COMMISSION
EUROPÉENNE

Bruxelles, le 25.1.2017
COM(2017) 41 final

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

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

Quatrième 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 quatrième 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 principaux piliers: *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 porte principalement sur quatre domaines clés, à savoir les systèmes d'information et l'interopérabilité, la protection des cibles vulnérables, les cybermenaces et la protection des données dans le cadre d'enquêtes pénales.

L'attaque sur le marché de Noël à Berlin en décembre a une nouvelle fois mis en lumière de graves faiblesses dans nos systèmes d'information auxquelles il faut d'urgence remédier, en particulier au niveau de l'UE, afin d'aider les autorités nationales frontalières et répressives sur le terrain à exercer plus efficacement leurs difficiles fonctions. Le fait que les différents systèmes d'information ne soient pas interconnectés – ce qui permet aux auteurs d'attaques d'utiliser plusieurs identités pour se déplacer sans être repérés, y compris lorsqu'ils franchissent des frontières – et le fait que ces informations ne soient pas systématiquement versées par les États membres dans les bases de données pertinentes de l'UE constituent des faiblesses dans la mise en œuvre concrète qu'il convient de pallier d'urgence. En outre, il est également nécessaire de poursuivre les travaux en matière de mesures répressives concernant les frontières et le retour des personnes dont la demande d'asile a été rejetée[1].

Pour ce qui est de la protection des cibles vulnérables, la Commission accélérera ses travaux en cours afin de rassembler des experts des États membres pour mettre en commun leurs bonnes pratiques et convenir de lignes directrices officielles.

La cybermenace à laquelle est confrontée l'UE bénéficie d'une large couverture médiatique et le présent rapport revient sur les différents axes de travail dans ce domaine qui sont déjà déployés. Ceux-ci portent à la fois sur la prévention – laquelle implique, d'une part, une collaboration avec les entreprises du secteur pour promouvoir la sécurité dès la conception et, d'autre part, la transposition et la mise en œuvre de la directive sur la sécurité des réseaux et de l'information – et sur une coopération renforcée entre les États membres et avec les organisations et partenaires internationaux pour faire face aux cyberattaques lorsqu'elles se produisent. Au cours des prochains mois, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité recenseront les actions nécessaires pour apporter une réponse européenne efficace à ces menaces, en prenant comme point de départ la stratégie de cybersécurité de l'UE de 2013.

La protection de la vie privée des personnes et des données à caractère personnel constitue un droit fondamental et, partant, une pierre angulaire dans toute action en faveur d'une réelle union de la sécurité. La directive sur la protection des données dans le

[1] La Commission présentera un plan d'action révisé en matière de retour dans les semaines à venir, voir le rapport de la Commission au Parlement européen, au Conseil européen et au Conseil sur l'entrée en opération du corps européen de garde-frontières et de garde-côtes, COM (2017) 42.

domaine de la police et de la justice pénale adoptée en avril 2016 garantissant une norme élevée commune de protection des données, elle facilitera le bon échange des données pertinentes entre autorités répressives des États membres. La Commission a également lancé un processus de révision de la directive «vie privée et communications électroniques» dans le cadre de son paquet «données» afin d'étendre le champ d'application de cet acte à tous les fournisseurs de services de communications électroniques et de mettre ses dispositions en conformité avec le règlement général sur la protection des données. Cette proposition vise à garantir le respect de la vie privée dans les communications électroniques, tout en énonçant les motifs pour lesquels on peut envisager de restreindre le champ d'application du règlement «vie privée et communications électroniques», y compris des motifs liés à la sécurité nationale ou à des enquêtes pénales.

II. RENFORCER LES SYSTÈMES D'INFORMATION ET L'INTEROPÉRABILITÉ

Dans le discours sur l'état de l'Union prononcé en septembre 2016 par le président Juncker et dans les conclusions du Conseil européen de décembre 2016, il est fait état de l'importance de surmonter les obstacles actuels en matière de gestion de l'information et d'améliorer **l'interopérabilité et l'interconnexion des systèmes d'information existants**. Les récents événements ont une nouvelle fois montré qu'il est urgent de relier les bases de données existantes de l'UE, notamment pour doter les autorités frontalières et répressives sur le terrain des outils nécessaires à la détection des fraudes à l'identité. Prenons l'exemple de l'auteur de l'attentat terroriste de décembre 2016 à Berlin: il a utilisé au moins 14 identités différentes et a pu se rendre d'un État membre à l'autre sans être repéré. Il est, dès lors, manifestement nécessaire de rendre les systèmes d'information de l'UE existants et à venir consultables simultanément par l'utilisation d'identifiants biométriques afin de fermer cette voie aux terroristes et aux criminels.

