibilités d'obtenir des données sur des transactions financières d'une manière beaucoup plus rapide que dans le cadre de l'entraide judiciaire. À ce jour, quelques mois après le délai de transposition, seuls 16 États membres ont transposé la décision d'enquête européenne et les autres États membres sont invités à le faire sans plus attendre. Enfin, les propositions législatives à venir sur l'utilisation des preuves électroniques, prévues pour le début de l'année 2018, permettront également de faciliter l'accès transfrontière à ces données.

Les parties prenantes ayant pris part à la consultation ont également attiré l'attention sur les **obstacles qui entravent l'obtention des données relatives aux transactions financières détenues dans d'autres États membres**. À titre de mesure pour lever ces obstacles et dans le cadre de son évaluation en cours, la Commission appréciera la nécessité, la faisabilité technique et la proportionnalité de l'interconnexion des registres centralisés des comptes bancaires, compte tenu de tous les instruments existants et prévus pour faciliter l'accès aux données sur les transactions financières détenues dans d'autres États membres.

À cette fin, la Commission **continuera de consulter toutes les parties prenantes** sur la nécessité, la faisabilité technique et la proportionnalité d'éventuelles mesures nouvelles au niveau de l'Union pour faciliter et accélérer l'accès transfrontière aux données sur les transactions financières, y compris les procédures permettant de garantir la confidentialité des informations. Sur la base de l'ensemble des évaluations en cours concernant l'utilisation des informations financières à des fins d'enquêtes antiterroristes, la Commission organisera une réunion à haut niveau avec les parties prenantes en novembre 2017. Les points essentiels qui seront abordés seront les suivants:

- les principaux obstacles à un accès effectif et en temps utile aux données sur les transactions financières détenues dans d'autres États membres à des fins d'enquêtes antiterroristes;
- la nécessité, la faisabilité technique et la proportionnalité d'éventuelles mesures supplémentaires pour faciliter l'accès transfrontière aux données sur les transactions financières à des fins d'enquêtes antiterroristes d'une manière rapide, efficace et sûre.

La Commission fera rapport sur le résultat de cette discussion.

[21] La décision-cadre 2006/960/JAI du Conseil (l'«initiative suédoise») prévoit que les autorités répressives répondent aux demandes étrangères dans les délais suivants: huit heures dans les cas urgents, lorsque les informations ou les renseignements demandés figurent dans une base de données à laquelle un service répressif peut avoir directement accès; et des délais les plus longs lorsque les informations ou les renseignements demandés ne figurent pas dans une base de données directement accessible.

[22] Directive (UE) 2014/41 du 3.4.2014.

2. *Explosifs: Restreindre davantage l'accès aux précurseurs d'explosifs*

Le **règlement sur les précurseurs d'explosifs**[23] limite l'accès du grand public à sept substances chimiques (les précurseurs d'explosifs faisant l'objet de restrictions qui sont énumérés à l'annexe I du règlement) ainsi que leur utilisation. En février 2017, la Commission a adopté un rapport sur l'application du règlement par les États membres[24]. Ce rapport concluait que la mise en œuvre du règlement avait contribué à réduire l'accès aux précurseurs d'explosifs dangereux susceptibles d'être utilisés pour fabriquer des explosifs de manière artisanale. Les États membres ont également signalé des exemples où l'application du règlement avait permis de découvrir précocement des complots terroristes[25]. Afin de garantir la pleine mise en œuvre du règlement, la Commission a engagé, en mai et en septembre 2016, des procédures d'infraction à l'encontre de plusieurs États membres pour défaut de mise en œuvre complète du règlement. En octobre 2017, seules deux procédures d'infraction sont toujours pendantes, respectivement à l'encontre de l'Espagne et de la Roumanie.

Malgré ces efforts conjoints, les incidents et attentats terroristes récents montrent que la **menace que représentent les explosifs de fabrication artisanale** demeure élevée en Europe. Ces substances restent accessibles et continuent d'être utilisées pour la fabrication artisanale d'explosifs. L'explosif utilisé dans la plupart des attentats était le triperoxyde de triacétone (TATP), soit l'explosif de fabrication artisanale qui est signalé comme étant l'explosif privilégié des terroristes[26].

