COMMISSION
EUROPÉENNE

Bruxelles, le 16.5.2017
COM(2017) 261 final

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

Septième 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 septième rapport mensuel sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective; il fait état de l'évolution de la situation en ce qui concerne deux piliers principaux: d'une part, lutter contre le terrorisme et la criminalité organisée et contre les moyens sur lesquels ils s'appuient, et, d'autre part, renforcer nos défenses et notre résilience face à ces menaces. Le présent rapport est centré sur les travaux menés en vue d'atteindre l'interopérabilité des systèmes d'information aux fins de la gestion de la sécurité, des frontières et des flux migratoires, afin de renforcer l'efficacité et l'efficience de la gestion des données dans l'UE, dans le strict respect des exigences en matière de protection des données, de mieux protéger les frontières extérieures et d'accroître la sécurité intérieure pour tous les citoyens. Le présent rapport fournit également des informations actualisées sur les progrès accomplis dans des dossiers législatifs et non législatifs cruciaux.

La récente cyberattaque mondiale au moyen d'un rançongiciel qui a désactivé des milliers de systèmes informatiques a une fois de plus mis en lumière l'urgence d'un renforcement de la cyber-résilience de l'UE et de ses mesures de sécurité, devant l'augmentation exponentielle de la criminalité organisée facilitée par les technologies de l'information, constatée dans le dernier rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité[1] et soulignée dans l'évaluation de la menace que représente la grande criminalité organisée réalisée par Europol[2]. La Commission accélère ses travaux dans le domaine de la cybersécurité, notamment en procédant à une révision de la stratégie de cybersécurité de l'UE de 2013[3] comme annoncé dans l'examen à mi-parcours du marché unique numérique[4], afin d'opposer une riposte actuelle et efficace à ces menaces.

Le président Juncker, dans son discours sur l'état de l'Union de septembre 2016[5], et le Conseil européen, dans ses conclusions de décembre 2016[6], ont insisté sur l'importance de remédier aux insuffisances dont souffre actuellement la gestion des données et d'améliorer l'interopérabilité des systèmes d'information existants. Les attentats terroristes récents ont mis davantage encore en exergue cette nécessité, révélant l'urgence à rendre les systèmes d'information interopérables et à supprimer les angles morts existants qui rendent possible l'enregistrement des terroristes présumés sous différents alias dans plusieurs bases de données non reliées entre elles. Le présent rapport expose l'approche de la Commission **pour atteindre, d'ici à 2020, l'interopérabilité des systèmes d'information aux fins de la gestion de la sécurité, des frontières et des flux migratoires** afin que les garde-frontières, les agents des services répressifs y compris les agents des douanes, les agents des services de l'immigration et les autorités judiciaires disposent des informations nécessaires. Il s'inscrit dans le prolongement de la communication d'avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité» [7] et

---

1 COM(2016) 213 final du 12.4.2017.

2 https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

3 JOIN(2013) 1 final du 7.2.2013.

4 COM(2017) 228 final du 10.5.2017. Voir également le quatrième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 41 final du 25.1.2017.

5 État de l'Union 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_fr.

6 Conclusions du Conseil européen du 15.12.2016, http://www.consilium.europa.eu/fr/meetings/european-council/2016/12/20161215-euco-conclusions-final_pdf/.

7 COM(2016) 205 final du 6.4.2016.

des travaux du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité que la Commission a constitué à la suite de ladite communication.

II. DES SYSTÈMES D'INFORMATION PLUS ROBUSTES ET PLUS INTELLIGENTS

1. Communication de la Commission d'avril 2016 et mesures prises à ce jour

La communication d'avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité» recense un certain nombre de lacunes structurelles affectant les systèmes d'information:

- fonctionnalités non optimales des systèmes d'information existants;
- déficits d'information dans l'architecture de la gestion des données de l'UE;
- mosaïque complexe de systèmes d'information régis de différentes façons; et
- architecture fragmentée de la gestion des données appliquée aux contrôles aux frontières et à la sécurité, dans laquelle les informations sont stockées séparément dans des systèmes non interconnectés, ce qui donne lieu à des angles morts.

Afin de remédier à ces lacunes, **la Commission a proposé une action dans trois domaines**, soulignant que les exigences de la charte des droits fondamentaux et en particulier celles du cadre général de protection des données à caractère personnel dans l'UE guideront les travaux de la Commission.

Premièrement, la Commission a esquissé certaines options possibles pour **optimiser les avantages des systèmes d'information existants, soulignant que les États membres devaient faire pleinement usage de ces systèmes**. Par la suite, la Commission a présenté, en décembre 2016, des propositions législatives visant à renforcer le système d'information Schengen (SIS)[8] qui est actuellement l'outil le plus abouti de coopération entre les garde-frontières, les autorités douanières, les policiers et les autorités judiciaires. La Commission a également présenté, en mai 2016, une proposition législative visant à renforcer la base de données utilisée dans le domaine de l'asile et de la migration irrégulière, Eurodac[9], pour faciliter les retours et contribuer à lutter contre la migration irrégulière. En janvier 2016, la Commission a présenté une proposition législative visant à faciliter l'échange, à l'intérieur de l'Union, des casiers judiciaires de ressortissants de pays tiers, en perfectionnant le système européen d'information sur les casiers judiciaires (ECRIS)[10]. Comme annoncé[11], et à la lumière des discussions qui ont eu lieu avec les colégislateurs sur la proposition de janvier 2016, la Commission présentera, en juin 2017, une proposition supplémentaire visant à créer un système centralisé[12] afin d'identifier les ressortissants de pays tiers qui sont l'objet d'une condamnation et les États membres qui détiennent des informations les concernant.