À cet égard, la Commission a lancé les travaux en avril 2016 en présentant ses propositions pour «des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité»[2]. Elle y constatait des insuffisances concernant les fonctionnalités des systèmes d'information existants, des lacunes dans l'architecture de la gestion des données de l'UE, des problèmes relatifs à une mosaïque complexe de systèmes d'information régis de différentes façons et une fragmentation générale due au fait que les systèmes actuels ont été conçus pour fonctionner séparément plutôt qu'ensemble. Dans le cadre de ce processus, la Commission a constitué le **groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité** avec les agences de l'UE, les États membres et les parties prenantes concernées. Le 21 décembre 2016[3], un rapport du président dudit groupe a présenté les **conclusions intermédiaires** de celui-ci qui comprennent l'option prioritaire de création d'un portail de recherche unique permettant aux autorités nationales répressives et frontalières d'interroger simultanément les bases de données et les systèmes d'information existants de l'Union. Le rapport intermédiaire souligne également l'importance de la qualité des données – l'efficacité des systèmes d'information dépendant de la qualité et du format

[2] Communication intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité», COM(2016) 205 final.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

des données qui y sont saisies – et formule des recommandations pour améliorer cette qualité dans les systèmes de l'UE au moyen de contrôles automatisés de la qualité des données.

La Commission donnera suite sans délai à l'option de création d'un portail de recherche unique et, en collaboration avec l'agence de l'UE pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), elle entamera ses travaux sur un portail permettant d'effectuer des recherches en parallèle dans tous les systèmes existants de l'UE concernés. Une étude connexe devrait être prête d'ici le mois de juin et servira de base à la conception et au test d'un prototype du portail avant la fin de l'année. La Commission considère qu'en parallèle Europol devrait poursuivre ses travaux sur une interface système qui permettra aux agents en première ligne des États membres, lorsqu'ils consultent leurs propres systèmes nationaux, de consulter en même temps automatiquement les bases de données d'Europol.

Les travaux en vue de l'interopérabilité des systèmes d'information visent à remédier à la fragmentation actuelle de l'architecture européenne de la gestion des données appliquée aux contrôles aux frontières et à la sécurité, ainsi qu'aux angles morts qui en résultent. Lorsque les bases de données utilisent un répertoire commun de données d'identité — comme envisagé pour les propositions de système d'entrée/sortie de l'UE et de système européen d'autorisation et d'information concernant les voyages (ETIAS) — une personne ne peut être enregistrée que sous une seule identité dans les différentes bases de données, ce qui empêche l'utilisation de plusieurs fausses identités. Dans un premier temps, comme suggéré dans les conclusions intermédiaires du groupe d'experts à haut niveau, la Commission a demandé à l'agence eu-LISA d'analyser les aspects techniques et opérationnels de la mise en œuvre d'un service partagé de mise en correspondance de données biométriques. Un tel service devrait permettre d'effectuer des recherches dans différentes bases de données au moyen de données biométriques, qui pourraient mettre au jour de fausses identités utilisées par la personne concernée dans un autre système. Par ailleurs, le groupe d'experts à haut niveau devrait à présent déterminer s'il est nécessaire, techniquement réalisable et proportionné d'étendre le **répertoire commun de données d'identité** envisagé pour le système d'entrée/sortie et le système ETIAS à d'autres systèmes. En plus des données biométriques stockées dans le service de mise en correspondance de données biométriques, un tel répertoire commun comprendrait également des données alphanumériques d'identité. Le groupe devrait présenter ses conclusions à ce sujet dans son rapport final d'ici la fin du mois d'avril 2017.