Compte tenu de la menace que représentent actuellement les précurseurs d'explosifs, il est nécessaire de prendre des mesures immédiates pour faire en sorte que le règlement en vigueur soit mis en œuvre par tous les États membres de façon optimale. C'est pourquoi la Commission a publié, en même temps que le présent rapport, une **recommandation**[27] donnant des orientations sur les mesures à prendre sans délai pour prévenir toute utilisation détournée des précurseurs d'explosifs. La Commission encourage les États membres à mettre pleinement en œuvre cette recommandation afin de restreindre autant que possible l'accès des terroristes aux précurseurs d'explosifs et l'utilisation qu'ils peuvent en faire, et à veiller à améliorer les contrôles de la légitimité des utilisations ainsi que les mesures prises en cas de transactions suspectes. Elle est disposée à aider les États membres à cette fin.

En outre, la Commission est en train de renforcer son **réexamen** du **règlement sur les précurseurs d'explosifs** avec une évaluation qui sera suivie d'une analyse d'impact au cours du premier semestre de 2018. Cette évaluation portera sur la pertinence, l'efficacité, l'efficience, la cohérence et la valeur ajoutée du règlement, et recensera les problèmes et les obstacles qui pourraient exiger des mesures supplémentaires. L'analyse d'impact consistera, quant à elle, à examiner différentes options stratégiques en vue de remédier aux problèmes et aux obstacles recensés.

---

23 Règlement (UE) n° 98/2013 du 15.1.2013.

24 COM(2017) 103 final du 28.2.2017.

25 Le 23 juin 2017, le ministère belge de l'intérieur a annoncé qu'il avait reçu, en l'espace d'une année, 30 signalements de ventes suspectes. De février à juin 2017, la France a reçu 11 signalements concernant, pour la plupart, du peroxyde d'hydrogène.

26 Rapport 2017 sur la situation et les tendances du terrorisme en Europe (rapport TE-SAT): https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017.

27 C(2017) 6950 final du 18.10.2017.

3. Chiffrement: soutenir les services répressifs dans le cadre des enquêtes pénales

Le recours au chiffrement est essentiel pour assurer la cybersécurité et la protection des données à caractère personnel. La législation de l'UE souligne en particulier le rôle du chiffrement pour assurer le niveau de sécurité approprié au traitement des données à caractère personnel[28]. Dans le même temps, dans le cadre des enquêtes pénales, les services répressifs et les autorités judiciaires rencontrent de plus en plus de problèmes posés par l'utilisation du chiffrement par les criminels. Cette situation porte atteinte à la capacité des services répressifs et des autorités judiciaires d'obtenir les informations nécessaires en tant qu'éléments de preuve dans le cadre des enquêtes pénales, ainsi que de poursuivre et de condamner les auteurs d'infraction. Le recours au chiffrement par les criminels et, partant, son incidence sur les enquêtes pénales devraient continuer à s'accroître dans les années à venir.

Faisant suite à l'appel du Conseil Justice et affaires intérieures de décembre 2016, la Commission a **examiné le rôle du chiffrement dans le cadre des enquêtes pénales, avec les parties prenantes**, en s'intéressant à la fois aux aspects techniques et juridiques. Il s'agit d'experts d'Europol, d'Eurojust, du réseau judiciaire européen en matière de cybercriminalité (EJCN), de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), de l'Agence des droits fondamentaux de l'Union européenne (FRA) et des services répressifs des États membres, d'entreprises du secteur et d'organisations de la société civile. Il a été régulièrement rendu compte des progrès au niveau du groupe de travail du Conseil, et un atelier avec les États membres a eu lieu le 18 septembre 2017. Plusieurs tables rondes avec des entreprises du secteur et des organisations de la société civile ont été organisées tout au long du processus.

À la suite des discussions menées avec les États membres et les parties prenantes et sur la base de leurs observations, la Commission conclut qu'il conviendrait de mettre en œuvre l'ensemble suivant de **mesures d'appui aux services répressifs et aux autorités judiciaires** lorsqu'ils font face à l'utilisation du chiffrement par les criminels dans le cadre des enquêtes pénales. Il s'agit (a) de mesures juridiques visant à faciliter l'accès à des éléments de preuve chiffrés, ainsi que (b) de mesures techniques visant à renforcer les capacités de déchiffrement. La Commission continuera à suivre l'évolution à cet égard.

(a) Cadre juridique applicable à l'accès transfrontière aux preuves électroniques

Les services répressifs sont souvent confrontés au problème de l'accès aux éléments de preuve qui se trouvent dans un autre pays. L'évolution législative en cours au niveau européen peut contribuer à aider les services répressifs et les autorités judiciaires à obtenir l'accès aux informations nécessaires, mais éventuellement chiffrées, qui sont détenues dans un autre État membre. L'efficacité des enquêtes et des poursuites pénales dépend de l'existence d'un cadre approprié. À cette fin, la Commission présentera au début de l'année 2018 des propositions visant à faciliter l'**accès transfrontière aux preuves électroniques**. Dans le même temps, la Commission mettra en œuvre un ensemble de mesures concrètes[29] visant à faciliter l'accès transfrontière aux preuves électroniques dans les enquêtes pénales, notamment en finançant la formation en matière de coopération transfrontière, en élaborant une plateforme électronique

[28] Article 32 du règlement (UE) n° 2016/679 du 27.4.2017.

