COMMISSION
EUROPÉENNE

Strasbourg, le 12.12.2017
COM(2017) 779 final

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

Douzième 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 douzième 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.

Cela fait presque un an que l'attentat sur le marché de Noël à Berlin du 19 décembre 2016, dont le bilan a été de douze morts et cinquante-six blessés, a été perpétré par un individu qui avait utilisé plusieurs identités pour échapper aux autorités frontalières et répressives. Cet acte et les autres attentats terroristes perpétrés par des auteurs qui ont utilisé plusieurs identités, comme l'attaque à l'arme blanche commise à Marseille en octobre 2017, ont mis en évidence non seulement l'importance d'un partage d'informations efficace entre les autorités des États membres, mais également l'importance cruciale des travaux entamés par la Commission au printemps 2016[1] afin de remédier aux failles actuelles de la gestion des informations au niveau de l'Union qui permettent à un individu d'apparaître dans différentes bases de données de l'Union sous plusieurs identités différentes. Les propositions législatives de règlements[2] sur l'interopérabilité des systèmes d'information, qui sont soumises dans le cadre d'un train de mesures accompagnant le présent rapport, visent à éliminer les possibilités d'exploiter les lacunes actuelles dont profitent les terroristes et les criminels pour commettre des fraudes à l'identité et, ainsi, à mieux protéger les frontières extérieures de l'Union, renforcer la sécurité intérieure et améliorer la gestion des flux migratoires[3]. Ces propositions constituent une évolution radicale, d'une part en ce qu'elles modifient la façon dont l'Union gère les informations pour la gestion de la sécurité, des frontières et des flux migratoires, et d'autre part en ce qu'elles mettent les données à la disposition des autorités nationales, afin que ces dernières aient accès aux informations dont elles ont besoin au moment et à l'endroit où elles en ont besoin. Compte tenu du caractère essentiel de ces propositions pour l'amélioration de l'efficacité des autorités frontalières et répressives, la Commission invite désormais les colégislateurs à examiner de façon hautement prioritaire les propositions législatives sur l'interopérabilité et à parvenir rapidement à un accord sur les autres propositions législatives présentées, qui concernent les différents systèmes d'information permettant aux acteurs présents en première ligne de disposer des informations dont ils ont besoin pour remplir leur mission consistant à veiller à la sécurité de nos concitoyens.

Le présent rapport est dès lors axé sur les prochaines étapes de la mise en place de systèmes d'information plus robustes et plus intelligents au service de la sécurité, des frontières et de la gestion des flux migratoires, afin d'améliorer et de rendre plus efficace l'architecture de données des systèmes d'information de l'Union, tout en garantissant le respect plein et entier des exigences en matière de protection des données.

Ce rapport fait aussi le point sur plusieurs mesures destinées à optimiser les avantages des systèmes d'information existants, en couvrant les travaux législatifs et les démarches en cours devant assurer leur pleine mise en œuvre et une meilleure application des systèmes d'information de l'Union. En octobre 2017, le Conseil européen a fait le point sur la mise en

[1] COM(2016) 205 du 6.4.2016.
[2] COM(2017) 793 final et COM(2017) 794 final du 12.12.2017.
[3] COM(2017) 261 final du 16.5.2017.

œuvre de la feuille de route de Bratislava[4] et a pris acte des progrès notables accomplis par l'Union, en particulier en ce qui concerne la sécurité intérieure, dans quatre domaines: l'intensification de la coopération et de l'échange d'informations, le renforcement des contrôles et de l'interconnexion des bases de données, la mise en place d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), et la lutte systématique contre la radicalisation. Le présent rapport montre que des progrès supplémentaires ont été réalisés dans tous ces domaines au cours des deux derniers mois.

II. DES SYSTÈMES D'INFORMATION PLUS ROBUSTES ET PLUS INTELLIGENTS AU SERVICE DE LA SÉCURITÉ, DES FRONTIÈRES ET DE LA GESTION DES FLUX MIGRATOIRES

D'après des enquêtes récentes, les citoyens de l'Union soutiennent fortement l'intensification de l'échange d'informations au sein de l'Union pour la lutte contre le terrorisme et la criminalité organisée[5]. Les informations fournies par les systèmes de l'Union sont déterminantes pour aider les autorités nationales à gérer les frontières extérieures, à lutter contre la criminalité et le terrorisme et à réduire l'immigration irrégulière. Afin de maximiser cette valeur ajoutée de l'Union, les informations susmentionnées doivent être complètes, précises et fiables. Actuellement, les informations sont fragmentées, complexes et difficiles à utiliser.

Pour remédier à ces failles[6], conformément à la communication de la Commission d'avril 2016, les travaux ont été axés sur trois domaines: optimiser les avantages des systèmes d'information existants, concevoir de nouveaux systèmes, complémentaires, visant à combler les lacunes et améliorer l'interopérabilité des systèmes d'information.

1. Vers l'interopérabilité des systèmes d'information

Premièrement, les mesures proposées aideront les agents sur le terrain à **exploiter de façon optimale les données existantes**. Un *portail de recherche européen* procurera un «guichet unique»; il permettra d'effectuer des recherches simultanées dans plusieurs systèmes d'information de l'Union[7] ainsi que dans les systèmes de données pertinents d'Europol et d'Interpol, conformément aux droits d'accès des utilisateurs. Les agents sur le terrain auront ainsi un accès efficace, rapide et aisé aux données dont ils ont besoin pour accomplir leur travail et ne seront plus confrontés à la question complexe de savoir quelle base de données consulter dans une situation donnée.

Deuxièmement, comme elles sont fondées sur l'utilisation des données biométriques, les mesures proposées permettront aux autorités nationales **de détecter les identités multiples et de lutter contre la fraude à l'identité**. Un *service partagé de mise en correspondance de données biométriques* permettra de rechercher et de comparer des données biométriques dans

---

4 http://www.consilium.europa.eu/media/21597/bratislava-implementation-report.pdf

5 Voir l'Eurobaromètre spécial 464b intitulé «L'attitude des Européens à l'égard de la sécurité», publié le 12 décembre 2017: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/1569.