---

8 COM(2016) 881 final du 21.12.2016, COM(2016) 882 final du 21.12.2016, COM(2016) 883 final du 21.12.2016.

9 COM(2016) 272 final du 4.5.2016.

10 COM(2016) 7 final du 19.1.2016.

11 Voir le cinquième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 203 final du 2.3.2017.

12 Lorsque les États membres recherchent des informations au sujet de la condamnation d'un ressortissant d'un pays tiers, le système centralisé les oriente vers les États membres qui pourraient détenir leur casier judiciaire.

En juin 2017, la Commission présentera également une proposition législative visant à réviser le mandat juridique de l'agence eu-LISA[13], pour étendre sa mission au développement de l'interopérabilité des systèmes d'information centralisés de l'UE pour la gestion de la sécurité, des frontières et des migrations.

Deuxièmement, la Commission a exposé les options possibles pour **concevoir de nouvelles actions qui soient complémentaires, visant à combler les lacunes dans l'architecture de la gestion des données de l'UE**. Plus précisément, la Commission a relevé d'importants déficits d'information en ce qui concerne les ressortissants de pays tiers qui se rendent dans l'espace Schengen et, au sein de ce même groupe, en ce qui concerne les ressortissants de pays tiers exemptés de l'obligation de visa entrant dans l'UE par une frontière terrestre. Actuellement, les franchissements des frontières extérieures par des ressortissants de pays tiers ne sont pas enregistrés et aucune information n'est disponible, avant leur arrivée à une frontière terrestre extérieure, sur les ressortissants de pays tiers exemptés de visa. En guise de suivi, la Commission a présenté des propositions législatives visant à mettre en place deux nouveaux systèmes d'information afin de remédier à ces lacunes importantes. En avril 2016, elle a proposé un système européen d'entrée/sortie permettant de moderniser la gestion des frontières extérieures en améliorant la qualité et l'efficacité des contrôles[14]. En novembre 2016, la Commission a proposé un système européen d'information et d'autorisation concernant les voyages (ETIAS) afin de recueillir des informations sur tous les voyageurs qui se rendent dans l'Union européenne au titre d'un régime d'exemption de l'obligation de visa, pour permettre de réaliser des vérifications préalables en matière d'immigration irrégulière et de sécurité[15].

Le troisième volet mis en exergue par la communication soulignait la nécessité d'**améliorer l'interopérabilité des systèmes d'information**. La communication indiquait que le cadre général de protection des données à caractère personnel dans l'UE et les progrès considérables accomplis dans les domaines technologique et de la sécurité informatique ouvraient la voie à l'interopérabilité de systèmes d'information nécessairement assortis de règles strictes en matière d'accès et d'utilisation, sans répercussions sur l'actuel principe de limitation des finalités. La communication présentait **quatre options** pour parvenir à une interopérabilité:

- une **interface de recherche unique** permettant d'interroger simultanément plusieurs systèmes d'information et de produire des résultats combinés sur un seul écran;
- l'**interconnexion des systèmes d'information**, qui permet aux données enregistrées dans un système d'être automatiquement consultées par un autre système;
- la mise en place d'un **service partagé de mise en correspondance de données biométriques** à l'appui de divers systèmes d'information; et
- un **répertoire commun de données d'identité** fondé sur des données d'identité alphanumériques servant à différents systèmes d'information (y compris des attributs biographiques communs tels que le nom et la date de naissance).

La Commission a amorcé une réflexion sur la façon dont les systèmes d'information dans l'Union européenne pourraient mieux contribuer à renforcer la gestion des frontières et la sécurité intérieure et a constitué un groupe d'experts de haut niveau sur les systèmes

[13] 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.
[14] COM(2016) 194 final du 6.4.2016.
[15] COM(2016) 731 final du 16.11.2016.

d'information et l'interopérabilité afin de faire progresser ces travaux (voir la section II.3 ci-dessous).

2. Avancées dans les dossiers prioritaires concernant les systèmes d'information

Les garde-frontières, les agents des services répressifs et les autorités judiciaires ont besoin, dans le cadre de leur mission, d'accéder à des données précises et complètes. **Il est donc essentiel que le Parlement européen et le Conseil progressent sur les propositions prioritaires concernant les systèmes d'information** dans le cadre du premier volet de la communication d'avril 2016. Comme indiqué précédemment, c'est la condition sine qua non pour rendre les systèmes d'information existants plus efficaces pour la gestion des frontières et de la sécurité et cela permettra de combler des lacunes importantes en établissant de nouveaux systèmes nécessaires pour sécuriser les frontières extérieures.

C'est le **système d'entrée/sortie de l'UE** qui constitue la proposition la plus avancée. Elle en est au stade du trilogue et les perspectives d'atteindre l'objectif d'une conclusion en juin 2017, fixé par le Conseil européen, sont bonnes. Les discussions techniques sur **le système européen d'information et d'autorisation concernant les voyages** (ETIAS), continuent de progresser mais les deux institutions doivent encore arrêter leurs positions de négociation. L'adoption du mandat du Conseil est prévue pour le mois de juin 2017, tandis que celle du mandat de négociation de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen est prévue pour septembre 2017. La déclaration commune sur les priorités législatives de l'Union européenne pour l'année 2017[16] a accordé un rang prioritaire à ce dossier afin d'assurer sa mise en œuvre avant la fin de 2017. La Commission continuera de soutenir les colégislateurs en vue de la réalisation de cet objectif. Les deux institutions travaillent également sur les propositions de la Commission visant à renforcer le **système d'information Schengen** (SIS). Le premier cycle de discussions sur les trois propositions au niveau du groupe de travail sera achevé sous la présidence maltaise du Conseil. Le rapporteur du Parlement européen envisage de présenter un projet de rapport à la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen d'ici à la fin du mois de juin 2017. En ce qui concerne la proposition législative visant à renforcer **Eurodac**, le Conseil a convenu, en décembre 2016, d'une approche générale partielle, tandis que la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen prévoit le vote de son rapport en mai 2017. La phase de trilogue devrait commencer immédiatement après.