[29] Voir le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 354 final du 29.6.2017].

pour l'échange d'informations au sein de l'UE et en harmonisant les formes de coopération judiciaire entre les États membres.

(b) Mesures techniques

Selon le mode de chiffrement utilisé par les criminels, les services répressifs et les autorités judiciaires peuvent être en mesure de recouvrer une partie des informations. Plusieurs États membres ont mis en place des services nationaux disposant d'une expertise en ce qui concerne le problème que pose le chiffrement dans le cadre des enquêtes pénales. En revanche, la plupart des États membres n'ont pas accès au niveau approprié d'expertise et de ressources techniques. Cette situation limite considérablement la capacité des autorités répressives et judiciaires d'accéder à des informations chiffrées dans les enquêtes pénales. C'est pourquoi la Commission propose une **série de mesures destinées à soutenir les autorités nationales**, sans interdire, limiter ni affaiblir le chiffrement.

En premier lieu, la Commission aidera **Europol** à continuer à développer ses capacités de déchiffrement. Pour ce faire, elle a proposé, dans le cadre de la préparation du budget de l'UE pour l'exercice 2018, la création d'un total de 86 postes supplémentaires liés à la sécurité pour Europol (soit 19 de plus que dans le budget 2017), notamment afin de renforcer son Centre européen de lutte contre la cybercriminalité (EC3). La nécessité de ressources supplémentaires fera l'objet d'une évaluation, et la Commission rendra compte, dans son prochain rapport sur l'union de la sécurité, des fonds mis à disposition à cette fin. Il conviendrait de tenir compte des évolutions technologiques futures sur la base de la recherche et du développement dans le cadre du programme Horizon 2020 et des autres programmes financés par l'UE. Les mesures susceptibles d'affaiblir le chiffrement ou d'avoir une incidence sur un nombre élevé, voire inconsidéré, de personnes ne seraient pas prises en considération.

Deuxièmement, pour aider les services répressifs et les autorités judiciaires au niveau national, un **réseau de points d'expertise** devrait être mis en place. Sans se substituer aux initiatives nationales, les capacités et l'expertise au niveau national pourraient être mieux partagées. Les États membres sont encouragés à utiliser le financement au titre des programmes nationaux du Fonds pour la sécurité intérieure Police (FSI-P) pour créer, étendre ou développer les points d'expertise nationaux. Au niveau européen, la Commission apportera son appui à Europol en servant de pivot du réseau afin de faciliter la collaboration entre ces points d'expertise nationaux.

En troisième lieu, les autorités des États membres devraient disposer d'un **arsenal de techniques d'enquête alternatives** pour faciliter l'élaboration et l'application de mesures permettant d'obtenir les informations requises qui ont été chiffrées par les criminels. Le réseau de points d'expertise devrait contribuer à développer cet arsenal et le Centre européen de lutte contre la cybercriminalité (EC3), au sein d'Europol, est le mieux placé pour établir et tenir un registre de ces techniques et instruments. Les mesures susceptibles d'affaiblir le chiffrement ou d'avoir une incidence sur un nombre élevé, voire inconsidéré, de personnes ne seraient pas prises en considération.

Quatrièmement, une attention particulière devrait être accordée au **rôle important des fournisseurs de services et autres partenaires du secteur** pour apporter des solutions à chiffrement puissant. Compte tenu de l'engagement de la Commission en faveur d'un

chiffrement puissant, une collaboration plus étroite et plus structurée entre les autorités, les prestataires de services et d'autres partenaires du secteur permettrait de mieux appréhender la situation actuelle et l'évolution des différents problèmes. La Commission soutiendra les dialogues structurés avec les fournisseurs de services et les autres entreprises dans le cadre du forum de l'UE sur l'internet et du réseau de points d'expertise, en associant au besoin la société civile.