6 COM(2016) 205 final du 6.4.2016.

7 Le système d'information Schengen, Eurodac, le système d'information sur les visas, le futur système d'entrée/de sortie, le système européen proposé d'information et d'autorisation concernant les voyages et le système européen proposé d'information sur les casiers judiciaires englobant les ressortissants de pays tiers.

plusieurs systèmes centraux[8], tandis qu'un *répertoire commun de données d'identité* contiendra les données d'identité biographiques et biométriques partagées des ressortissants de pays tiers présents dans les systèmes d'information de l'Union[9]. Sur la base de ces deux composantes de l'interopérabilité, un *détecteur d'identités multiples* vérifiera si les données relatives à une identité demandée existent dans plus d'un des systèmes qui y sont connectés[10]. Chaque fois que les agents des services d'immigration et des services d'asile enregistrent une personne dans les systèmes d'information de l'Union, ou lorsque les policiers et les garde-frontières contrôlent l'identité d'une personne dans ces systèmes, ils seront informés si la personne est déjà connue sous une autre identité ou si elle utilise plusieurs identités. Ce détecteur permettra de combler les lacunes actuelles et de fermer les angles morts que les terroristes et autres criminels cherchent à exploiter en se dissimulant derrière de fausses identités ou plusieurs identités.

Troisièmement, les mesures proposées permettront aux policiers de mener des **contrôles d'identité rapides et efficaces sur leur territoire**. Lors de ces contrôles, les policiers auront accès aux données d'identité des ressortissants de pays tiers dont les données sont enregistrées dans les systèmes d'information de l'Union, ce qui permettra l'identification correcte et la détection des identités multiples. Ainsi, les contrôles sur le territoire des États membres seront nettement plus efficaces, également conformément à la recommandation de la Commission relative à des contrôles de police proportionnés et à la coopération policière dans l'espace Schengen[11].

Pour compléter ces composantes de l'interopérabilité, la Commission propose par ailleurs **de faciliter et de rationaliser l'accès des autorités répressives** aux systèmes de services non répressifs en introduisant une nouvelle approche de consultation des données, qui compte deux étapes. En vertu des règles actuelles, les autorités répressives peuvent déjà consulter des systèmes d'information de services non répressifs à des fins de prévention, d'enquête, de détection ou de poursuite d'actes de terrorisme et d'autres infractions pénales graves. Cependant, les systèmes concernés sont soumis à différentes conditions d'accès et garanties, et certaines des règles actuelles entravent l'efficacité de l'utilisation légitime des systèmes par ces autorités. Dans le cadre de la nouvelle approche de consultation des données en deux temps, un agent des services répressifs commencerait par contrôler en parallèle tous les systèmes stockant des données dans le *répertoire commun de données d'identité* afin de savoir si des informations sur la personne recherchée existaient dans un système. Afin de garantir la protection des données, la seule réponse serait «*concordance/non-concordance*». L'agent n'aurait accès aux données d'aucun système; il serait surtout informé de l'existence éventuelle de ces données et du système qui les contiendrait. Dans un deuxième temps, l'agent pourrait ensuite demander un accès complet au(x) système(s) d'information ayant donné une concordance, en formulant une demande d'accès individuelle pour chaque système concerné conformément aux différentes règles établies pour chacun de ces systèmes. Comme c'est le

[8] Le système d'information Schengen, Eurodac, le système d'information sur les visas, le futur système d'entrée/de sortie et le système européen proposé d'information sur les casiers judiciaires englobant les ressortissants de pays tiers.

[9] Eurodac, le système d'information sur les visas, le futur système d'entrée/de sortie, le système européen proposé d'information et d'autorisation concernant les voyages et le système européen proposé d'information sur les casiers judiciaires englobant les ressortissants de pays tiers.

[10] Le système d'information Schengen, Eurodac, le système d'information sur les visas, le futur système d'entrée/de sortie, le système européen proposé d'information et d'autorisation concernant les voyages et le système européen proposé d'information sur les casiers judiciaires englobant les ressortissants de pays tiers.

[11] C(2017) 3349 final du 12.5.2017.

cas actuellement, l'agent devrait justifier la nécessité d'accéder au système, conformément aux droits d'accès de ce système d'information et aux principes de limitation des finalités. L'accès complet resterait soumis à une autorisation préalable délivrée par une autorité désignée et continuerait à exiger un identifiant d'utilisateur et un login spécifiques. Une fois que cette approche de consultation des données en deux temps s'appliquera, il ne sera plus nécessaire d'effectuer une recherche préalable dans les bases de données nationales ou de lancer une recherche préalable dans le système automatisé d'identification des empreintes digitales d'autres États membres au titre de la décision 2008/615/JAI («vérification Prüm»).

Les propositions sur l'interopérabilité **respectent et promeuvent les droits fondamentaux, et notamment le droit à la protection des données**. Grâce à l'instauration du nouveau cadre général de protection des données à caractère personnel dans l'Union et aux progrès considérables accomplis dans les domaines technologiques et de la sécurité informatique, le principe de limitation des finalités peut être plus facilement mis en œuvre en ce qui concerne l'accès aux données stockées et leur utilisation, dans le strict respect de la Charte des droits fondamentaux et de la jurisprudence récente de la Cour de justice de l'Union européenne. Les mesures proposées ne déboucheront pas sur l'interconnectivité des différents systèmes. Chaque système conservera sa limitation à ses finalités spécifiques, ses règles d'accès et ses règles en matière de conservation des données. Les mesures proposées n'entraîneront pas non plus de collecte de nouvelles données. Elles représentent une solution ciblée et intelligente exploitant de façon optimale les informations existantes dans les systèmes de l'Union.

Les propositions législatives sont le fruit d'un **processus inclusif et transparent** qui a débuté avec la communication de la Commission intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité» d'avril 2016, qui a fait l'objet d'un suivi par un groupe d'experts de haut niveau[12] chargé de résoudre les problèmes juridiques, techniques et opérationnels découlant des différentes options afin de parvenir à l'interopérabilité.

Les propositions législatives comprennent des dispositions détaillées concernant les **modifications nécessaires des instruments juridiques** qui sont actuellement des textes stables adoptés par les colégislateurs, à savoir le code frontières Schengen, le règlement sur le système d'entrée/de sortie et les instruments juridiques régissant le système d'information sur les visas. Les autres instruments couverts[13] sont en cours de négociation au Parlement

[12] Ce groupe a été institué par la décision 2016/C 257/03 de la Commission du 17.6.2016. Il a réuni des experts des États membres et des pays Schengen associés, ainsi que des agences de l'UE: eu-LISA, Europol, Bureau européen d'appui en matière d'asile, Agence européenne de garde-frontières et de garde-côtes et Agence des droits fondamentaux. Le Coordinateur de l'UE pour la lutte contre le terrorisme et le Contrôleur européen de la protection des données ont participé en tant que membres à part entière. Des représentants du secrétariat de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen et du secrétariat général du Conseil étaient présents en tant qu'observateurs. Le rapport final du groupe d'experts peut être consulté à l'adresse suivante: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1. Ses annexes comprennent la synthèse d'un rapport de l'Agence des droits fondamentaux ainsi que des déclarations du Contrôleur européen de la protection des données et du Coordinateur de l'UE pour la lutte contre le terrorisme.