3. Travaux du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité

En juin 2016, la Commission a constitué le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité. La mission de ce groupe d'experts était de se pencher sur les **aspects juridiques, techniques et opérationnels des quatre options** permettant de parvenir à l'interopérabilité, en examinant notamment l'utilité, la faisabilité technique et la proportionnalité des options disponibles et leurs conséquences sur le plan de la protection des données[17]. Le groupe d'experts a également été invité à recenser et à combler les lacunes et à pallier les déficits d'information potentiels résultant de la complexité et de la fragmentation

[16] Déclaration commune sur les priorités législatives de l'Union européenne pour l'année 2017, du 13.12.2016, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.C_.2016.484.01.0007.01.FRA&toc=OJ:C:2016:484:TOC.

[17] Décision 2016/C 257/03 de la Commission du 17.6.2016.

des systèmes d'information[18]. 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) et du secrétariat général du Conseil étaient présents en tant qu'observateurs.

La Commission se félicite du rapport final[19] du groupe d'experts de haut niveau du 11 mai 2017. Le groupe d'experts a conclu qu'**il est nécessaire et techniquement possible d'œuvrer dans le sens des trois solutions suivantes en matière d'interopérabilité** et que ces dernières pouvaient, en principe, à la fois **produire des avantages opérationnels** et être mises en œuvre **conformément aux exigences en matière de protection des données**:

- un portail de recherche européen[20];
- un service partagé de mise en correspondance de données biométriques et
- un répertoire commun de données d'identité.

Selon les membres du groupe d'experts, l'option de l'interconnectivité des systèmes devrait n'être considérée qu'au cas par cas. L'un de ces cas est l'interconnexion du système d'entrée/sortie de l'UE qui a été proposé et du système d'information sur les visas[21]. La proposition de la Commission relative au système d'entrée/sortie de l'UE prévoit que ce système consulte systématiquement et automatiquement les données contenues dans le système d'information sur les visas afin de stocker dans le système d'entrée/sortie un petit sous-ensemble de données (vignette-visa, nombre d'entrées, période de séjour) lui permettant de traiter les données sur les titulaires de visa conformément aux exigences en matière de minimisation et de cohérence des données. Le groupe d'experts a considéré que, si les progrès réalisés en ce qui concerne les trois autres solutions d'interopérabilité sont suffisants, l'interconnectivité entre les systèmes à la seule fin d'améliorer l'échange de données ne sera pas aussi nécessaire.

Le rapport final du groupe d'experts a également insisté sur **l'importance de mettre en œuvre et d'appliquer pleinement les systèmes d'information existants**. Il a également examiné le **cadre Prüm** décentralisé pour l'échange de données relatives à l'ADN, aux empreintes digitales et à l'immatriculation des véhicules[22], recommandant une étude de faisabilité du passage à une composante de routage centralisé et de l'ajout éventuel de nouvelles fonctionnalités. En ce qui concerne le système décentralisé créé par **la directive relative aux données des dossiers passagers (PNR)**[23], le groupe d'experts a recommandé

---

18 Voir le document d'orientation du groupe d'experts (juin 2016): http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24081&no=2.

19 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.

20 Le terme «interface de recherche unique» a été changé en «portail de recherche européen» afin d'éviter toute confusion avec des interfaces de recherche unique nationales qui existent dans les États membres pour les systèmes d'information nationaux.

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

22 Décision 2008/615/JAI du Conseil du 23.6.2008.

23 Directive (UE) 2016/681 du 27.4.2016.

une étude de faisabilité portant sur une composante centralisée pour les informations préalables sur les passagers et les données des dossiers passagers, en tant qu'outil de support technique visant à faciliter la connectivité avec les transporteurs aériens. Le groupe d'experts a considéré que cela renforcerait l'efficacité des unités d'information passagers une fois que les États membres auront mis en œuvre la directive de l'UE sur les données des dossiers passagers.

La Commission continuera à concentrer ses efforts sur la **mise en œuvre intégrale des systèmes d'information existants**. Il est essentiel que les États membres fassent pleinement usage des systèmes existants, en exploitant intégralement leur potentiel. La Commission continuera à fournir une aide globale, ainsi que le prévoit son plan de mise en œuvre[24], afin de contribuer à ce que les États membres mettent en œuvre la directive PNR de l'Union d'ici le mois de mai 2018. Elle collaborera étroitement avec les États membres afin d'achever le déploiement complet du cadre Prüm, en particulier avec les cinq États membres qui n'ont pas encore mis en œuvre les décisions de Prüm. Dans l'esprit des recommandations du groupe d'experts, la Commission examinera des manières de renforcer le fonctionnement et l'efficacité de ces systèmes lors de leur application par les États membres.

Le groupe d'experts a relevé des **lacunes dans les informations concernant les franchissements des frontières extérieures par des citoyens de l'UE**. Son rapport final mentionne la récente introduction des vérifications systématiques dans les bases de données pour toutes les personnes jouissant du droit de circuler librement en vertu du droit de l'Union, tant à l'entrée qu'à la sortie[25]. Il souligne que la date et le lieu de ces vérifications ne sont pas enregistrés et note que cela pourrait fournir une information utile aux services répressifs. Le groupe d'experts a dès lors recommandé une analyse plus approfondie de la proportionnalité et de la faisabilité d'étendre l'enregistrement systématique des franchissements des frontières extérieures à tous les citoyens de l'Union[26].