En cinquième lieu, les **programmes de formation** des services répressifs et des autorités judiciaires devraient mieux préparer les agents responsables à l'obtention des informations requises qui ont été chiffrées par les criminels. Afin de soutenir l'élaboration de programmes de formation, la Commission entend apporter un financement de 500 000 EUR au titre du programme de travail annuel 2018 du Fonds pour la sécurité intérieure Police. L'expertise du groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG) sera prise en compte, le cas échéant. La Commission soutiendra également la mise en place de formations dispensées par l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) et les États membres sont encouragés à utiliser, pour la formation, le financement disponible au titre de leurs programmes nationaux du Fonds pour la sécurité intérieure Police.

Sixièmement, il est nécessaire de procéder à une **évaluation continue des aspects techniques et juridiques** du rôle du chiffrement dans les enquêtes pénales, compte tenu de l'évolution constante des techniques de chiffrement, de leur utilisation accrue par les criminels et de l'incidence sur les enquêtes pénales. La Commission poursuivra ces travaux importants. Elle soutiendra également la mise en place d'une fonction d'observatoire en collaboration avec le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, le réseau judiciaire européen en matière de cybercriminalité (EJCN) et Eurojust.

IV. LUTTER CONTRE LA RADICALISATION

1. Groupe d'experts de haut niveau sur la radicalisation

Les récentes attaques, notamment celles perpétrées par des individus isolés, et la vitesse à laquelle certains de leurs auteurs se sont radicalisés, nous ont cruellement rappelé l'importance de la prévention de la radicalisation et de la lutte contre celle-ci. La Commission a institué un **Groupe d'experts de haut niveau sur la radicalisation** afin de renforcer les mesures de prévention de la radicalisation et de lutte contre celle-ci ainsi que pour améliorer la coordination et la coopération entre toutes les parties prenantes en tirant parti des avancées réalisées à ce jour[30]. Ce groupe, chargé d'émettre des recommandations en vue de mener plus avant les travaux dans ce domaine, achèvera un premier rapport intermédiaire cette année. En décembre 2017, la Commission fera un rapport sur les progrès accomplis au Conseil «Justice et affaires intérieures». Le groupe d'experts abordera également les conditions-cadres nécessaires pour renforcer les capacités et le savoir-faire en matière de lutte contre la radicalisation, compte tenu de la nécessité éventuelle d'élaborer de nouvelles structures de coopération au niveau de l'UE. À cet égard, certains États membres ayant appelé de leurs vœux un centre de prévention de la radicalisation de l'UE, le groupe évaluera la nécessité et la valeur ajoutée de la création d'une telle structure.

[30] Voir le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, [COM(2017) 354 final du 29.7.2017].

Parmi les questions prioritaires devant être discutées par ce groupe, figure **la radicalisation dans les prisons**. L'accent est placé actuellement sur la mise en œuvre, par les États membres, des conclusions du Conseil JAI du 20 novembre 2015 sur le renforcement de la réponse pénale à la radicalisation[31]. La Commission organisera une conférence des parties prenantes sur la réponse pénale à la radicalisation, le 27 février 2018, dans le but de partager les résultats des projets en cours.

La Commission tiendra compte des conclusions et des recommandations du groupe d'experts dans le plan de travail des initiatives existantes (notamment au sein du centre d'excellence du réseau de sensibilisation à la radicalisation), ainsi que pour l'utilisation et la finalité principale de ses instruments de financement (y compris le Fonds pour la sécurité intérieure, mais aussi d'autres fonds liés tels qu'Erasmus+, le programme «Justice» ou le Fonds social européen).

2. Lutter contre la radicalisation en ligne

Les terroristes continuent d'utiliser l'internet à des fins de radicalisation, de recrutement, ainsi que pour préparer et encourager des attentats terroristes et pour se vanter des atrocités qu'ils commettent. Le Conseil européen[32], le G7[33] et le G20[34], ont récemment demandé des mesures supplémentaires pour relever ce défi mondial et ont rappelé la responsabilité du secteur concerné à cet égard.

En juillet 2017, le forum de l'Union sur l'internet a mis au point **un plan d'action pour lutter contre les contenus terroristes en ligne**, appelant le secteur de l'internet à prendre des mesures résolues, à consacrer des ressources et à développer les outils technologiques nécessaires pour assurer la détection rapide de contenus préjudiciables en ligne et les supprimer. Le plan d'action appelle à progresser sans attendre dans un vaste éventail de domaines[35] et à instaurer un mécanisme de rapport régulier pour mesurer et évaluer les résultats.