[13] Les propositions de règlements relatifs au système européen d'information et d'autorisation concernant les voyages et au système d'information sur les casiers judiciaires pour les ressortissants de pays tiers, les règlements concernant Eurodac, le système d'information Schengen et eu-LISA, ainsi que les modifications corrélatives de la proposition de règlement relatif au système européen d'information et d'autorisation concernant les voyages qui concernent le règlement sur l'Agence européenne de garde-frontières et de garde-côtes.

européen et au Conseil. Pour ces instruments, il n'est donc pas possible d'exposer les modifications nécessaires à ce stade. La Commission présentera ces modifications pour chacun de ces instruments dans un délai de deux semaines à compter de l'accord politique sur les différents projets de règlement. Elle invite les colégislateurs à trouver rapidement un accord dans le cadre des négociations en cours sur ces instruments.

2. Concevoir de nouvelles actions complémentaires visant à combler les lacunes

Outre les nouvelles propositions relatives à l'interopérabilité susmentionnées, il est indispensable de continuer à progresser pour combler les déficits d'information actuels que la Commission a recensés dans sa communication d'avril 2016 en ce qui concerne les ressortissants de pays tiers qui se rendent dans l'espace Schengen. Les textes finaux du règlement relatif au **système d'entrée/de sortie**[14] (EES) et du règlement modifiant le code frontières Schengen afin de l'aligner sur l'EES[15] ont été adoptés par les colégislateurs à la fin du mois de novembre et entreront en vigueur à la fin 2017. Par la suite, le développement du système commencera en 2018, afin que celui-ci soit pleinement opérationnel pour 2020.

Un autre manque d'informations, qui concerne les ressortissants de pays tiers n'ayant pas besoin de visa, a été abordé dans la proposition législative de la Commission de novembre 2016 visant à créer un nouveau système informatique à grande échelle, le **système européen d'information et d'autorisation concernant les voyages (ETIAS)**. Le Conseil a approuvé son orientation générale en juin 2017 et le mandat de négociation du Parlement européen a été confirmé le 25 octobre 2017. Les négociations du trilogue ont débuté le même jour et se sont poursuivies le 16 novembre 2017 et le 29 novembre 2017. Le prochain trilogue politique est prévu pour le 12 décembre 2017. La Commission invite les deux colégislateurs à parvenir à un accord politique sur le dossier d'ici à la fin 2017, conformément aux conclusions du Conseil européen de décembre 2016 et à la déclaration commune.

3. Optimiser les avantages des systèmes d'information existants

a) Travaux législatifs en cours visant à renforcer les systèmes d'information existants

Dans le cadre de ses efforts déployés pour optimiser le potentiel des systèmes d'information existants de l'Union, la Commission a adopté en décembre 2016 trois propositions législatives visant à renforcer le **système d'information Schengen (SIS)**[16]. Celles-ci comportent des mesures essentielles pour intensifier la lutte contre le terrorisme, comme l'introduction d'une obligation pour les États membres de créer une alerte dans le SIS si une personne est recherchée en rapport avec une infraction terroriste. Les débats au Parlement européen et au Conseil ont aussi porté sur la nécessité d'échanger avec Europol les informations sur les infractions terroristes présentes dans le SIS. Une modification proposée consiste à permettre à Europol et aux États membres d'échanger des informations supplémentaires sur les concordances dans le SIS liées au terrorisme, et à permettre à Europol de contrôler les informations sur les alertes nouvellement créées et les concordances correspondantes par recoupement avec ses bases de données et ses fichiers de travail analytiques. Les négociations du Parlement européen et du Conseil sur ces propositions ont commencé le 16 novembre 2017. Compte tenu de l'importance de ces propositions, la Commission prie instamment les colégislateurs de parvenir à un accord à ce sujet d'ici au début 2018.

[14] Règlement (UE) 2017/2226 du 30.11.2017.
[15] Règlement (UE) 2017/2225 du 30.11.2017.
[16] COM(2016) 881 final, COM(2016) 882 final et COM(2016) 883 final du 21.12.2016.

Parallèlement, comme prévu depuis 2016, les travaux continuent en vue de renforcer le SIS, avec l'introduction d'un **système automatisé d'identification des empreintes digitales (AFIS)**. Ce système permettra aux utilisateurs finaux du SIS (comme les policiers et les garde-frontières) d'effectuer des recherches dans le SIS sur la base des données dactyloscopiques, afin de pouvoir identifier de façon fiable les individus, y compris ceux qui se déplacent sous une fausse identité. Neuf États membres se sont portés volontaires pour participer à la première phase du déploiement de l'AFIS, qui devrait débuter en mars 2018. Le déploiement complet dans tous les États membres utilisant le SIS devrait être achevé dans le courant 2018.

En ce qui concerne la proposition législative visant à renforcer le système **Eurodac**[17], les trilogues sont en cours. Eurodac est l'un des systèmes d'information qui seront couverts par les composantes de l'interopérabilité. Il est donc important que les colégislateurs parviennent rapidement à un accord sur ce dossier. Dans la communication intitulée «Contribution de la Commission à la réunion des dirigeants sur la voie à suivre concernant les dimensions interne et externe de la politique migratoire»[18], la Commission appelle à adopter la proposition pour mars 2018.

Afin de continuer à restreindre la marge de manœuvre des terroristes et des criminels, la Commission a présenté le 29 juin 2017 une proposition supplémentaire destinée à faciliter l'échange d'informations extraites des casiers judiciaires des ressortissants de pays tiers dans l'Union par l'intermédiaire du **système européen d'information sur les casiers judiciaires (ECRIS)**[19]. Le 8 décembre 2017, le Conseil «Justice et affaires intérieures» a adopté une orientation générale sur la proposition de directive[20] et la proposition de règlement. Les discussions en trilogue entre les colégislateurs pourraient commencer dès que le Parlement européen aura adopté son mandat de négociation sur les deux propositions relatives à l'ECRIS. La Commission invite les deux colégislateurs à trouver rapidement un accord sur ces propositions.