La Commission note que le rapport du groupe d'experts ne démontre pas la nécessité et la proportionnalité d'un enregistrement des franchissements des frontières extérieures s'appliquant à tous les citoyens de l'UE. Si des éléments nouveaux devaient montrer que cet enregistrement est nécessaire et proportionné, elle se tient prête à évaluer la nécessité de nouvelles mesures. Entre-temps, la Commission examinera la recommandation connexe du groupe d'experts tendant à rendre possible l'enregistrement des réponses positives obtenues dans le système d'information Schengen en ce qui concerne les personnes faisant l'objet d'un signalement, en tant que possibilité d'enregistrer les déplacements des citoyens de l'UE qui sont soupçonnés de terrorisme ou d'autres formes de criminalité grave.

Le groupe d'experts a également relevé des **déficits d'information concernant les visas de long séjour, les titres de séjour et les cartes de séjour**. Il a observé que les États membres ne disposaient que de moyens limités pour vérifier la validité de ces documents lorsqu'ils sont délivrés par un autre État membre, et suggéré que cela pouvait justifier d'explorer la solution d'un répertoire centralisé de l'UE contenant les informations sur les visas de long séjour, les titres de séjour et les cartes de séjour. La Commission évaluera la nécessité d'un tel répertoire, y compris sa nécessité, sa faisabilité technique et sa proportionnalité.

---

[24] SWD(2016) 426 final du 28.11.2016.

[25] Règlement (UE) 2017/458 du 15.3.2017.

[26] Le groupe d'experts a également discuté des options consistant à élargir le système d'entrée/sortie de l'UE qui a été proposé, afin d'y inclure les citoyens de l'UE ou d'étendre l'utilisation de journaux du système d'information Schengen. Ces deux options ont été écartées.

Enfin, le rapport du groupe d'experts indique que les **autorités douanières** sont un acteur-clé de la coopération interagences aux frontières extérieures. Dès lors, la Commission examine plus avant les aspects techniques, opérationnels et juridiques d'une interopérabilité avec les systèmes douaniers.

III. VERS L'INTEROPÉRABILITÉ DES SYSTÈMES D'INFORMATION

1. Objectif de la Commission pour atteindre, d'ici à 2020, l'interopérabilité des systèmes d'information

Le principal objectif est d'assurer que les garde-frontières, les agents des services répressifs, les agents des services de l'immigration et les autorités judiciaires puissent disposer des informations nécessaires pour mieux protéger les frontières extérieures et renforcer la sécurité intérieure au bénéfice de tous les citoyens. C'est pourquoi il y a lieu avant tout de veiller à ce que les différents systèmes d'information dans ce domaine fonctionnent efficacement et à ce que les propositions législatives déjà sur la table soient rapidement adoptées.

Conformément à la communication d'avril 2016 et ainsi que l'ont confirmé les conclusions et les recommandations du groupe d'experts, la Commission expose **une nouvelle approche de la gestion des données pour les frontières et la sécurité,** dans le cadre de laquelle tous les systèmes d'information centralisés de l'UE assurant la gestion de la sécurité, des frontières et des flux migratoires[27] seront interopérables dans le plein respect des droits fondamentaux, de telle sorte que:

- les systèmes puissent être interrogés simultanément en utilisant un **portail de recherche européen**, dans le plein respect des limitations de la finalité et des droits d'accès, afin de faire un meilleur usage des systèmes d'information existants, éventuellement à l'aide de règles simplifiées pour l'accès des services répressifs[28];
- les systèmes utilisent un **service partagé de mise en correspondance** permettant d'effectuer des recherches dans différents systèmes d'information contenant des données biométriques, éventuellement avec des indicateurs de concordance/non-concordance signalant le rapport avec des données biométriques connexes trouvées dans un autre système[29];

---

[27] Le système d'information Schengen, le système d'information sur les visas, Eurodac, le système proposé d'entrée/sortie de l'UE, le système européen proposé d'information et d'autorisation concernant les voyages (ETIAS), et le système européen proposé d'information sur les casiers judiciaires (ECRIS) englobant les ressortissants de pays tiers.

[28] Après avoir donné mandat à la présidence du Conseil pour ouvrir les négociations interinstitutionnelles sur le système d'entrée/sortie de l'UE le 2 mars 2017, le Comité des représentants permanents du Conseil (Coreper) a appelé la Commission à proposer un cadre global pour l'accès des services répressifs aux différentes bases de données dans le domaine de la justice et des affaires intérieures, en vue d'assurer une plus grande simplification, cohérence, efficacité et attention aux besoins opérationnels. Le groupe d'experts recommande qu'un cadre soit établi pour l'accès des services répressifs aux systèmes, qui consisterait en une approche en deux temps n'envisageant la visualisation proprement dite des données qu'après vérification de l'existence de ces données, de manière à améliorer l'efficacité des accès à des fins répressives mais à en réduire le nombre et la portée.

[29] Une analyse technique plus approfondie est nécessaire en ce qui concerne l'inclusion potentielle de fonctionnalités de signalement dans un service partagé de mise en correspondance de données biométriques et les implications en matière de protection des données – voir section III.2 ci-dessous.

- les systèmes partagent **un répertoire commun de données d'identité** contenant des données d'identité alphanumériques[30], afin de détecter les enregistrements de personnes sous des identités multiples dans différentes bases de données.

Cette nouvelle approche devrait garantir que les systèmes conservent leurs **dispositions spécifiques en matière de protection des données**, assorties de règles spécifiques concernant l'accès des autorités compétentes, de règles distinctes concernant les limitations de la finalité pour chaque catégorie de données et de règles propres en matière de conservation des données. Cette approche de l'interopérabilité ne mènerait pas à l'interconnectivité de tous les systèmes.