Le 29 septembre 2017, la Commission a accueilli une réunion de hauts fonctionnaires du forum de l'UE sur l'internet afin de prendre connaissance de la mise en œuvre du **plan d'action pour lutter contre les contenus terroristes en ligne**. En ce qui concerne la détection automatisée, les entreprises se tournent davantage vers cette option qui leur permet de déployer un savoir-faire technique pour identifier les contenus terroristes au moment où ils sont mis en ligne. Certaines entreprises ont indiqué que 75 % des contenus sont désormais détectés automatiquement et transmis à des examinateurs humains qui décident en dernier lieu de leur suppression éventuelle tandis que, pour d'autres, 95 % des contenus sont détectés par des outils de détection propriétaires. Bien que ces progrès soient tangibles, la Commission a appelé toutes les entreprises à accélérer le déploiement de ces outils afin d'assurer une détection plus rapide, de réduire le temps pendant lequel le contenu terroriste demeure en ligne et de supprimer plus vite et plus efficacement la propagande terroriste. La Commission a également invité les entreprises à étendre leur outil «base de données d'empreintes

---

31 Conclusions du Conseil de l'Union européenne et des États membres, réunis au sein du Conseil, sur le renforcement de la réponse pénale à la radicalisation conduisant au terrorisme et à l'extrémisme violent (14382/15).

32 http://www.consilium.europa.eu/fr/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.

33 http://www.consilium.europa.eu/fr/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

34 http://www.consilium.europa.eu/fr/press/press-releases/2017/07/07-g20-counter-terrorism/.

35 COM(2017) 407 final du 26.7.2017;

numériques», afin d'empêcher que le contenu terroriste ne soit remis en ligne sur d'autres plateformes, à partir desquelles il pourrait essaimer vers des plateformes multiples. Cet outil devrait être étendu tant en ce qui concerne son contenu – au-delà des vidéos et des images qui sont actuellement couvertes – que les entreprises participantes.

La Commission continue également d'apporter son soutien aux organisations de la société civile qu'elle encourage à diffuser des **messages contenant des contre-discours** en ligne. Le 6 octobre 2017, la Commission a lancé un appel à propositions en vue de l'octroi d'un concours financier de 6 millions d'EUR à des consortiums d'acteurs de la société civile qui développent et mettent en œuvre ces campagnes.

Par la suite, le 6 décembre 2017, la Commission européenne entend convoquer le **forum de l'Union sur l'internet au niveau ministériel** auquel participeront de hauts représentants du secteur de l'internet afin d'évaluer les progrès réalisés et de jeter les bases des futures actions.

Les mesures prises pour lutter contre les contenus terroristes en ligne dans le cadre du forum de l'Union sur l'internet devraient être envisagées sous l'angle plus général de la lutte contre le contenu illicite sur internet. Ces mesures ont été étayées par une communication adoptée par la Commission le 28 septembre 2017, présentant des **orientations et principes afin que les plateformes en ligne** intensifient la lutte contre le contenu illicite en ligne[36] en collaboration avec les autorités nationales, les États membres et les autres parties intéressées. La communication vise à faciliter et à accélérer la mise en œuvre de bonnes pratiques pour interdire, détecter, supprimer et bloquer l'accès au contenu illicite de façon à garantir le retrait effectif de celui-ci, une transparence accrue et la protection des droits fondamentaux en ligne. Elle vise aussi à apporter aux plateformes des précisions sur leurs responsabilités lorsqu'elles prennent des mesures proactives pour détecter, supprimer ou bloquer l'accès au contenu illicite. La Commission attend des plateformes en ligne qu'elles prennent des mesures rapides au cours des prochains mois, notamment dans le cadre des dialogues concernés, en particulier dans le cadre du forum Internet de l'UE sur la propagande terroriste et les discours de haine illégaux.

Dans le même temps, la Commission suivra les progrès accomplis et déterminera si des mesures supplémentaires s'imposent pour assurer la détection rapide et proactive et la suppression des contenus illicites en ligne, telles que des mesures législatives complétant le cadre réglementaire en vigueur. Ces travaux s'achèveront au plus tard en mai 2018.

Sur le plan législatif, la proposition de directive[37] sur **la révision des services de médias audiovisuels (directive SMA)**, déposée en mai 2016, renforce la lutte contre les discours de haine. Elle a pour objectif d'harmoniser la directive avec la décision-cadre sur la lutte contre certaines formes et manifestations de racisme et de xénophobie[38] et la Charte des droits fondamentaux. Elle prévoit également l'obligation, pour les États membres, de veiller à ce que les plateformes de partage de vidéos appliquent des mesures propres à protéger adéquatement tous les citoyens de l'incitation à la violence ou à la haine. Ces mesures consistent, par exemple, à mettre en place des mécanismes permettant d'indiquer et de signaler les contenus illicites.