Le 29 juin 2017, la Commission a adopté une proposition visant à réviser le **mandat de l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice**[21]. L'Agence devrait se voir confier la mission de contribuer au développement de l'interopérabilité entre les systèmes d'information à grande échelle et, dans cette perspective, la proposition a pour objectif de réviser le règlement portant création de l'Agence afin de tenir compte des recommandations résultant de l'évaluation de l'Agence, ainsi que d'améliorer son fonctionnement et de renforcer et d'accroître son rôle afin de faire en sorte qu'elle puisse répondre aux problèmes actuellement rencontrés au niveau de l'Union. Elle vise également à insérer les modifications découlant de l'évolution de la situation politique, juridique ou factuelle et, en particulier, à tenir compte du fait que de nouveaux systèmes vont être confiés à l'Agence. La commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen a adopté son mandat de négociation le 7 décembre 2017, et le Conseil a convenu d'une orientation générale le même jour.

---

17 COM(2016) 272 final du 4.5.2016.
18 COM(2017) 820 final du 7.12.2017.
19 COM(2017) 344 final du 29.6.2017.
20 COM(2016) 7 final du 19.1.2016.
21 COM(2017) 352 final du 29.6.2017.

b) Garantir la mise en œuvre intégrale des systèmes d'information existants

La **directive relative aux données des dossiers passagers (PNR)**[22] constitue un outil essentiel de la lutte contre le terrorisme et la criminalité organisée. Bien que tous les États membres poursuivent leurs travaux afin d'assurer la pleine mise en œuvre de la directive avant l'échéance du 25 mai 2018, il subsiste, un an après le plan de mise en œuvre des PNR de novembre 2016,[23] des différences marquées entre les États membres en ce qui concerne les progrès accomplis dans la mise en place de leurs systèmes PNR nationaux. L'expiration du délai de transposition approche rapidement. Il est dès lors impératif d'intensifier ces efforts pour respecter l'échéance du 25 mai 2018. Il est particulièrement important de mettre en place des procédures et des canaux de communication permettant aux unités nationales d'information passagers (UIP) de partager toutes les données PNR pertinentes avec les UIP des autres États membres et avec Europol. Cet outil essentiel de l'Union en matière de sécurité ne réalisera pleinement son potentiel que lorsque tous les États membres auront mis en place des systèmes PNR fonctionnels et seront effectivement en mesure d'échanger des données entre eux et avec Europol. Au 15 novembre 2017, la situation était la suivante:

- sept États membres disposent déjà des capacités juridiques et techniques pour collecter et traiter les données PNR. Toutefois, la plupart de ces États membres doivent encore adapter leur base juridique respective pour être en parfaite conformité avec les exigences de la directive PNR;
- treize États membres sont à un stade intermédiaire de mise en œuvre. Dans quatre de ces États membres, les UIP sont en place et dotées des moyens nécessaires, mais elles ne procèdent pas à la collecte et au traitement de données PNR réelles en raison de l'absence d'une base juridique autorisant la collecte de données à caractère personnel. Dans les neuf autres États membres, la conception et la mise en place des UIP se trouvent à des stades variés, tout comme le développement de la solution technique à utiliser pour traiter les données PNR conformément aux exigences de la directive PNR, tandis que le dialogue avec les transporteurs aériens est toujours en cours. Toutefois, certains de ces neuf États membres ont déjà adopté une législation sur les PNR;
- sept États membres se trouvent à un stade trop peu avancé du processus de mise en œuvre et doivent encore définir l'architecture administrative de leurs UIP, soumettre la législation pertinente à leur parlement respectif, commencer à installer la solution technique devant être utilisée par les UIP ou entamer la procédure visant à garantir la connectivité avec les transporteurs aériens.

La Commission continue à soutenir les États membres dans leurs efforts visant à mettre en œuvre la directive en temps utile. La sixième réunion sur la mise en œuvre de la directive PNR a eu lieu le 3 octobre 2017; elle a permis aux experts des États membres d'échanger entre eux et avec la Commission des informations sur l'état d'avancement du processus de mise en œuvre, ainsi que de procéder à un échange d'enseignements, de bonnes pratiques et d'expérience pratique.

Une assistance financière a été mise à disposition par l'intermédiaire des programmes nationaux et des actions de l'Union dans le cadre du Fonds pour la sécurité intérieure-Police

[22] Directive (UE) 2016/681 du 27.4.2016.
[23] SWD(2016) 426 final du 28.11.2016.

(FSI-Police) afin d'aider à mettre en place des UIP fonctionnelles au niveau national et de permettre les échanges de données PNR conformément à la directive PNR[24].

Les travaux continuent par ailleurs en vue de la mise en œuvre intégrale des **décisions de Prüm**[25] pour l'échange des données dactyloscopiques, des données ADN et des données relatives à l'immatriculation des véhicules. Si la plupart des États membres ont enregistré des progrès à cet égard, la Commission a dû utiliser ses pouvoirs en matière d'infractions. Elle a envoyé des avis motivés à la Croatie, à l'Irlande et à l'Italie le 18 mai 2017, et à la Grèce le 5 octobre 2017. Parallèlement, la Commission continue à aider les États membres en finançant la mise en œuvre des programmes nationaux dans le cadre du FSI-Police. La Commission a mis à la disposition de ces programmes nationaux pour 2017 une enveloppe supplémentaire de 22 millions d'EUR, qui pourra être utilisée pour la mise en œuvre des décisions de Prüm.

c) Aider à mieux utiliser les systèmes d'information existants

Outre qu'elle s'attache à renforcer les systèmes existants et à garantir leur mise en œuvre intégrale, la Commission déploie aussi d'importants efforts pour aider à mieux utiliser les systèmes d'information existants. Dans le cadre du **mécanisme d'évaluation de Schengen**[26], des évaluations sur place de la mise en œuvre du SIS sont menées dans les États membres tous les cinq ans par des experts des États membres et de la Commission européenne dans ce domaine. En 2017, des visites d'évaluation ont été effectuées au Danemark, en Islande, en Suède, au Portugal, en Espagne, en Croatie, en Norvège et au Royaume-Uni. Les problèmes de mise en œuvre constatés lors des évaluations sont traités au moyen de recommandations formelles adressées par le Conseil à l'État membre concerné. Le suivi des recommandations précédentes est également vérifié lors des contrôles réalisés par les équipes d'évaluation au cours des visites sur place. La Commission tiendra compte des conclusions des évaluations de Schengen réalisées jusqu'à présent en ce qui concerne l'utilisation du SIS pour élaborer une liste **de bonnes pratiques et d'enseignements tirés** apportant une valeur ajoutée dans l'ensemble des États membres afin d'améliorer l'utilisation des systèmes d'information existants, pour en débattre avec les États membres.

