COMMISSION
EUROPÉENNE

Bruxelles, le 29.6.2017
COM(2017) 354 final

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

Huitième 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 huitième 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.

Ces dernières semaines, l'Europe a de nouveau été frappée par une série d'attentats terroristes. Le 22 mai 2017, Manchester était victime d'un attentat atroce: l'explosion d'une bombe à l'extérieur d'une salle de concert provoquait la mort de 22 personnes, principalement des adolescents. Douze jours plus tard, le 3 juin 2017, un nouvel attentat frappait Londres: des terroristes fonçaient au hasard avec leur camionnette sur des piétons qui traversaient le London Bridge, avant de sortir de leur véhicule près de Borough Market, armés de couteaux pour poignarder des passants. Le 18 juin, un attentat similaire à la camionnette se produisait à l'extérieur d'une mosquée, tuant et blessant des fidèles innocents. Plus récemment, le 19 juin 2017, un terroriste tentait de commettre un attentat contre des gendarmes sur les Champs-Élysées à Paris, mais était abattu. Le 20 juin 2017, les forces de sécurité belges abattaient un homme qui tentait de commettre un attentat-suicide à la gare centrale de Bruxelles et dont la bombe n'avait pas explosé. L'ampleur et la fréquence de ces attentats soulignent une fois de plus l'importance capitale de la lutte contre l'extrémisme violent et du défi posé aux États membres consistant à contrecarrer les attentats tout en prévenant et combattant la radicalisation qui les alimente.

Le présent rapport présente les mesures prises au niveau de l'UE pour **prévenir et combattre la radicalisation**, dressant le bilan des progrès accomplis en réponse aux défis de la radicalisation un an après l'adoption de la communication de la Commission de juin 2016 intitulée «Soutien à la prévention de la radicalisation conduisant à l'extrémisme violent»[1]. Il fournit également des informations actualisées sur les progrès accomplis dans la mise en œuvre des autres dossiers prioritaires en matière de sécurité, avec les mesures à venir pour améliorer l'**échange d'informations** grâce à l'interopérabilité des systèmes d'information et pour mettre en œuvre le plan d'action contre le financement du terrorisme[2] afin de **détecter et de prévenir le financement du terrorisme**.

Les conclusions du Conseil européen[3] des 22 et 23 juin 2017 ont réitéré avec force la détermination de l'Union à coopérer pour lutter contre la propagation de la radicalisation en ligne, pour coordonner les efforts visant à prévenir et combattre l'extrémisme violent et à lutter contre l'idéologie qui le sous-tend, pour faire échec au financement du terrorisme, pour faciliter les échanges rapides et ciblés d'informations entre les services répressifs, y compris avec des partenaires de confiance, et pour améliorer l'interopérabilité des bases de données. La récente déclaration du sommet du G7 à Taormine[4] sur la lutte contre le terrorisme et l'extrémisme violent a envoyé un signal fort de la communauté internationale, déterminée à faire face à la menace croissante du terrorisme, et souligné la nécessité de poursuivre une action concertée au niveau mondial.

---

1 COM(2016) 379 final (14.6.2016).
2 COM(2016) 50 final (2.2.2016).
3 http://www.consilium.europa.eu/fr/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/.
4 http://www.consilium.europa.eu/fr/press/press-releases/2017/05/26-statement-fight-against-terrorism/.

Enfin, le présent rapport aborde également la question de l'**aggravation de la menace informatique** et expose des mesures à court terme pour y faire face, en s'appuyant sur les enseignements tirés de la réaction à la cyberattaque *WannaCry*.

II. L'ACTION DE L'UE VISANT À SOUTENIR LA PRÉVENTION DE LA RADICALISATION

Bien que la radicalisation violente ne constitue pas un phénomène nouveau, les attentats terroristes perpétrés récemment dans l'UE ont montré de manière alarmante avec quelle rapidité et avec quelle ampleur certains citoyens de l'Union se radicalisent. Les recruteurs de terroristes déploient tout un éventail de techniques différentes pour cibler les personnes vulnérables. L'utilisation des outils de communication numérique pose des défis nouveaux et particuliers aux autorités des États membres. La lutte contre la radicalisation au moyen d'une réponse pluridimensionnelle à l'échelle de l'Union, tant en ligne qu'hors ligne, joue donc un rôle essentiel dans le soutien apporté aux États membres pour combattre le terrorisme.