---

[36] Communication visant à lutter contre le contenu illicite en ligne intitulée «Pour une responsabilité accrue des plateformes en ligne» [COM(2017) 555 final du 28.9.2017].

[37] COM(2016) 287 final du 25.5.2016.

[38] Décision-cadre 2008/913/JAI du Conseil du 28.11.2008.

V. DIMENSION EXTÉRIEURE DE LA LUTTE CONTRE LE TERRORISME

1. Action extérieure de l'UE en matière de lutte contre le terrorisme

L'action extérieure en matière de lutte contre le terrorisme contribue à l'objectif prioritaire du renforcement de la sécurité intérieure de l'Union. Il convient en conséquence de renforcer encore le lien, sur le plan stratégique et politique, entre la sécurité intérieure et extérieure de l'UE, afin d'accroître l'efficacité des actions de lutte contre le terrorisme dans tous les domaines.

La Commission soutien un large éventail d'actions extérieures visant à renforcer la sécurité, moyennant un financement de 2,3 milliards d'EUR, débloqués pour plus de 600 projets en cours depuis le 1er janvier 2017. Un certain nombre d'activités sont axées sur la sécurité (à savoir les actions spécifiques concernant le financement du terrorisme, la lutte contre la radicalisation, les frontières, les prisons), d'autres présentent un intérêt pour la sécurité (comme les programmes qui s'attaquent aux causes profondes de l'insécurité et aux griefs en contribuant à améliorer l'éducation, l'accès aux ressources naturelles et à l'énergie, la gouvernance et le secteur de la sécurité ainsi que l'aide à la société civile).

Le Conseil des affaires étrangères du 19 juin 2017 a renouvelé l'orientation stratégique de ces domaines en adoptant un ensemble complet de **conclusions du Conseil sur l'action extérieure de l'UE en matière de lutte contre le terrorisme**[39]. La haute représentante et la Commission européenne collaboreront si nécessaire à la mise en œuvre fructueuse de ces conclusions. Afin d'assurer une mise en œuvre complète des conclusions et de faire rapport au Conseil d'ici à juin 2018, un processus de coordination entre le Service européen pour l'action extérieure et la Commission européenne a été mis en place. La priorité sera donnée aux volets suivants:

- **Renforcer le réseau d'experts en matière de lutte contre le terrorisme dans les délégations de l'UE**: il convient d'accroître progressivement la participation des experts en matière de lutte contre le terrorisme à la programmation du soutien de l'UE et à la coordination locale de la coopération de chaque État membre avec nos partenaires. Afin de promouvoir ce rôle renforcé, la formation avant et pendant le déploiement de ces experts sera améliorée. Les missions qui leur seront confiées seront mieux ciblées, grâce à des lettres de mission spécifiques, et leurs relations avec les agences de l'UE chargées de la justice et des affaires intérieures seront plus régulières. Afin de couvrir l'ensemble des domaines hautement prioritaires, la portée du réseau des experts[40] en matière de lutte contre le terrorisme sera étendue à la Corne de l'Afrique et à l'Asie centrale et du Sud-Est.
- **Renforcer la coopération entre les missions et opérations relevant de la politique de sécurité et de défense commune et les agences de l'UE chargées de la justice et des affaires intérieures** en ce qui concerne la collecte, l'analyse et l'échange d'informations, et explorer plus avant les moyens de resserrer les liens entre les acteurs militaires et les services répressifs aux fins de la lutte contre le terrorisme. Afin

[39] http://www.consilium.europa.eu/fr/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/

[40] À ce jour, l'UE déploie les experts en matière de lutte contre le terrorisme dans ses délégations dans les pays suivants: Algérie, Bosnie-Herzégovine (avec un mandat régional pour les Balkans occidentaux), Tchad (Sahel), Iraq, Jordanie, Liban, Libye (siège à Tunis), Maroc, Nigéria, Pakistan, Arabie saoudite, Tunisie et Turquie.

de faciliter l'échange de données et d'informations entre la politique de sécurité et de défense commune et celle en matière de justice et d'affaires intérieures, il importera de promouvoir une révision de certains éléments des cadres règlementaires actuels et de piloter l'intégration des cellules de renseignement spécialisées en matière criminelle dans certaines opérations et missions relevant de la politique de sécurité et de défense commune. Il importera de faciliter et d'améliorer davantage les synergies avec les activités des agences de l'UE chargées de la justice et des affaires intérieures dans les pays tiers prioritaires, y compris, lorsque cela est possible, d'intensifier le partage d'informations entre les acteurs internes ou externes à l'UE.