Elle compenserait les faiblesses actuelles de l'architecture de gestion des données de l'UE et éliminerait les angles morts recensés. Le rôle de **l'agence eu-LISA** sera déterminant s'agissant d'assurer l'interopérabilité des systèmes d'information, y compris au moyen des analyses techniques actuelles et futures (voir section III.2 ci-dessous). La proposition législative que la Commission présentera en juin 2017 va renforcer le mandat de l'agence eu-LISA, ce qui lui permettra d'assurer la mise en œuvre de cette nouvelle approche. La Commission continuera également d'associer le Contrôleur européen de la protection des données et l'Agence des droits fondamentaux aux travaux sur l'interopérabilité.

Un niveau élevé de **qualité des données est essentiel pour assurer l'efficacité des systèmes d'information**. L'interopérabilité ne peut fonctionner que si les données versées dans les systèmes d'information sont exactes et complètes. La Commission a déjà reconnu la nécessité d'un renforcement de l'action de l'UE dans le domaine de la qualité des données[31]. De manière urgente, et avec l'aide de l'agence eu-LISA, elle mettra en œuvre les recommandations formulées par le groupe d'experts pour améliorer la qualité des données dans les systèmes d'information de l'UE.

La Commission fera progresser les recommandations du groupe d'experts sur le contrôle de qualité automatisé, sur un «entrepôt de données» permettant l'analyse de données anonymisées extraites des systèmes d'information pertinents à des fins statistiques et de rapport, ainsi que sur des modules de formation en matière de qualité des données à l'intention du personnel chargé d'alimenter les systèmes au niveau national. Il sera également tenu compte, dans la proposition législative à venir, du rôle important de l'agence eu-LISA pour l'assurance d'une qualité élevée des données dans les systèmes d'information centralisés de l'UE.

L'interopérabilité exige une interaction technique entre les systèmes d'information existants. Faciliter cette interaction est l'objectif du **format universel pour les messages** (UMF) à l'échelon de l'UE. La Commission, en collaboration avec l'agence eu-LISA, fera progresser les recommandations du groupe d'experts afin d'améliorer le format universel pour les messages conformément aux travaux en cours, dans le but de s'assurer que le développement du format soit pris en compte dans les systèmes d'information centralisés de l'UE.

2. La voie à suivre pour atteindre, d'ici à 2020, l'interopérabilité des systèmes d'information

[30] Y figureraient des attributs biographiques communs tels que le nom, la date de naissance et le sexe.

[31] Voir le quatrième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 41 final du 25.1.2017.

Parallèlement aux travaux visant l'aboutissement des dossiers prioritaires concernant les systèmes d'information, la Commission invite le Parlement européen et le Conseil à tenir **une discussion commune sur la voie à suivre** en matière d'interopérabilité telle qu'envisagée dans la présente communication. À cette fin, la Commission présentera ces idées et en discutera avec la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) le 29 mai 2017 et avec les États membres lors du Conseil «Justice et affaires intérieures» du 8 juin 2017. Les trois institutions devraient organiser, dans le sillage de ces discussions, des réunions tripartites au niveau technique[32] en automne 2017, afin de discuter plus avant de la voie à suivre en matière d'interopérabilité, telle qu'exposée dans la présente communication, y compris des besoins opérationnels pour les frontières et la sécurité, ainsi que de la manière de garantir la proportionnalité et le plein respect des droits fondamentaux. L'objectif est de dégager le plus rapidement possible, et au plus tard avant la fin de 2017, **une vision commune de la voie à suivre** et des mesures nécessaires à adopter pour assurer l'interopérabilité des systèmes d'information d'ici 2020.

Parallèlement à la discussion commune entre les trois institutions et sans préjuger de son issue, la Commission et l'agence eu-LISA continueront de procéder à **de nouvelles analyses techniques sur les solutions retenues pour l'interopérabilité** au cours de 2017, au moyen d'une série d'études techniques et de validations de concept. La Commission tiendra le Parlement européen et le Conseil régulièrement informé des progrès réalisés dans cette analyse technique.

Tirant parti des échanges avec le Parlement européen et le Conseil ainsi que des résultats des travaux législatifs en cours sur les systèmes d'information et d'autres analyses techniques, **la Commission travaille sans relâche afin de présenter, aussitôt que possible[33], une proposition législative sur l'interopérabilité**. Conformément aux principes d'amélioration de la réglementation, l'élaboration de la proposition législative comprendra une consultation publique et une analyse d'impact, portant notamment sur les droits fondamentaux et sur le droit à la protection des données à caractère personnel. En même temps que la proposition législative sur l'interopérabilité, la Commission présentera une proposition législative visant à réviser la base juridique du système d'information sur les visas[34], pour donner suite au rapport d'évaluation présenté en octobre 2016[35]. Le système d'information sur les visas est l'un des systèmes d'information centralisés de l'UE devant faire partie de la nouvelle approche de la gestion des données pour les frontières et la sécurité.

La **discussion conjointe entre les trois institutions sur la voie à suivre pour réaliser l'interopérabilité d'ici à 2020 ne devrait pas retarder les travaux sur les propositions législatives** relatives aux systèmes d'information actuellement discutées par les colégislateurs. La déclaration commune classait la plupart de ces propositions au rang de priorités urgentes et essentielles, qui visent toutes à remédier à d'importants déficits d'information nécessitant des mesures urgentes, conformément d'ailleurs aux recommandations du groupe d'experts. La proposition législative supplémentaire relative à un système européen d'information sur les casiers judiciaires (ECRIS) englobant les

[32] Ces réunions techniques pourraient s'inspirer de la réunion sur les frontières intelligentes qui a eu lieu en février 2015.