Afin de lutter contre la **radicalisation en ligne**, la Commission a travaillé ces deux dernières années avec les principales plateformes internet, notamment dans le cadre du Forum de l'UE sur l'internet pour veiller à la suppression, sur base volontaire, des contenus terroristes en ligne. Dans le cadre de ces activités, des progrès réels ont été accomplis en matière de suppression des contenus terroristes en ligne[5] et de lutte contre les discours haineux illégaux en ligne[6], mais il reste encore beaucoup à faire. Les conclusions du Conseil européen des 22 et 23 juin 2017 indiquent que «*[d]ans le prolongement des travaux menés par le Forum de l'UE sur l'internet, le Conseil européen attend des entreprises du secteur qu'elles créent leur propre forum et mettent au point de nouvelles technologies et de nouveaux outils en vue d'améliorer la détection automatique et la suppression des contenus qui incitent à la commission d'actes terroristes. Cela devrait être complété par les mesures législatives appropriées au niveau de l'UE, si nécessaire*». La Commission a organisé, le 27 juin 2017, une réunion de hauts fonctionnaires du Forum de l'UE sur l'internet afin de convenir de mesures supplémentaires avec les principaux fournisseurs de services internet pour lutter contre les contenus terroristes en ligne. L'**objectif est d'associer davantage les plateformes internet**, notamment pour intensifier la détection automatisée des contenus à caractère terroriste, partager les technologies et outils connexes avec de petites entreprises et faire pleinement usage de la «base de données d'empreintes numériques (hashes)», y compris en donnant à Europol accès aux informations clés, et mettre en place un système de signalement du retrait d'un contenu à caractère terroriste. En outre, afin de compléter les travaux menés par l'unité d'Europol chargée du signalement des contenus sur l'internet, la Commission invite tous les États membres à créer des **unités nationales de signalement des contenus sur**

[5] Grâce à l'**unité de signalement des contenus sur l'internet** (IRU) d'Europol, 30 000 contenus à caractère terroriste ont ainsi pu être signalés aux plateformes internet, donnant lieu à un taux moyen de suppression des contenus signalés de 80-90 %. En outre, l'initiative du secteur de l'internet visant à créer une **«base de données d'empreintes numériques»** garantit que le contenu à caractère terroriste, une fois retiré d'une plateforme, ne peut plus être chargé sur une autre.

[6] La Commission a adopté, en mai 2016, un **code de conduite pour lutter contre les discours haineux illégaux en ligne** qui a été signé par Facebook, YouTube, Twitter et Microsoft, qui se sont engagées à examiner et à supprimer rapidement et efficacement les contenus signalés comme discours haineux illégaux. Un an après son adoption, ce code se solde par des progrès significatifs. Les entreprises ont retiré les contenus dans deux fois plus de cas de discours haineux illégaux et ce, plus rapidement, par rapport à la situation antérieure à l'accord sur le code.

l'internet et à les mettre en réseau aux fins d'une coopération commune avec les plateformes internet et ladite unité d'Europol.

Comme en témoignent les récents attentats, l'ampleur sans précédent de la radicalisation exige également des mesures supplémentaires afin de soutenir la prévention et la lutte contre la radicalisation aux niveaux national et local. La Commission mettra rapidement en place[7] un **groupe d'experts de haut niveau sur la radicalisation** en vue de faciliter l'élaboration des nouvelles politiques de l'UE dans ce domaine. Ce groupe sera chargé de donner un élan aux travaux à mener dans les domaines hautement prioritaires tels que la lutte contre la radicalisation en milieu carcéral, la lutte contre la propagande terroriste en ligne, et la question du retour des combattants terroristes étrangers. Les travaux du groupe viseront à soutenir le **réseau de sensibilisation à la radicalisation (RSR)** qui a été au premier plan de l'action de la Commission pour aider les États membres dans ce domaine, en collaboration avec les acteurs de terrain locaux au niveau communautaire[8]. Plus récemment, le 19 juin 2017, ce réseau a présenté un **manuel sur les réponses à apporter au phénomène du retour des combattants étrangers** afin d'aider les États membres à relever les défis posés par ce phénomène. Ce manuel donne un aperçu des approches des acteurs de terrain pour faire face aux différents cas de figure de personnes de retour des zones de conflit. Dans les mois à venir, le réseau organisera une série d'ateliers destinés aux autorités nationales afin d'approfondir ces pratiques et d'encourager une action dans les États membres.