- **Renforcer la coopération internationale dans le domaine de la lutte contre le terrorisme et de la prévention de l'extrémisme violent et de la lutte contre ce phénomène** avec des pays partenaires dans les Balkans occidentaux, le Moyen-Orient, l'Afrique du Nord, la Turquie, les États du Golfe, le Sahel et la Corne de l'Afrique; avec des partenaires stratégiques de premier plan comme les États-Unis, le Canada et l'Australie; avec des partenaires régionaux et multilatéraux clés, dont les Nations unies, l'OTAN, le Forum mondial de lutte contre le terrorisme, le Groupe d'action financière, l'Union africaine, l'Association des nations de l'Asie du Sud-Est, le Conseil de coopération du Golfe, la Ligue des États arabes.

2. Convention du Conseil de l'Europe pour la prévention du terrorisme

Afin d'intensifier la coopération internationale en matière de lutte contre le terrorisme, la Commission avance, en même temps que le présent rapport, **des propositions**[41] **de décisions du Conseil relatives à la conclusion de la convention du Conseil de l'Europe pour la prévention du terrorisme et de son protocole additionnel**. La convention[42], adoptée par le Conseil de l'Europe le 16 mai 2005, concerne l'incrimination des activités terroristes et des activités liées au terrorisme, la coopération internationale concernant ces infractions et la protection et le dédommagement des victimes du terrorisme ainsi que l'aide qui leur est apportée. La Convention est entrée en vigueur le 1er juin 2007. Tous les États membres de l'UE l'ont signée et 23 États membres l'ont ratifiée. L'objectif du protocole additionnel[43], adopté par le Conseil le 18 mai 2015, est de compléter la convention par une série de dispositions visant à mettre en œuvre les aspects de droit pénal de la résolution 2178(2014) du Conseil de sécurité de l'Organisation des Nations Unies[44] intitulée «Menaces contre la paix et la sécurité internationales résultant d'actes de terrorisme». Le protocole additionnel répond à cette résolution en promouvant, en ce qui concerne les infractions liées aux combattants terroristes étrangers, une interprétation et une réponse communes. Le protocole additionnel est entré en vigueur le 1er juillet 2017.

L'UE a signé la Convention et son protocole additionnel le 22 octobre 2015. L'Union ayant adopté un ensemble complet d'instruments juridiques visant à lutter contre le terrorisme, et notamment la directive relative à la lutte contre le terrorisme[45], elle est désormais prête à mener à bien son engagement à devenir partie à la convention et à son protocole additionnel.

---

41 COM(2017) 606 final du 18.10.2017 et COM(2017) 607 final du 18.10.2017.
42 https://rm.coe.int/168008371c.
43 https://rm.coe.int/168047c5ea.
44 http://www.un.org/en/sc/ctc/docs/2015/N1454799_FR.pdf.
45 Directive (UE) 2017/541 du 15.3.2017.

3. Vers un accord révisé sur les données des dossiers passagers (PNR) avec le Canada

Dans son avis du 26 juillet 2017[46], la Cour de justice de l'UE a déclaré que l'accord entre l'Union européenne et le Canada sur le transfert des données des dossiers passagers, signé le 25 juin 2014, ne pouvait pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union, notamment en ce qui concerne le droit à la protection des données à caractère personnel. La Commission a pris contact avec les autorités canadiennes, y compris en marge de la réunion des ministres de l'Intérieur du G7 à Ischia, les 19 et 20 octobre 2017, afin de préparer les négociations à venir en vue de la révision du texte de l'accord. À cette fin, elle a soumis, parallèlement au présent rapport, une **recommandation**[47] **au Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord révisé** tenant compte de toutes les exigences formulées par la Cour dans son avis. Le Conseil est invité à autoriser rapidement l'ouverture de ces négociations. L'utilisation des données PNR étant essentielle pour lutter contre le terrorisme et les formes graves de criminalité transnationale, la Commission prendra les mesures nécessaires pour assurer la poursuite des transferts de données PNR au Canada dans le plein respect des droits fondamentaux conformément à l'avis de la Cour.

Dans ce contexte, la Commission tient à souligner qu'elle continuera d'apporter son soutien aux États membres en vue de la mise en œuvre de la directive PNR de l'UE[48]; les obligations découlant de la directive qui pèsent sur les États membres ne sont pas affectées par l'avis de la Cour.