[33] Il faudra à cet effet l'accord des colégislateurs sur les dossiers législatifs connexes qui sont actuellement en débat – voir la section II.2 ci-dessus.

[34] Règlement (CE) n° 767/2008 du 9.7.2008.

[35] COM(2016) 655 final du 14.10.2016.

ressortissants de pays tiers, que la Commission présentera en juin 2017, sera également pleinement compatible avec les recommandations du groupe d'experts sur l'interopérabilité et l'approche exposée dans la présente communication. Afin de mettre en œuvre cette nouvelle approche d'une manière qui soit gérable, la stabilité des bases juridiques de tous les systèmes d'information concernés est primordiale. C'est pourquoi priorité doit être donnée à l'obtention d'un accord sur les propositions législatives en cours de discussion.

IV. MISE EN OEUVRE D'AUTRES DOSSIERS PRIORITAIRES CONCERNANT LA SÉCURITÉ

1. Initiatives législatives

En mai 2017, le nouveau **règlement Europol**[36] est entré en vigueur. Il constitue un tournant pour Europol et ajoute un certain nombre d'éléments nouveaux qui permettront à l'Agence de l'UE pour la coopération des services répressifs de devenir une véritable plateforme de l'UE pour l'échange d'informations sur les formes graves de criminalité transfrontière et le terrorisme. Europol disposera des outils pour devenir plus efficace, plus efficient et plus responsable. En particulier, une modification du cadre de traitement des données augmentera sa capacité à élaborer des analyses de la criminalité au service des États membres et un système de protection des données plus solide assurera une supervision indépendante et effective de la protection des données.

Ainsi que l'exige le traité, les activités d'Europol seront également examinées de près par le Parlement européen, en collaboration avec les parlements nationaux, ce qui améliorera encore la transparence des activités de l'agence et consolidera sa légitimité aux yeux des citoyens.

Afin de réduire au minimum les effets négatifs du retrait du Danemark d'Europol à la suite des résultats du référendum organisé dans cet État membre le 3 décembre 2016, **un accord de coopération opérationnelle entre Europol et le Danemark** a été signé le 30 avril 2017. Comme convenu dans la déclaration conjointe du président Juncker, du présent du Conseil, M. Tusk, et du premier ministre danois, M. Rasmussen, le 15 décembre 2016[37], l'accord établit des dispositions opérationnelles spéciales permettant un niveau suffisant de coopération opérationnelle entre le Danemark et Europol, y compris l'échange de données opérationnelles et l'échange d'officiers de liaison, sous réserve de garanties appropriées. Bien que cet accord ne remplace pas une participation à part entière du Danemark à Europol accordant un accès aux répertoires de données d'Europol ou le statut de membre à part entière des organes directeurs d'Europol, le Danemark a accepté la compétence de la Cour de justice de l'Union européenne et celle du Contrôleur européen de la protection des données, et a transposé dans le droit danois les règles de protection de données pertinentes de l'UE[38]. Comme indiqué dans la déclaration conjointe, ces dispositions sont subordonnées au maintien du Danemark dans l'Union européenne et dans l'espace Schengen.

Le 28 avril 2017, la Commission a adopté une décision d'exécution sur les protocoles communs et les formats de données devant être utilisés par les transporteurs aériens lors d'un transfert des données **des dossiers passagers (PNR)** aux unités d'information passagers (UIP) en vertu de la directive de l'UE sur les données des dossiers passagers[39]. Cette décision

---

36 Règlement (UE) 2016/794 du 11.5.2016.

37 Déclaration du président de la Commission européenne, M. Jean-Claude Juncker, du président du Conseil européen, M. Donald Tusk, et du premier ministre du Danemark, M. Lars Løkke Rasmussen, du 15.12.2016, http://europa.eu/rapid/press-release_IP-16-4398_fr.htm.

38 Directive (UE) 2016/680 du 27.4.2016.

39 Directive (UE) 2016/681 du 27.4.2016.

d'exécution harmonise les aspects techniques de la transmission des données des dossiers passagers par les transporteurs aériens. Les formats de données et les protocoles convenus seront obligatoires pour tous les transferts de données de dossiers passagers par les transporteurs aériens aux unités d'information passagers, à compter du 28 avril 2018.

Le 25 avril 2017, le Conseil a formellement adopté la nouvelle **directive sur les armes à feu**[40]. Les États membres disposent à présent d'un délai de 15 mois pour mettre en place les contrôles nécessaires portant sur l'acquisition et la possession d'armes à feu, afin d'éviter l'exploitation par des terroristes de la disparité des réglementations dans l'Union. Le 28 avril 2017, le groupe d'experts sur les normes de neutralisation est parvenu à un accord sur les nouvelles normes de neutralisation en vue d'adopter le règlement (UE) 2015/2403 révisé avant juillet 2017. La version révisée actuelle a pour but de clarifier certaines normes techniques afin d'assurer la bonne application de l'ensemble des procédures techniques pour la neutralisation d'une arme.