Les défis complexes entourant la radicalisation nécessitent une réponse pluridimensionnelle comprenant des mesures à long terme, ainsi que le soulignait la communication de juin 2016 sur la prévention de la radicalisation conduisant à l'extrémisme violent[9]. Au cours de l'année dernière, la Commission a mis en œuvre la plupart des **actions clés définies dans d'autres domaines liés à la prévention et à la lutte contre la radicalisation**[10]. Afin d'aider les États membres à lutter contre la radicalisation en milieu carcéral, un groupe «Prison et probation», relevant du réseau de sensibilisation à la radicalisation, a été tout spécialement constitué pour guider les professionnels de première ligne tels que les agents pénitentiaires et de probation, les psychologues et les représentants religieux. L'éducation joue un rôle clé dans la prévention de la radicalisation, et la Commission a pris une série de mesures visant à mettre en œuvre la déclaration de Paris sur la promotion de l'éducation à la citoyenneté et aux valeurs communes de liberté, de tolérance et de non-discrimination. Le programme Erasmus+ est essentiel à cet égard[11]. Compte tenu des liens entre marginalisation, vulnérabilité et

---

7 La Commission constituera ce groupe en juillet 2017.

8 Le réseau de sensibilisation à la radicalisation a offert des formations et des conseils aux États membres, et établi un grand nombre de bonnes pratiques, lignes directrices, manuels et recommandations. Les thèmes et sujets couverts incluent la polarisation, la radicalisation en milieu carcéral et les programmes de sortie, les mesures de soutien aux familles, le travail socio-éducatif auprès des jeunes, la police de proximité, la communication et les discours, la participation et la responsabilisation des jeunes.

9 Voir le tableau figurant à l'annexe 1 qui énumère les mesures prises pour mettre en œuvre la communication de juin 2016.

10 La communication de juin 2016 porte essentiellement sur **sept domaines spécifiques**: (1) soutien à la recherche, à la collecte de données probantes, à des actions de suivi et aux réseaux; (2) lutte contre la propagande terroriste et les discours haineux en ligne; (3) lutte contre la radicalisation en milieu carcéral; (4) promotion d'une éducation ouverte à tous et des valeurs communes de l'UE; (5) promotion d'une société inclusive, ouverte et résiliente et actions en faveur des jeunes; (6) la dimension sécuritaire de la lutte contre la radicalisation; et (7) la dimension internationale.

11 Au titre du **programme Erasmus+**, en 2016, plus de 200 millions d'euros ont été consacrés à l'élaboration de nouvelles approches et pratiques à travers 1 200 projets de partenariat transnational, associant des acteurs locaux et mettant l'accent sur une éducation ouverte à tous, l'animation socio-éducative, l'éducation à la

radicalisation, le socle européen des droits sociaux[12], adopté le 26 avril 2017, constitue un élément important pour s'attaquer à certaines des causes profondes de la radicalisation et de l'extrémisme violent[13]. Pour renforcer la cohésion des sociétés européennes, la Commission met également en œuvre le plan d'action pour l'intégration des ressortissants de pays tiers[14], avec un vaste ensemble de mesures destinées à aider les États membres et les autres acteurs dans leurs efforts d'intégration.

Sur le **plan extérieur**, l'UE œuvre actuellement dans des enceintes internationales, notamment l'Organisation pour la sécurité et la coopération en Europe (OSCE) et des organismes[15] découlant du Forum mondial de lutte contre le terrorisme, afin de soutenir la prévention et la lutte contre la radicalisation dans les pays partenaires dans les Balkans occidentaux, au Moyen-Orient et en Afrique du Nord, y compris la formation des professionnels concernés et un soutien financier aux initiatives de terrain dans le domaine de la prévention. Une nouvelle initiative relevant du programme Erasmus+ et consistant en échanges virtuels de jeunes sera lancée en 2018 afin d'améliorer la compréhension interculturelle entre les jeunes à l'intérieur et à l'extérieur de l'UE et de les sensibiliser davantage aux aspects interculturels. Le réseau de sensibilisation à la radicalisation a également déployé des experts chargés de soutenir les actions de prévention en Turquie, dans les Balkans occidentaux et en Tunisie.