Pour continuer à améliorer les flux d'information, les États membres devraient faire pleinement usage de solutions techniques permettant d'améliorer le partage d'informations avec Europol. L'automatisation du processus de téléchargement des données sur le **système d'information d'Europol** aux fins des contrôles croisés peut nettement améliorer le partage d'informations pertinentes et actualisées avec Europol et avec d'autres États membres. Les «chargeurs de données» sont des outils techniques permettant d'automatiser ce processus de téléchargement des données. Europol a développé de tels chargeurs de données afin de

[24] Comme annoncé dans le cinquième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, l'autorité budgétaire a renforcé le budget 2017 de l'Union à hauteur de 70 millions d'EUR au titre du FSI-Police pour financer des actions dans le domaine des PNR au cours de la période 2017-2020. Ces ressources supplémentaires ont été allouées en complément des programmes nationaux des États membres selon la clé de répartition du Fonds. En ce qui concerne les actions de l'Union, l'actuel projet «PIU.net», sélectionné à la suite d'un appel à propositions 2016 dans le cadre du FSI-Police (avec une subvention maximale de 3,78 millions d'EUR), vise à fournir une solution technique afin de faciliter l'échange de données PNR entre les UIP des États membres. En novembre 2017, la Commission a publié un appel à propositions, d'un budget total de 1,5 million d'EUR, pour des actions de formation, de sensibilisation et de renforcement des capacités ciblant le personnel travaillant pour les UIP.

[25] Décisions 2008/615/JAI et 2008/616/JAI du Conseil du 23.6.2008.

[26] Règlement (UE) nº 1053/2013 du Conseil du 7.10.2013.

permettre aux États membres d'améliorer leur efficacité en ce qui concerne le téléchargement, la mise à jour et la suppression des données dans le système d'information d'Europol. Ces chargeurs de données sont déjà utilisés dans plusieurs États membres[27]. Afin de rendre les données d'Europol accessibles à un groupe beaucoup plus large de policiers, un projet pilote sur l'utilisation de **QUEST**, une interface système qui permet l'intégration automatique des demandes de données d'Europol émanant des systèmes d'information policière nationaux, est en cours dans cinq États membres (Espagne, Estonie, Finlande, Grèce et Pologne). Cette interface devrait être opérationnelle au début de 2018, après la validation par le service européen de la protection des données et les essais opérationnels des États membres.

La Commission a commandé une étude afin d'évaluer l'exhaustivité et la conformité des mesures prises par les États membres pour transposer la **décision-cadre suédoise**[28] qui fournit un cadre juridique commun aux fins de l'échange d'informations entre les services répressifs des États membres. Les résultats sont attendus au cours du premier trimestre 2018 et la Commission les examinera afin de déterminer si de nouvelles mesures sont nécessaires. Le 3 octobre 2017, la Commission a envoyé un avis motivé au Luxembourg pour défaut de communication des mesures nationales prises pour mettre en œuvre cette décision.

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

Outre les actions destinées à combler les déficits d'information et à renforcer les systèmes d'information, les travaux se sont poursuivis dans plusieurs autres domaines de l'union de la sécurité.

1. Mesures visant à améliorer la protection et la résilience face au terrorisme et à la criminalité

À la suite de l'adoption du **plan d'action de la Commission relatif à la protection des espaces publics**[29], la première réunion du Réseau de sécurité pour la protection des espaces publics à haut risque a eu lieu les 14 et 15 novembre 2017. L'unité de la Guardia Civil espagnole chargée de la protection des lieux à haut risque a accueilli cette première conférence à son siège de Logroño, en Espagne. Ce nouveau réseau vise à soutenir le développement de nouvelles tactiques visant à mieux protéger les espaces publics à haut risque. Par ailleurs, la première réunion du Forum des exploitants d'espaces publics aura lieu à Bruxelles le 20 décembre 2017, et une réunion thématique consacrée aux locations de voitures suivra le lendemain 21 décembre 2017. Les préparatifs ont également débuté en vue d'une réunion avec les maires de villes européennes qui sera organisée en coopération avec le Comité des régions au printemps de l'année prochaine.

En réaction à une augmentation du niveau de la menace dans le domaine des transports, et notamment dans les réseaux ferroviaires, certains États membres ont renforcé leurs mesures de sécurité afin de protéger les transports ferroviaires. Ces mesures ont été appliquées de manière fragmentée, ce qui met en évidence la nécessité d'une meilleure coordination dans le domaine de la sécurité ferroviaire. La Commission a donc annoncé, dans son programme de

[27] Par exemple: la Belgique, la Finlande, la Pologne, le Royaume-Uni et, depuis peu, la République tchèque et la Croatie.
[28] Décision-cadre 2006/960/JAI du Conseil du 18.12.2006.
[29] COM(2017) 612 final du 18.10.2017.

travail pour 2018, son intention d'œuvrer à l'adoption de nouvelles mesures destinées à améliorer la **sécurité des passagers dans les transports ferroviaires**.

Dans le domaine de la recherche, l'événement **Recherche en matière de sécurité** 2017 a été organisé conjointement par la Commission européenne et la Présidence estonienne à Tallinn les 14 et 15 novembre 2017. Il a été largement reconnu que des efforts supplémentaires étaient nécessaires pour combler le fossé existant entre les résultats de la recherche et les produits et services permettant de lutter efficacement contre différentes menaces pour la sécurité, telles que le terrorisme, la cybercriminalité et les catastrophes naturelles. Associer l'industrie, le monde universitaire, les pouvoirs publics et les praticiens dans un processus de cocréation permettrait de regrouper les acteurs de l'offre (l'industrie) et ceux de la demande (les utilisateurs finaux) afin de consolider les exigences futures et de convenir d'éventuelles solutions pouvant avoir un effet concret et faciliter le travail des spécialistes de la sécurité dans un proche avenir. La Commission envisagera des solutions pour faire progresser ces idées.

2. S'attaquer aux moyens d'action des terroristes

Les discussions avec les colégislateurs se sont poursuivies sur la proposition de la Commission visant à modifier la **quatrième directive antiblanchiment**, afin de contribuer à la lutte contre le financement du terrorisme. La Commission invite de nouveau les colégislateurs à achever rapidement les négociations législatives sur ce dossier prioritaire et à dégager un compromis qui renforce l'ensemble actuel de règles de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme, notamment en améliorant la transparence des informations relatives aux bénéficiaires effectifs.