Les récents événements ayant compromis la sécurité mettent en évidence la nécessité de réexaminer la question du **partage obligatoire des informations** entre les États membres. La proposition de la Commission de décembre 2016 visant à renforcer le **système d'information Schengen** prévoit, pour la première fois, une obligation pour les États membres d'introduire des signalements de personnes liées aux infractions terroristes. Il importe que les colégislateurs œuvrent à présent en faveur d'une adoption rapide des mesures proposées. La Commission est prête à examiner s'il convient d'introduire une obligation contraignante concernant l'échange d'informations pour d'autres bases de données de l'UE.

III. PROTÉGER NOS CIBLES VULNÉRABLES CONTRE LES ATTAQUES TERRORISTES

L'attaque de Berlin est la plus récente dans l'UE à avoir frappé ce qu'on appelle des cibles vulnérables; celles-ci sont généralement des sites civils où les personnes se retrouvent en grand nombre (par ex. des lieux publics, des hôpitaux, des écoles, des enceintes sportives, des centres culturels, des cafés et des restaurants, des centres commerciaux et des nœuds de transport). De par leur nature, ces lieux sont vulnérables et difficiles à protéger et ils se caractérisent également par la forte probabilité d'un nombre considérable de victimes en cas d'attaque. C'est pour toutes ces raisons qu'ils sont privilégiés par les terroristes. La menace de futures attaques contre des cibles vulnérables, y compris les transports, reste élevée, comme le confirment les analyses disponibles, notamment le rapport d'Europol portant sur l'évolution du mode opératoire de Daech[4].

Le programme européen en matière de sécurité de 2015 et la communication de 2016 sur l'union de la sécurité ont mis en évidence la nécessité d'intensifier les actions visant à améliorer la sécurité et l'utilisation d'outils de détection innovants et de technologies de détection dans le domaine de la protection des cibles vulnérables. La Commission a œuvré pour soutenir les États membres dans l'élaboration de meilleurs outils afin de prévenir les attaques contre des cibles vulnérables et y répondre, et pour encourager l'échange de bonnes pratiques entre ceux-ci, ce qui lui a permis d'élaborer des manuels opérationnels et des documents d'orientation. La Commission met actuellement au point, en étroite coopération avec des experts des États membres, un manuel complet sur les procédures de sécurité et les modèles applicables aux différentes cibles vulnérables (par ex. centres commerciaux, hôpitaux, manifestations sportives et culturelles). L'objectif visé est de publier début 2017 des orientations sur la protection des cibles vulnérables à l'adresse des États membres, sur la base de leurs meilleures pratiques.

Dans le même temps, la Commission organisera en février le premier atelier avec des autorités nationales sur la protection des cibles vulnérables, en vue d'échanger des informations et de mettre au point de bonnes pratiques sur la question complexe suivante: la protection des cibles vulnérables et la sûreté et la sécurité publiques. La Commission finance également, au titre du Fonds pour la sécurité intérieure, un projet pilote mené par la Belgique, les Pays-Bas et le Luxembourg afin d'instituer un centre d'excellence régional pour les interventions spéciales des forces de l'ordre, qui proposera des formations destinées aux officiers de police, qui sont souvent les premiers intervenants en cas d'attentat.

La réaction à des attaques contre des cibles vulnérables constitue une composante majeur du travail de la Commission en matière de protection civile. En décembre, la Commission a annoncé les actions qu'elle entendait mener avec les États membres afin de protéger les citoyens de l'Union et de réduire les points faibles au lendemain des attentats terroristes. Ces actions permettront de renforcer la coordination entre tous les acteurs intervenant dans la gestion des conséquences des attentats et la Commission s'est engagée à soutenir les efforts des États membres en facilitant l'organisation de formations

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited* (Changements dans le mode opératoire de l'État islamique - rapport révisé), novembre 2016 – publication d'Europol disponible à l'adresse suivante: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

et d'exercices communs et en assurant un dialogue suivi par l'intermédiaire des points de contact et des groupes d'experts existants. La Commission soutiendra également la mise au point de modules spécialisés pour répondre aux attentats terroristes dans le cadre du mécanisme de protection civile de l'Union et d'initiatives de partage des enseignements tirés et de sensibilisation du public.

En collaboration avec les États membres, la Commission étudiera également le type d'appui que l'UE pourrait mobiliser pour aider à accroître la résilience et renforcer la sécurité autour des cibles vulnérables potentielles. Les États membres pourraient aussi demander un financement auprès de la Banque européenne d'investissement (BEI) (y compris du Fonds européen pour les investissements stratégiques), conformément aux politiques de l'UE et du groupe BEI. Tout projet serait soumis aux procédures décisionnelles habituelles prévues dans la législation.