III. L'ACTION DE L'UE FACE AUX CYBERMENACES ET À LA CYBERCRIMINALITÉ

La cyberattaque de mai 2017 commise au moyen d'un rançongiciel, *WannaCry*, a été un avertissement mettant en évidence les lacunes du cadre actuel en matière de cybersécurité, notamment en matière de préparation et de coopération. Comme annoncé déjà avant l'attaque, dans l'examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique, **la Commission accélère ses travaux dans le domaine de la cybersécurité**, notamment en procédant à une révision de la stratégie de cybersécurité de 2013. La Commission et le Service européen pour l'action extérieure évaluent actuellement les progrès accomplis dans la mise en œuvre de la stratégie existante. L'objectif est de mettre en lumière les lacunes auxquelles devra remédier la révision de la stratégie en septembre 2017.

---

citoyenneté et interculturelle. Une nouvelle «boîte à outils», mise au point en coopération avec des experts des États membres, fournit des orientations et des conseils aux animateurs socio-éducatifs amenés à travailler avec des jeunes exposés au risque de radicalisation violente. La Commission a également lancé un **réseau de personnes véhiculant un modèle positif**, mis en œuvre grâce à Erasmus+. Cette initiative permettra aux acteurs locaux de bénéficier de financements modestes de l'UE pour constituer des réserves de personnes véhiculant un modèle positif, prêtes à se lancer dans des activités visant à promouvoir l'inclusion sociale auprès des élèves et des jeunes.

12 https://ec.europa.eu/commission/priorities/deeper-and-fairer-economic-and-monetary-union/european-pillar-social-rights/european-pillar-social-rights-20-principles_fr.

13 En mai 2017, la Commission a lancé une consultation publique en ligne, en vue d'élaborer une proposition de recommandation du Conseil visant à promouvoir l'inclusion sociale et les valeurs communes avant la fin de 2017. L'objectif est d'établir un cadre d'action pour aider les États membres à promouvoir une éducation ouverte à tous qui favorise l'appropriation des valeurs communes, en contribuant à prévenir la radicalisation conduisant à l'extrémisme violent.

14 COM(2016) 377 final (7.6.2016).

15 Le Fonds mondial pour la mobilisation et la résilience communautaires (GCERF), le Centre d'excellence Hedayah pour la lutte contre l'extrémisme violent et l'Institut international pour la justice et l'État de droit.

Parallèlement à cela et en réponse aux enseignements tirés de la réaction à la cyberattaque *WannaCry*, un certain nombre d'**actions à court terme** devraient être prises à présent pour renforcer nos moyens d'action face à l'aggravation de la cybermenace. Il est notamment nécessaire de progresser rapidement en ce qui concerne le renforcement de notre résilience, en particulier sur les questions liées à la coopération opérationnelle.

La cyberattaque *WannaCry* a constitué le premier incident amenant le **réseau des centres nationaux de réponse aux incidents de sécurité informatique** (réseau CSIRT) à coopérer, celui-ci ayant été établi en vertu de la **directive relative à la sécurité des réseaux et de l'information** (SRI). Cet incident a démontré que le système n'était pas encore pleinement opérationnel. Il a aussi clairement souligné la nécessité d'accélérer les travaux en cours pour améliorer les outils informatiques existants, et de déployer des capacités supplémentaires pour permettre la poursuite de la coopération entre les centres nationaux. Pour renforcer ces derniers, la Commission apportera un financement de 10,8 millions d'EUR en faveur de 14 États membres dans le cadre du mécanisme pour l'interconnexion en Europe, les projets ayant une durée de deux ans à compter de septembre 2017. Un autre appel à propositions est actuellement ouvert et tous les autres États membres sont invités à présenter leurs demandes de financement.