En outre, la proposition de **directive visant à harmoniser la définition et les sanctions pénales en matière de blanchiment de capitaux**[30] permettra de surmonter les obstacles à la coopération transfrontière dans le domaine de la lutte contre le blanchiment de capitaux. Le Conseil a adopté une orientation générale le 8 juin 2017. Le Parlement européen ayant adopté sa position le 11 décembre 2017, les discussions interinstitutionnelles pourront bientôt débuter en vue de parvenir à un accord au cours du premier semestre 2018.

Les travaux se poursuivent sur d'éventuelles mesures visant à améliorer l'accès transfrontière des autorités répressives aux données financières pertinentes susceptibles de procurer les pistes nécessaires sur les activités terroristes, comme annoncé dans le programme de travail de la Commission pour 2017. Le 20 novembre 2017, la Commission a organisé une réunion de parties prenantes de haut niveau avec les États membres et les organes de l'Union afin d'évaluer la nécessité de **mesures supplémentaires visant à faciliter l'accès transfrontière aux informations financières à des fins de lutte contre le terrorisme**. Au cours de cette réunion, les États membres ont pris note du fait que les différentes mesures existantes, en cours ou prévues pourraient mettre en place les outils et solutions nécessaires, notamment la **décision d'enquête européenne**[31], la **directive antiblanchiment**[32] (y compris les

30 COM(2016) 826 final du 21.12.2016.
31 Directive 2014/41/UE du 3.4.2014.
32 Directive (UE) 2015/849 du 20.5.2015.

modifications proposées[33], en cours de négociation) et un prochain appel à propositions destiné à soutenir des projets de lutte contre le financement du terrorisme[34].

La proposition de révision de la quatrième directive antiblanchiment envisage la création obligatoire de **registres nationaux centralisés des comptes bancaires et de systèmes de recherche**, auxquels les cellules de renseignement financier et les services de lutte contre le blanchiment de capitaux auraient accès. La Commission évalue actuellement l'impact des options stratégiques pertinentes en vue de proposer, au printemps 2018, une directive visant à donner aux autorités répressives et aux bureaux de recouvrement d'avoirs l'accès aux registres et aux systèmes de recherche de données dans leur propre État membre.

Elle est aussi en train d'élaborer des initiatives visant à améliorer la **coopération entre les cellules de renseignement financier**, ainsi que leur coopération avec les autorités répressives. Ces travaux devraient également s'achever au printemps 2018. Parallèlement, et en vue de préparer les initiatives nécessaires pour faciliter l'accès transfrontière des autorités répressives aux données financières, la Commission continuera à évaluer la nécessité, la faisabilité technique et la proportionnalité de toute mesure supplémentaire.

La Commission a adopté aujourd'hui un rapport sur l'évaluation du règlement 258/2012 **sur les autorisations d'exportation, ainsi que sur des mesures concernant l'importation et le transit d'armes à feu**. Elle conclut que ce règlement reste nécessaire, mais que son efficacité est limitée par le manque de précision de certaines de ses dispositions, ainsi que par la complexité de l'interaction avec d'autres instruments du droit de l'Union. La Commission rencontrera les experts nationaux à la fin de janvier 2018 pour procéder à des échanges de vues sur ces conclusions. Elle organisera aussi plusieurs réunions afin d'aller de l'avant sur certains défis (statistiques en matière de saisies, balistique et coopération avec les pays des Balkans occidentaux).

Le 18 octobre 2017, la Commission a émis une **recommandation énonçant des mesures immédiates pour empêcher tout usage détourné de précurseurs d'explosifs**, dans laquelle elle prie instamment les États membres de prendre d'urgence plusieurs mesures visant à renforcer la protection face à l'utilisation d'explosifs artisanaux à des fins terroristes et à aider à la réalisation des objectifs du règlement 98/2013 sur les précurseurs d'explosifs. Les 12 et 13 décembre 2017, une réunion du comité permanent sur les précurseurs permettra de faire le point sur les progrès accomplis par les États membres dans la mise en œuvre de cette recommandation. Le 6 décembre 2017, la Commission a décidé de clôturer la procédure d'infraction contre la France concernant le non-respect du règlement 98/2013, étant donné que la France a informé la Commission de la pleine mise en œuvre du règlement. Parallèlement, la Commission a entrepris de **réviser le règlement 98/2013** en vue de renforcer les restrictions et les contrôles sur la vente, la détention, l'introduction et l'utilisation des précurseurs d'explosifs, d'améliorer la capacité des opérateurs économiques et des autorités compétentes et répressives des États membres de détecter et de prévenir les cas d'usage détourné, et d'assurer un niveau d'uniformité plus élevé dans l'application du règlement dans les États membres. L'analyse d'impact sur les différentes options possibles dans le cadre de la révision du règlement sera conclue au printemps 2018.

---

33 COM(2016) 450 final du 5.7.2016.

34 http://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/home/call-fiche/isfp-call-fiche-2017-ag-terfin_en.pdf

3. Cybersécurité et justice pénale dans le cyberespace

Dans ses conclusions du 19 octobre 2017[35], le Conseil européen a pris acte des initiatives relevant du **train de mesures en matière de cybersécurité**[36]. Le 20 novembre 2017, le Conseil a adopté des conclusions sur la communication conjointe au Parlement européen et au Conseil intitulée «*Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide*»[37]. Un plan d'action visant à mettre en œuvre ces conclusions du Conseil sera adopté par le Conseil des affaires générales le 12 décembre 2017.

Les discussions avec le Conseil sur la proposition de «**règlement sur la cybersécurité**» (couvrant le nouveau mandat de l'ENISA et le cadre de certification)[38] ont débuté. La **proposition législative concernant les moyens de paiement autres que les espèces** a été présentée au Parlement européen et au Conseil et son examen est en cours. La Commission prie instamment le Parlement européen de commencer ses travaux dès lors que le rapporteur a été nommé le 13 novembre 2017. En ce qui concerne la mise en œuvre de la directive sur la sécurité des réseaux et de l'information (SRI)[39], une réunion du groupe de coopération a eu lieu le 28 novembre. Ce groupe a adopté deux de ses éléments livrables concernant des éléments essentiels de la directive: des lignes directrices pour l'identification des opérateurs de services essentiels[40] concernant les bonnes pratiques liées aux critères définissant le caractère critique d'un opérateur, et des lignes directrices sur les mesures de sécurité donnant un aperçu des critères de référence pour les mesures devant être appliquées afin de sécuriser les réseaux et systèmes d'information[41]. Un troisième élément livrable, qui porte sur les exigences en matière de notification et présentera les circonstances dans lesquelles les opérateurs de services essentiels seront tenus de notifier un incident, devrait être bientôt adopté par procédure écrite. Le groupe a entamé des discussions sur son premier programme de travail (2018-2020), lequel devrait être adopté d'ici à février 2018.