2. Mise en œuvre des actions non législatives

La cyberattaque mondiale du 12 mai 2017, commise au moyen d'un rançongiciel, a mis en lumière la nécessité urgente pour l'UE, ses agences et ses États membres, de renforcer les mesures prises pour combattre la menace croissante de la **cybercriminalité**, tout en se concentrant sur la détection et la dissuasion. Le centre européen de lutte contre la cybercriminalité d'Europol (EC3) a joué un rôle de premier plan dans la réaction des services répressifs à la dernière attaque, tirant parti des travaux qu'il avait menés auparavant dans ce domaine notamment dans le cadre de la campagne «No more ransom» (En finir avec le rançonnage). L'équipe d'intervention en cas d'urgence informatique de l'Union (EU-CERT) a également établi un contact étroit avec le centre européen de lutte contre la cybercriminalité, les centres de réponse aux incidents de sécurité informatique des pays touchés, les unités spécialisées en cybercriminalité et les partenaires clés du secteur afin de réduire la menace et d'aider les victimes. La Commission a annoncé, dans son examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique, le 10 mai 2017, son intention de réviser la stratégie de cybersécurité de l'Union européenne d'ici septembre 2017. Les travaux s'accélèrent afin d'élargir la portée des mesures actuelles, axées sur la prévention, pour en renforcer les aspects liés à la détection et à la dissuasion. L'objectif devrait être de réduire tant la probabilité des cyberattaques que leur incidence, en renforçant la résilience et en intensifiant davantage les efforts déployés par les États membres pour la construction de leurs capacités nationales et la mise en œuvre intégrale de la directive sur la sécurité des réseaux et de l'information [41]. Le potentiel de la cybercriminalité (et de la criminalité facilitée par les technologies de l'information) ne se nourrit pas seulement des lacunes affectant les systèmes et les logiciels mais aussi des comportements qui conduisent à une mauvaise cyber-hygiène. La Commission entend non seulement renforcer le mandat de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) mais aussi formuler des propositions pour l'élaboration de normes de sécurité, de certification et d'étiquetage, afin de renforcer la cybersécurité des systèmes et des dispositifs. Elle se concentrera également sur l'acquisition de compétences informatiques et d'une capacité technique au sein de l'Union.

---

40 http://www.consilium.europa.eu/fr/press/press-releases/2017/04/25-control-acquisition-possession-weapons/

41 Directive (UE) 2016/1148 du 6.7.2016.

Dans le contexte actuel des menaces qui pèsent sur l'ordre public ou la sécurité intérieure, **des contrôles de police renforcés** dans le territoire des États membres, y compris dans les zones frontalières, peuvent à la fois être nécessaires et justifiés pour accroître la sécurité au sein de l'espace Schengen. C'est pourquoi, le 2 mai 2017, la Commission a présenté une recommandation relative à des contrôles de police proportionnés et à la coopération policière dans l'espace Schengen[42]. La recommandation énonce des mesures que les États Schengen devraient prendre afin de permettre une utilisation plus efficace des pouvoirs de police actuels pour faire face aux menaces pesant sur l'ordre public ou la sécurité intérieure. Lorsque cela est nécessaire et justifié, les États membres devraient intensifier les contrôles de police dans les zones frontalières et sur les principaux axes routiers. La décision concernant de tels contrôles, ainsi que leur lieu et leur intensité, continue de relever intégralement de la compétence des États membres et devrait toujours être proportionnée aux menaces constatées. En outre, la Commission recommande que l'ensemble des États membres renforcent la coopération policière transfrontière afin de contrer les menaces pour l'ordre public ou la sécurité intérieure.

Dans le domaine de la **sûreté aérienne**, des évolutions sont intervenues ces dernières semaines avec l'imposition par les États-Unis et le Royaume-Uni de nouvelles mesures de sécurité sur les vols en provenance d'un certain nombre de pays du Moyen-Orient, d'Afrique du Nord et de la Turquie, exigeant le placement des dispositifs électroniques de grande taille dans des bagages enregistrés. Du côté de l'UE, les travaux ont progressé en matière d'évaluation des risques concernant les menaces et les vulnérabilités liées aux vols en provenance des pays tiers. À la suite d'informations selon lesquelles les États Unis pourraient prévoir l'instauration de mesures similaires sur les vols en provenance des aéroports de l'UE, la Commission a organisé des contacts au niveau politique afin d'assurer une coordination des actions entre les États-Unis et l'UE. Une rencontre entre les États-Unis et l'UE aura lieu a à Bruxelles, le 17 mai 2017, au cours de laquelle les parties évalueront conjointement les risques potentiels et œuvreront à l'élaboration d'une approche commune permettant de faire face au développement de la menace.

Les travaux sont en cours au sein du comité permanent de coopération opérationnelle en matière de sécurité intérieure (COSI) sur le prochain **cycle politique de l'UE pour lutter contre la grande criminalité internationale** pour les années 2018 à 2021, qui tiennent compte des huit menaces criminelles prioritaires, relevées par la Commission dans son dernier rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité[43]. Le Conseil devrait adopter des conclusions sur le nouveau cycle politique de l'UE le 18 mai 2017.

À l'issue du rapport présenté par la Commission au Conseil «Justice et affaires intérieures», en décembre 2016, sur l'état d'avancement des travaux sur l'amélioration de l'accès transfrontière des enquêteurs en matière pénale aux **preuves électroniques**[44], la Commission

---

[42] Le 2 mai 2017, la Commission a approuvé dans son principe la recommandation relative à des contrôles de police proportionnés et à la coopération policière dans l'espace Schengen [C(2017) 2923]. L'adoption formelle a eu lieu le 12 mai 2017.

[43] COM(2017) 213 final du 12.4.2017. Les huit menaces criminelles prioritaires relevées par la Commission sont: la cybercriminalité, les infractions liées au trafic de stupéfiants, le trafic de migrants, la criminalité organisée contre les biens, la traite des êtres humains, le trafic d'armes à feu, la fraude à la TVA et la criminalité au détriment de l'environnement.

[44] Voir le document informel des services de la Commission: Rapport sur l'état des travaux à la suite des conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace du 2.12.2016: http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf. Dans ses conclusions sur

achève actuellement son évaluation et proposera une voie à suivre qui sera débattue au sein du Conseil «Justice et affaires intérieures» le 8 juin 2017.