Le **Centre européen de lutte contre la cybercriminalité** (EC3) a conduit la réaction des services répressifs face à cette cyberattaque. Afin de renforcer ce centre et les services qu'il fournit, il est nécessaire de le doter de nouvelles compétences informatiques. Pour ce faire, le conseil d'administration d'Europol devrait améliorer, d'ici à septembre 2017, les possibilités de recrutement de spécialistes en informatique prévues dans le règlement intérieur d'Europol. Ces activités d'Europol seront, en outre, soutenues par le recrutement de personnel supplémentaire en 2018.

L'**équipe d'intervention de l'UE en cas d'urgence informatique** (CERT-EU) aide les institutions européennes à se protéger contre les attaques intentionnelles et malveillantes qui compromettraient l'intégrité de leurs biens informatiques et nuiraient aux intérêts de l'UE. La Commission va maintenant accélérer le processus formel de renforcement de la CERT-UE en concluant des accords entre les institutions et organes concernés afin d'améliorer la réponse collective aux menaces. Il s'agit notamment du Parlement européen, du Conseil, de la Cour de justice de l'Union européenne, de la Banque centrale européenne, de la Cour des comptes, du Service européen pour l'action extérieure, du Comité économique et social européen, du Comité des régions et de la Banque européenne d'investissement. La Commission signera d'ici peu un accord administratif interinstitutionnel avec les autres institutions et organes.

Ces mesures à court terme s'inscrivent dans le cadre plus large de la **révision de la stratégie de cybersécurité de 2013** qui suivra en septembre 2017, accompagnée des mesures nécessaires pour renforcer la résilience et la sécurité du cyberespace de l'Union. Dans ses conclusions des 22 et 23 juin 2017, le Conseil européen salue l'intention de la Commission de réexaminer en septembre la stratégie de cybersécurité et de proposer avant la fin de l'année de nouvelles actions ciblées.

Une dissuasion réussie passe aussi par des mesures de suivi et de détection, des enquêtes et des poursuites efficaces. L'accès aux **preuves électroniques** constitue une question essentielle à cet égard. Les cadres actuels de la justice pénale reflètent toujours des notions traditionnelles de la territorialité et sont remis en question par la nature transfrontière des services électroniques et des flux de données. Les conclusions du Conseil européen des 22 et 23 juin 2017 soulignent que l'accès effectif aux preuves électroniques est essentiel dans le

cadre de la lutte contre les formes graves de criminalité et le terrorisme et que, sous réserve de garanties appropriées, la disponibilité des données devrait être assurée. Lors du Conseil «Justice et affaires intérieures» du 8 juin 2017, les ministres ont exprimé un large soutien aux mesures concrètes proposées par la Commission en vue d'améliorer la situation dans le cadre législatif actuel. Les ministres ont également invité la Commission à présenter une proposition législative dès que possible, en gardant à l'esprit les défis techniques et juridiques. Sur cette base, la Commission continuera à mettre en œuvre des mesures concrètes, tout en procédant à une analyse d'impact aux fins d'une éventuelle proposition législative à présenter dans les plus brefs délais.

Le **chiffrement** constitue une autre question tout aussi importante dans ce contexte. Le chiffrement est indispensable pour assurer la cybersécurité et pour protéger les données à caractère personnel. Son exploitation par les criminels pose, en revanche, des problèmes importants dans le cadre de la lutte contre les formes graves de criminalité, notamment la cybercriminalité et le terrorisme. Les conclusions du Conseil européen des 22 et 23 juin 2017 appellent à relever les défis que posent les systèmes qui permettent aux terroristes de communiquer par des moyens auxquels les autorités compétentes ne peuvent avoir accès, y compris le chiffrement de bout en bout, tout en préservant les avantages que ces systèmes offrent en matière de protection de la vie privée, des données et des communications. Comme l'a demandé le Conseil «Justice et affaires intérieures» en décembre 2016, la Commission travaille en étroite collaboration avec les agences de l'UE et les entreprises pour déterminer comment aider les autorités répressives à surmonter les défis les plus significatifs, en tenant compte des implications pour la cybersécurité et les droits fondamentaux. En collaboration avec Europol, Eurojust, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et l'Agence des droits fondamentaux de l'UE, la Commission a examiné tous les aspects de cette question importante avec des experts compétents en la matière dans le cadre d'une série d'ateliers. La Commission communiquera ses conclusions au Parlement européen et au Conseil d'ici octobre 2017.