La Commission s'est engagée dans son onzième rapport sur l'union de la sécurité[42] à évaluer la nécessité de doter Europol [en particulier le Centre européen de lutte contre la cybercriminalité (EC3)] de ressources supplémentaires afin de permettre à l'EC3 d'aider les États membres à s'attaquer aux problèmes liés au **chiffrement dans les enquêtes pénales**. Compte tenu des économies d'échelle rendues possibles par la fourniture de capacités au niveau de l'Union (par rapport à des solutions individuelles au niveau des États membres), la Commission a également pris note de la nécessité de renforcer le soutien dans ce domaine, comme demandé par le Conseil «Justice et affaires intérieures» les 7 et 8 décembre 2017. L'évaluation des besoins spécifiques de ressources supplémentaires est en cours et la Commission rendra compte, dans son prochain rapport sur l'union de la sécurité, des fonds mis à disposition à cette fin. Permettre aux services répressifs des États membres d'utiliser les instruments fournis par l'EC3 dans un domaine en perpétuelle mutation procurera le meilleur retour sur investissement et garantira que les capacités européennes restent adaptées aux défis, sans interdire, limiter ou affaiblir le chiffrement.

---

35 http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/fr/pdf
36 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
37 JOIN(2017) 450 final du 13.9.2017.
38 COM(2017) 477 final/2 du 4.10.2017.
39 Directive (UE) 2016/1148 du 6.7.2016.
40 «Partage de bonnes pratiques concernant les critères définissant le caractère critique d'un opérateur conformément à l'article 5, paragraphe 2, de la directive au moyen de lignes directrices».
41 «Document de référence relatif aux mesures de sécurité pour les opérateurs de services essentiels».
42 COM(2017) 608 final du 18.10.2017.

Lors de la réunion du Conseil «Justice et affaires intérieures» des 7 et 8 décembre 2017, les États membres ont décidé de poursuivre les discussions au niveau des experts en vue de dégager une conception commune des solutions possibles en matière de **conservation des données** conformément à l'arrêt Tele2 du 21 décembre 2016. La Commission continuera à soutenir les États membres dans ce processus. La Commission considère que ce processus fait partie de sa propre évaluation des implications de l'arrêt et de ses travaux en cours visant à finaliser ses orientations sur la voie à suivre en matière de conservation des données, comme annoncé dans son programme de travail pour 2018.

Comme cela avait été annoncé précédemment, la Commission envisage de présenter une initiative législative sur les **preuves électroniques** au début 2018, afin de faciliter l'accès des services répressifs aux preuves électroniques situées dans un autre pays.

4. Lutter contre la radicalisation

Depuis le dernier rapport sur l'union de la sécurité, la Commission a poursuivi ses efforts de lutte contre la radicalisation, à la fois en ligne et hors ligne.

Le **groupe d'experts de haut niveau sur la radicalisation**, créé en juillet 2017, a poursuivi à un rythme élevé ses travaux en vue de son premier rapport intermédiaire, qui a été adopté par les membres du groupe le 24 novembre 2017. Dans ses constatations et recommandations préliminaires, le groupe a recensé plusieurs thèmes et questions transversales prioritaires, dont la radicalisation dans les prisons, les réponses locales dans un cadre associant plusieurs services, le renforcement des connaissances sur les parcours de radicalisation, les mécanismes et structures de coopération, l'éducation et l'inclusion sociale, ainsi que la dimension extérieure de la prévention. La Commission exposera son point de vue sur ces constatations et recommandations préliminaires dans le prochain rapport sur l'union de la sécurité.

La troisième réunion ministérielle du **forum de l'UE sur l'internet** a eu lieu le 6 décembre 2017 et a rassemblé les États membres, des entreprises du secteur de l'internet, Europol, des universitaires et des représentants de la société civile[43]. Les progrès réalisés dans le cadre du plan d'action visant à lutter contre les contenus à caractère terroriste en ligne ont été évalués, et cette évaluation a porté sur l'automatisation de la détection des contenus à caractère terroriste, l'amélioration des bases de données d'empreintes numériques des entreprises en vue d'enrayer la diffusion de ces contenus, le renforcement des signalements ainsi que la fourniture à la société civile des moyens d'accroître les contre-discours visant à combattre la propagande terroriste. Les entreprises du secteur de l'internet ont signalé que la base de données des contenus à caractère terroriste connus («database of hashes»), annoncée lors du forum de l'UE sur l'internet 2016 et lancée au printemps 2017, est désormais opérationnelle et a déjà recueilli plus de 40 000 empreintes numériques («hashes») de vidéos et d'images à caractère terroriste connues. Le potentiel de cet outil devrait désormais être pleinement exploité et des informations relatives au nombre et à la rapidité des suppressions résultant de la base de données d'empreintes numériques devraient être régulièrement communiquées aux membres du forum de l'UE sur l'internet. Le taux des signalements non automatisés, tels que ceux qui parviennent de l'unité de l'UE chargée du signalement des contenus sur l'internet, continue également à augmenter et les entreprises ont été invitées à accroître à la fois la rapidité des suppressions et la périodicité des rapports au forum de l'UE sur l'internet. Les plateformes internet ont indiqué qu'elles s'appuient de plus en plus sur des

[43] http://europa.eu/rapid/press-release_IP-17-5105_fr.htm

outils automatiques pour la détection des contenus à caractère terroriste[44]. Il est également important de renforcer la transparence, la cohérence et la régularité de la communication des résultats. Toutes les entreprises du secteur de l'internet doivent participer à cet effort commun et partager avec les autres plateformes les informations importantes sur les suppressions de contenus, en ayant pour priorité de toucher les entreprises nouvelles et les petites entreprises qui ne sont pas encore engagées dans cette voie et de les associer à l'initiative.

Les résultats du forum de l'UE sur l'internet serviront aussi de base à des efforts politiques à plus grande échelle concernant les contenus illégaux en ligne, et la Commission a annoncé qu'elle continuera à promouvoir la coopération avec les entreprises de médias sociaux pour détecter et supprimer les contenus à caractère terroriste et autres contenus illégaux en ligne et, si nécessaire, qu'elle proposera des mesures législatives dans le domaine de la suppression des contenus à caractère terroriste[45].