La Commission a soutenu les travaux entrepris jusqu'à ce jour par un groupe d'État membres pour assurer la maintenance d'e-CODEX, un système de coopération judiciaire transfrontière et d'accès numérique aux procédures judiciaires. La Commission a pris note de la position de ce groupe selon laquelle la maintenance d'e-CODEX par un groupe d'États membres ne constitue pas une solution viable. Au niveau du groupe de travail du Conseil, les États membres ont examiné différentes options et ont conclu que l'agence eu-LISA serait la mieux placée pour garantir la maintenance et l'opérabilité du système e-CODEX. Soucieuse de rechercher une solution optimale, la Commission prépare actuellement une analyse d'impact permettant d'envisager plusieurs options pour la maintenance d'e-CODEX. Les résultats de l'analyse d'impact seront disponibles à l'automne 2017.

L'adoption précitée de la directive sur les armes à feu est une avancée importante en vue de l'application des règles régissant l'acquisition et la possession légales d'armes à feu. La Commission travaille également à la lutte contre **le trafic illicite d'armes à feu** tant au sein de l'UE qu'au-delà de ses frontières. Le 16 mars 2017, une table ronde technique entre l'UE et l'Ukraine sur le trafic d'armes à feu a eu lieu à Kiev. Cette réunion était la première entre l'UE et l'Ukraine visant à améliorer l'échange d'informations liées au trafic illicite d'armes à feu. La deuxième table ronde technique entre l'UE et la Tunisie sur le trafic d'armes à feu s'est tenue à Tunis, le 28 mars 2017. Pour l'Ukraine comme pour la Tunisie, un plan d'action a été convenu, comprenant des missions d'experts afin d'évaluer le cadre administratif de chaque pays, d'organiser une conférence de haut niveau sur la législation en la matière et de proposer une formation, des visites d'étude et des ateliers sur la gestion pratique des données ainsi qu'une coopération opérationnelle.

La Commission et le Service européen pour l'action extérieure ont présenté au Conseil **un document informel conjoint sur l'action extérieure de l'UE dans le domaine de la lutte antiterroriste**, le 12 mai 2017, qui recense les pays, les domaines et les instruments prioritaires de l'action de l'UE dans ce domaine. Ce document conjoint constitue une contribution à la discussion sur la révision des conclusions du Conseil de février 2015 relatives à la lutte contre le terrorisme[45], dans le but d'adopter de nouvelles conclusions lors du Conseil des affaires étrangères de juin 2017.

Un premier atelier rassemblant des pays voisins de l'UE sur le thème de **la protection des infrastructures critiques** a eu lieu à Bucarest les 16 et 17 mars 2017, dans le cadre d'un élargissement de la dimension extérieure du programme européen de protection des infrastructures critiques. Outre les États membres, figuraient parmi les participants des représentants de huit pays d'Europe de l'Est et des Balkans occidentaux. Ce premier atelier avait pour but d'établir des contacts et d'échanger des informations sur les mesures et les instruments permettant de protéger des infrastructures critiques. Les domaines de coopération possibles ont été recensés, y compris des formations ou des exercices conjoints axés sur des aspects pratiques (opérationnels), des études portant sur les interdépendances régionales et

---

l'amélioration de la justice pénale dans le cyberespace, du 9 juin 2016, le Conseil a invité la Commission à prendre des mesures concrètes, à élaborer une approche européenne commune et à présenter au plus tard en juin 2017 les résultats escomptés.

[45] Conclusions du Conseil relatives à la lutte contre le terrorisme, du 9.2.2015: http://www.consilium.europa.eu/fr/press/press-releases/2015/02/150209-council-conclusions-counter-terrorism/.

des évaluations par des pairs de stratégies nationales de protection des infrastructures critiques.

V. CONCLUSIONS

La Commission appelle le Parlement européen et le Conseil à progresser sur les dossiers législatifs prioritaires relatifs aux systèmes d'information assurant la gestion de la sécurité, des frontières et des flux migratoires. Ces actes législatifs renforceront les systèmes existants et combleront les déficits d'information déjà recensés, en répondant aux besoins des garde-frontières, des agents des services répressifs, des agents des services de l'immigration et des autorités judiciaires, ainsi qu'en créant la base permettant d'assurer l'interopérabilité de ces systèmes.

En guise de suivi de la communication d'avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», et à la lumière des recommandations du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité, la Commission a adopté une nouvelle approche de la gestion des données pour les frontières et la sécurité, dans le cadre de laquelle tous les systèmes d'information centralisés de l'UE permettant la gestion de la sécurité, des frontières et des flux migratoires seront interopérables, dans le plein respect des droits fondamentaux. À cette fin, et tirant parti des travaux en cours sur le plan législatif et technique en ce qui concerne les systèmes d'information, la Commission présentera une proposition législative en juin 2017, afin de renforcer le mandat de l'agence eu-LISA pour lui permettre d'assurer la mise en œuvre de cette nouvelle approche, qui sera suivie d'une proposition législative sur l'interopérabilité, dès que possible. La Commission invite le Parlement européen et le Conseil à mener une discussion conjointe sur la voie à suivre à l'avenir. Les trois institutions pourront ainsi arrêter une vision commune de la voie à suivre en matière d'interopérabilité et déterminer les étapes nécessaires de sa mise en œuvre d'ici à 2020, dans le plein respect des droits fondamentaux. La mise en œuvre de l'approche de l'interopérabilité qui a été exposée rendrait la gestion des données dans l'UE plus efficace et plus efficiente, pour une meilleure protection des frontières extérieures et un renforcement de la sécurité dans l'UE au bénéfice de tous les citoyens.