Sur le **plan extérieur**, le Conseil est convenu, le 19 juin 2017, de définir un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance, à savoir la **boîte à outils en matière de cyberdiplomatie**[16]. Ce cadre pour une réponse diplomatique conjointe de l'UE tirera pleinement parti des mesures relevant de la politique étrangère et de sécurité commune, y compris, si nécessaire, des mesures restrictives. Toute réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance devrait être proportionnée à la portée, l'échelle, la durée, l'intensité, la complexité, la sophistication et l'incidence de la cyberactivité. Ce cadre vise à encourager la coopération, à faciliter la réduction des menaces immédiates et à long terme, et à influencer le comportement d'agresseurs potentiels à long terme. En collaboration avec les États membres, la Commission et le Service européen pour l'action extérieure mettront en place, dans les prochains mois, des lignes directrices relatives à la mise en œuvre, y compris les procédures préparatoires et de communication, et des exercices.

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

1. Prochaines étapes pour parvenir à l'interopérabilité des systèmes d'information

[16] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/fr/pdf .

La Commission prend actuellement des mesures supplémentaires pour mettre en œuvre la nouvelle approche de la gestion des données pour les frontières et la sécurité, telle qu'elle est exposée dans le septième rapport[17]. Le 28 juin 2017, la Commission a présenté une **proposition législative[18] visant à renforcer le mandat de l'agence eu-LISA**[19]. Cette agence jouera un rôle essentiel dans les travaux techniques nécessaires à l'interopérabilité des systèmes d'information, notamment l'analyse technique en cours portant sur les solutions recensées pour y parvenir. Sous réserve de l'adoption par les colégislateurs des propositions législatives correspondantes, les modifications qu'il est proposé d'apporter au mandat de l'agence eu-LISA l'habiliteront à développer des solutions d'interopérabilité, assurant ainsi la mise en œuvre technique de cette nouvelle approche. Les conclusions du Conseil européen des 22 et 23 juin 2017 mentionnent l'importance de l'interopérabilité des systèmes d'information pour la sécurité intérieure et la lutte contre le terrorisme.

La Commission a également présenté, le 28 juin 2017, une proposition complémentaire à sa proposition de janvier 2016[20] visant à faciliter l'**échange des casiers judiciaires de ressortissants de pays tiers** dans l'Union européenne au moyen du système européen d'information sur les casiers judiciaires (ECRIS)[21]. Cette proposition complémentaire fait suite aux discussions engagées avec les colégislateurs sur la proposition de l'année dernière et s'inscrit dans le cadre de l'approche de la Commission relative à l'interopérabilité des systèmes d'information. L'amélioration de l'ECRIS en ce qui concerne l'échange d'informations sur les ressortissants de pays tiers est une priorité législative qui figure dans la déclaration commune[22] des Présidents du Parlement européen, du Conseil et de la Commission.

Des **progrès dans d'autres dossiers prioritaires relatifs aux systèmes d'information** sont également à noter. Les discussions se sont poursuivies entre les colégislateurs sur la proposition de système d'entrée/sortie de l'UE[23], des réunions de trilogue s'étant tenues le 31 mai ainsi que les 13, 19 et 26 juin 2017. Le Conseil a marqué son accord sur une orientation générale concernant la proposition de système européen d'information et d'autorisation concernant les voyages (ETIAS)[24] lors du Conseil «Justice et affaires intérieures» des 8 et 9 juin 2017. Le vote de la commission du Parlement européen chargée des libertés civiles, de la justice et des affaires intérieures (LIBE) sur les modifications déposées concernant cette proposition est prévu pour septembre 2017 et les négociations en trilogue devraient débuter en octobre 2017. Il est essentiel que le Parlement européen et le Conseil progressent sur ces propositions prioritaires, ainsi que l'ont souligné les conclusions du Conseil européen des 22 et 23 juin 2017.