5. *Dimension extérieure*

Le 7 décembre 2017, le Conseil «Justice et affaires intérieures» a donné son feu vert à la Commission pour l'ouverture de négociations avec le Canada en vue de la conclusion d'un accord entre l'Union européenne et le Canada concernant le transfert et l'utilisation des données des dossiers passagers (données PNR) afin de se conformer à l'avis 1/15 de la Cour de justice sur l'accord UE-Canada en matière de PNR envisagé précédemment. Les négociations officielles débuteront dès que le Canada aura reçu son mandat de négociation.

Ainsi que la Commission l'a annoncé dans le rapport sur l'union de la sécurité d'octobre, elle adoptera aussi, d'ici à la fin de l'année, des recommandations au Conseil afin d'autoriser l'ouverture de négociations en vue de la conclusion de différents accords entre l'Union européenne et l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie sur l'**échange de données à caractère personnel entre Europol et les autorités compétentes de ces pays** pour lutter contre le terrorisme et les formes graves de criminalité. De tels accords renforceront davantage les capacités d'Europol de nouer un dialogue avec ces pays tiers afin de prévenir et de combattre les actes criminels qui relèvent des objectifs d'Europol.

En ce qui concerne la coopération avec les partenaires internationaux, **l'Union et les États-Unis ont tenu une réunion ministérielle «Justice et affaires intérieures»** le 17 novembre. Cette réunion a porté sur la coopération transatlantique dans le domaine de la lutte contre le terrorisme, les menaces informatiques et le trafic de drogue. En ce qui concerne la lutte contre le terrorisme, la discussion a porté spécifiquement sur l'importance d'une coopération opérationnelle et d'un échange d'informations efficace. Les deux parties ont pris acte de l'importance de la collecte, de l'utilisation et du partage des données des dossiers passagers (données PNR). La discussion a également porté sur les progrès réalisés dans la mise en œuvre des mesures communes destinées à faire face à la menace terroriste dans le secteur de l'aviation et à améliorer le niveau mondial de la sûreté aérienne. L'Union et les États-Unis ont évoqué leurs actions en matière de lutte contre le financement du terrorisme et le blanchiment de capitaux, y compris leurs efforts communs et les travaux relevant du Groupe d'action

[44] Twitter a indiqué que les trois quarts des 300 000 comptes supprimés entre janvier et juin 2017 l'avaient été avant que leur premier contenu ne soit publié. Selon YouTube, plus de 150 000 vidéos ont été retirées depuis juin 2017. Après avoir identifié un contenu terroriste, Facebook supprime 83 % des copies dans l'heure qui suit leur chargement.

[45] COM(2017) 650 final du 24.10.2017.

financière (GAFI). En ce qui concerne l'usage détourné de l'internet à des fins terroristes, les deux parties ont convenu que de nombreuses parties prenantes, dont le secteur privé et la société civile, devaient être associées aux travaux. La prochaine réunion ministérielle «Justice et affaires intérieures» entre l'Union et les États-Unis aura lieu à Sofia en mai 2018.

En ce qui concerne la sûreté de l'aviation, la Commission européenne et d'autres services de l'Union se réunissent régulièrement avec les États membres pour convenir d'une **approche intégrée visant à renforcer et hiérarchiser les efforts de renforcement des capacités dans les pays tiers**. Les actions proposées concernent des formations et des exercices sur la culture de la sécurité, le contrôle des accès, les procédures de filtrage, la certification des inspecteurs, etc. Des réunions ad hoc pour chacun des pays tiers examinés sont organisées afin de concevoir des actions adaptées à chacun de ces pays.

Dans le prolongement de la déclaration commune sur le **partenariat stratégique OTAN-UE**, le Conseil a adopté le 5 décembre un deuxième rapport sur la mise en œuvre[46]. Ce rapport présente les principaux domaines dans lesquels des progrès ont été accomplis, la cybersécurité et la lutte contre les menaces hybrides. Pour la première fois, l'Union et l'OTAN ont mené un exercice parallèle et coordonné (EU PACE17/CMX17) en septembre et octobre 2017 sur la base d'un scénario de menace hybride. Outre le rapport, 24 propositions supplémentaires ont été adoptées en vue du renforcement et de l'approfondissement ultérieurs de la coopération entre l'Union et l'OTAN. Ces nouvelles propositions couvrent tous les sept domaines de coopération définis dans la déclaration commune de Varsovie: la lutte contre les menaces hybrides; l'élargissement de la coopération opérationnelle, y compris en mer et en matière de migration; la sécurité et la défense dans le domaine informatique; les capacités de défense; la recherche et l'industrie de la défense; la réalisation d'exercices; le renforcement des capacités de défense et de sécurité, ainsi que le dialogue politique. Plusieurs de ces propositions visent à renforcer la coopération dans le domaine de la lutte contre le terrorisme. Par exemple, un atelier informel sera coorganisé au cours du premier semestre 2018 afin de développer une conception commune de la façon dont les efforts de lutte contre le terrorisme peuvent bénéficier du renforcement des capacités de défense. Sur la base de l'expérience acquise et des enseignements tirés dans le cadre de l'exercice mené en 2017, un plan sera élaboré pour la mise en œuvre d'exercices parallèles et coordonnés entre l'Union et l'OTAN en 2019 et 2020. En outre, à partir de 2018, une série de modules communs de formation et d'exercice sera progressivement mise à disposition.

IV. CONCLUSIONS

Ce rapport présente plusieurs mesures prises au niveau de l'Union pour intensifier l'échange d'informations afin de renforcer la sécurité intérieure et de mieux gérer les frontières extérieures. La proposition de règlement sur l'interopérabilité prévoit une méthode ciblée et intelligente consistant à exploiter de façon optimale les données existantes et à intégrer le principe de protection des données dès la conception. Elle constitue un changement radical dans la manière dont l'Union gère les données au service de la sécurité et des frontières extérieures, en aidant les autorités nationales à mieux faire face aux menaces transnationales et à mieux repérer les terroristes qui agissent au-delà des frontières.

[46] En réponse à la demande de rapports biannuels formulée par les ministres des deux organisations, le premier rapport sur l'état d'avancement de la mise en œuvre des propositions a été présenté aux Conseils respectifs en juin 2017. Le deuxième rapport d'étape couvrira la période juillet-décembre 2017.

Le prochain rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective devrait être adopté en janvier 2018.