4. Renforcer la coopération d'Europol avec les pays tiers

La coopération avec les pays tiers est essentielle dans la lutte contre le terrorisme et la criminalité organisée, comme souligné par les conclusions de juin 2017 du Conseil sur l'action extérieure de l'UE en matière de lutte contre le terrorisme[49] et les stratégies régionales pertinentes[50]. Avant l'entrée en vigueur du nouveau règlement Europol[51] le 1er mai 2017, Europol avait conclu, en vertu de sa base juridique[52] antérieure, des accords avec certains pays tiers afin d'assurer un cadre de coopération en vue de l'échange d'informations stratégiques et techniques. Certains de ces accords prévoient également la possibilité d'échanger des données à caractère personnel[53] et demeurent en vigueur.

Depuis le 1er mai 2017, le nouveau **règlement Europol** définit les règles qui régissent les relations extérieures d'Europol avec les pays tiers, notamment les conditions auxquelles sont soumis les échanges de données à caractère personnel avec les organes de l'Union, les pays

---

46 Avis 1/15 du la Cour de justice du 26.7.2017.

47 COM(2017) 605 final du 18.10.2017.

48 Directive (UE) 2016/681 du 27.4.2016.

49 http://www.consilium.europa.eu/fr/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/

50 Cela comprend la politique européenne de voisinage révisée [JOIN(2015) 50 final du 18.11.2015].

51 Règlement (UE) n° 2016/794 du 11.5.2016.

52 Décision 2009/371/JAI du Conseil du 6.4.2009.

53 Europol a conclu des accords autorisant l'échange de données à caractère personnel avec les pays tiers suivants: Albanie, Australie, Bosnie-Herzégovine, Canada, Colombie, ancienne République yougoslave de Macédoine, Géorgie, Islande, Liechtenstein, Moldavie, Monaco, Monténégro, Norvège, Serbie, Suisse, Ukraine et États-Unis. Le Conseil d'administration d'Europol avait autorisé l'ouverture de négociations sur un accord entre Europol et Israël, mais ces dernières n'étaient pas achevées lors de l'entrée en application du nouveau règlement Europol.

tiers et les organisations internationales. Conformément au traité et au règlement, la Commission est autorisée à négocier, au nom de l'Union, des accords internationaux avec des pays tiers en vue de l'échange de données à caractère personnel avec Europol[54]. Dans la mesure où cela est nécessaire à l'accomplissement de ses missions, Europol peut établir et entretenir des relations de coopération avec des partenaires extérieurs au moyen d'arrangements de travail et d'arrangements administratifs qui ne permettent pas l'échange de données à caractère personnel.

Eu égard aux besoins opérationnels de l'Union en ce qui concerne la coopération en matière de sécurité avec les pays tiers, et conformément au règlement Europol, **la Commission présentera des recommandations au Conseil avant la fin de l'année** afin d'autoriser l'ouverture de négociations entre l'UE et l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie, afin de fournir une base juridique au transfert de données à caractère personnel entre Europol et ces pays tiers[55]. De tels accords renforceront davantage les capacités d'Europol de nouer un dialogue avec les pays tiers afin de prévenir et de combattre les actes criminels qui relèvent des objectifs d'Europol.

VI. CONCLUSIONS

Le présent rapport présente un train de mesures visant à lutter contre le terrorisme et à soutenir davantage les États membres face aux menaces pour la sécurité. La Commission encourage les États membres et le Conseil à mettre en œuvre ces mesures de façon prioritaire. Elle tiendra le Parlement européen et le Conseil informés des progrès réalisés.

Le prochain rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité sera publié en décembre 2017 et mettra l'accent sur l'interopérabilité des systèmes d'information de l'UE aux fins de la gestion de la sécurité, des frontières et des flux migratoires. Sur cette toile de fond, la Commission rappelle combien il est important de progresser sur les priorités législatives en ce qui concerne ces systèmes d'information.

---

[54] Le règlement Europol prévoit également le transfert de données à caractère personnel entre Europol et un pays tiers sur la base d'une décision de la Commission constatant que le pays concerné assure un niveau adéquat de protection des données («décision d'adéquation»).

[55] Au-delà de ces pays tiers, la Commission rappelle le cadre stratégique pour les «décisions d'adéquation» ainsi que d'autres outils applicables aux transferts de données et aux instruments internationaux de protection des données, conformément à la formulation de la communication de la Commission au Parlement européen et au Conseil concernant l'échange et la protection de données à caractère personnel à l'ère de la mondialisation [COM(2017) 7 final du 10.1.2017], dans laquelle la Commission encourage l'adhésion des pays tiers à la convention 108 du Conseil de l'Europe et à son protocole additionnel.