Le 29 mai 2017, la Commission, en collaboration avec le contrôleur européen de la protection des données, l'Agence des droits fondamentaux de l'UE et le coordinateur de l'UE pour la lutte contre le terrorisme, a présenté à la commission LIBE les conclusions du groupe

---

17 COM(2017) 261 final (16.5.2017).
18 COM(2017) 352 final (29.6.2017).
19 Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.
20 COM(2016) 7 final (19.1.2016).
21 COM(2017) 344 final (29.6.2017).
22 https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_en.pdf.
23 COM(2016) 194 final (6.4.2016).
24 COM(2016) 731 final (16.11.2016).

d'experts de haut niveau sur les systèmes d'information et l'interopérabilité[25] et sa nouvelle approche de la gestion des données pour les frontières et la sécurité. Le 8 juin 2017, le Conseil a adopté des conclusions[26] sur l'échange d'informations et l'interopérabilité, saluant à cet égard le point de vue de la Commission et la voie à suivre proposée pour parvenir à l'interopérabilité des systèmes d'information d'ici à 2020 sur la base des recommandations du groupe d'experts de haut niveau. S'appuyant sur ces discussions, la Commission continuera de travailler avec le Parlement européen et le Conseil en vue d'assurer l'interopérabilité des systèmes d'information d'ici à 2020.

2. Action de l'UE visant à couper les sources et canaux de financement du terrorisme

Des travaux sont en cours pour mettre en œuvre le **plan d'action contre le financement du terrorisme**, de février 2016, suivant deux grands axes d'action: d'une part, détecter et prévenir le financement du terrorisme et, d'autre part, désorganiser les sources de revenus. En décembre 2016, la Commission a présenté trois propositions législatives visant à compléter et à renforcer le cadre juridique de l'UE dans les domaines du blanchiment de capitaux[27], des mouvements illicites d'argent liquide[28] et du gel et de la confiscation d'avoirs[29]. La Commission invite les colégislateurs à faire progresser rapidement les travaux sur ces propositions importantes.

En outre, les colégislateurs ont considérablement progressé dans les négociations sur les modifications à apporter à la **4e directive anti-blanchiment de capitaux**, fondées sur une proposition législative de juillet 2016[30]. La Commission reste pleinement déterminée à mener à bien rapidement les trilogues en cours. Considérées dans leur ensemble, ces mesures **complètent les engagements que la Commission s'était engagée à honorer dans le plan d'action**[31]. Elles permettront également à l'UE de respecter ses obligations internationales dans ce domaine, telles que convenues dans le cadre du groupe d'action financière (GAFI) et la convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (convention de Varsovie).

Comme indiqué dans le plan d'action, la Commission entend également adopter une proposition visant à lutter contre le commerce illicite de biens culturels afin d'étendre le champ d'application de la législation en vigueur à d'autres pays tiers. Elle envisage aussi une proposition visant à donner aux services répressifs et autres autorités publiques accès aux registres des comptes bancaires. Qui plus est, elle a récemment adopté un rapport sur l'évaluation supranationale des risques de blanchiment de capitaux et de financement du terrorisme[32], ainsi qu'un document de travail sur l'amélioration de la coopération entre les

---

25 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

26 Conclusions du Conseil sur la voie à suivre pour améliorer l'échange d'informations et assurer l'interopérabilité des systèmes d'information de l'UE: http://data.consilium.europa.eu/doc/document/ST-9448-2017-INIT/fr/pdf.

27 Proposition de **directive visant à harmoniser la définition des infractions et sanctions pénales dans le domaine du blanchiment de capitaux**, COM(2016) 826 final (21.12.2016).

28 Proposition de **règlement visant à découvrir les mouvements illicites d'argent liquide**, COM(2016) 825 final (21.12.2016).

29 Proposition de **règlement relatif à la reconnaissance mutuelle des décisions de gel et de confiscation d'avoirs d'origine criminelle**, COM(2016) 819 final (21.12.2016).

30 COM(2016) 450 final (5.7.2016).

31 Voir le tableau figurant à l'annexe 2 qui énumère les mesures prises pour mettre en œuvre le plan d'action de février 2016.

32 COM(2017) 340 final (26.6.2017).

cellules de renseignement financier[33]. Dans le courant de cette année, elle rendra compte de son évaluation en cours de la nécessité de prendre d'éventuelles mesures supplémentaires pour surveiller le financement du terrorisme au sein de l'UE. La Commission est également en train de revoir la législation relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces pour tenir compte des nouvelles formes de criminalité et de contrefaçon dans le domaine des instruments financiers, dans le but d'en limiter l'ampleur et de dissuader les activités criminelles potentielles telles que le financement du terrorisme.

3. Dimension extérieure

Les conclusions du Conseil du 19 juin 2017 sur l'action extérieure de l'UE en matière de la lutte contre le terrorisme[34] mettent en évidence la nécessité de renforcer la **dimension extérieure** de la lutte contre le financement du terrorisme et le blanchiment de capitaux. Elles confirment les priorités géographiques et thématiques de l'action extérieure future en la matière, à savoir le renforcement de la coopération avec les pays tiers prioritaires du Moyen-Orient, d'Afrique du Nord, des Balkans occidentaux et la Turquie, ainsi qu'avec les partenaires stratégiques et les organisations internationales. Ces conclusions reposent largement sur la note libre concernant l'action extérieure en matière de lutte contre le terrorisme que le Service européen pour l'action extérieure et la Commission ont présenté en mai 2017 aux États membres.

Le 16 juin 2017, une **réunion ministérielle «Justice et affaires intérieures» entre l'UE et les États-Unis** s'est tenue à Malte. Il s'est agi de la première réunion de ce type avec la nouvelle administration américaine. Les États-Unis ont affirmé leur souhait de poursuivre une coopération étroite avec l'UE et souligné la nécessité de mettre en œuvre rapidement le partage d'informations dans le cadre de la lutte contre le terrorisme et la criminalité organisée. La Commission a présenté les actions menées par l'UE à l'encontre des combattants terroristes étrangers, en mettant l'accent sur le partage transatlantique d'informations. L'UE et les États-Unis ont fourni des informations actualisées sur leurs actions de lutte contre la radicalisation en ligne et hors ligne, sur l'évolution de la situation en ce qui concerne les données des dossiers passagers (PNR), le blanchiment de capitaux, la gestion des frontières et la sûreté aérienne. Sur la question des risques pour la sûreté aérienne liés aux appareils électroniques personnels, l'UE et les États-Unis sont convenus de continuer à collaborer afin de relever les normes mondiales en matière de sûreté aérienne. La Commission a communiqué aux États membres des informations sur les discussions et les éventuelles mesures d'atténuation au sein du comité pour la sûreté de l'aviation civile le 21 juin 2017, et continuera de coopérer étroitement avec les États-Unis aux niveaux technique et politique pour faire face aux menaces grandissantes.

V. CONCLUSION

Le présent rapport met l'accent sur les mesures prises ces derniers mois pour mettre en place une union de la sécurité réelle et effective. L'augmentation des attentats terroristes commis au cours des dernières semaines et des derniers mois souligne à nouveau l'importance de cette action et la nécessité de progresser rapidement. Il est urgent de mettre en œuvre les mesures décrites dans le présent rapport pour combattre cette menace terroriste accrue, renforcer la coopération au niveau de l'UE visant à prévenir et combattre la radicalisation, couper le financement du terrorisme et intensifier l'échange d'informations, et parvenir à

[33] SWD(2017) 275 (26.6.2017).

[34] http://www.consilium.europa.eu/fr/press/press-releases/2017/06/19-conclusions-counterterrorism/.

l'interopérabilité des systèmes d'information qui permettra de combler les déficits d'information. Les conclusions du Conseil européen des 22 et 23 juin 2017 confirment l'importance et l'urgence des actions en cours. La Commission invite le Parlement européen et le Conseil à poursuivre et à intensifier ces efforts communs visant à renforcer la sécurité de tous les citoyens.

Le prochain rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, de juillet 2017, présentera les résultats de l'évaluation globale de l'action de l'Union dans le domaine de la sécurité intérieure et les conclusions que la Commission aura tirées du processus de consultation ouvert lancé en décembre 2016.