En ce qui concerne les cibles vulnérables spécifiques liées à des lieux publics de transport comme les parties publiques des aéroports ou des gares ferroviaires, l'atelier qu'a consacré la Commission à la question en novembre 2016 a réuni un large éventail de parties prenantes et a mis en avant la nécessité de maintenir l'équilibre entre les exigences en matière de sécurité, le confort des passagers et les opérations de transport. Ses conclusions insistent sur l'importance de forger une culture de la sécurité qui englobe non seulement le personnel, mais aussi les passagers, l'importance des évaluations des risques au niveau local servant de base à la définition des contremesures appropriées et la nécessité d'améliorer la communication entre toutes les parties concernées.

IV. FAIRE FACE AUX CYBERMENACES

La cybercriminalité et les cyberattaques constituent des défis de taille auxquels l'Union est confrontée et un domaine dans lequel une action au niveau de l'UE peut contribuer à renforcer notre résilience collective. Chaque jour, des incidents liés à la cybersécurité nuisent gravement à la vie des personnes et causent d'importants dommages économiques aux entreprises et à l'économie européennes. Les cyberattaques forment un élément essentiel des menaces hybrides; combinées avec précision à des menaces physiques, par exemple en lien avec le terrorisme, elles peuvent avoir un effet dévastateur. Elles peuvent également contribuer à déstabiliser un pays ou à mettre à mal ses institutions politiques et ses processus démocratiques fondamentaux. À mesure que notre dépendance aux technologies en ligne s'accroît, nos infrastructures critiques (des hôpitaux aux centrales nucléaires) deviennent de plus en plus vulnérables.

La stratégie de cybersécurité de l'UE de 2013 fait partie du noyau dur des mesures prises pour répondre aux défis en matière de cybersécurité. La composante principale est la directive sur la sécurité des réseaux et de l'information (SRI)[5], adoptée en juillet dernier. Elle crée les conditions propices à l'amélioration de la coopération et de la cyber-résilience au niveau de l'UE en soutenant la coopération et l'échange d'informations entre les États membres et en encourageant une coopération opérationnelle lors d'incidents spécifiques de cybersécurité et le partage des informations sur les risques.

[5] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Afin d'assurer une transposition et une mise en œuvre cohérentes dans l'ensemble des différents secteurs et par-delà les frontières, la Commission organisera la première réunion du groupe de coopération SRI avec les États membres en février.

En avril 2016, la Commission et la haute représentante de l'UE ont adopté un cadre commun en matière de lutte contre les menaces hybrides[6] qui proposait 22 actions opérationnelles visant à sensibiliser l'opinion, à accroître la résilience, à mieux réagir aux crises et à renforcer la coopération entre l'UE et l'OTAN. Ainsi que le Conseil l'a demandé, la Commission et la haute représentante de l'UE présenteront un rapport d'ici juillet 2017 afin d'évaluer les progrès accomplis.

La Commission promeut et soutient également l'innovation technologique, y compris en recourant aux fonds de recherche de l'UE afin de susciter de nouvelles solutions et de mettre au point de nouvelles technologies pouvant contribuer au renforcement de notre résilience aux cyberattaques (par exemple, les projets relatifs à la «sécurité dès la conception»). L'été dernier, elle a lancé un partenariat public-privé de 1,8 milliard d'EUR dans le domaine de la cybersécurité avec les entreprises[7].

Dans les transports, la numérisation est devenue un moteur essentiel pour la transformation nécessaire de l'actuel système de transport. La rapidité de la numérisation comporte de nombreux avantages, mais elle rend aussi les transports plus vulnérables aux risques liés à la cybersécurité ou cybersûreté. De nombreuses actions sont entreprises pour réduire la menace à différents niveaux, et plus particulièrement dans le secteur aéronautique, mais également dans le transport maritime, fluvial, ferroviaire et routier[8]. Il est toutefois encore nécessaire de continuer à clarifier, harmoniser et compléter les mesures prises par les différents acteurs engagés dans l'amélioration de différents aspects de la cyber-résilience.

D'une manière plus large et compte tenu de la nature rapidement évolutive de la menace, au cours des prochains mois, la Commission et la haute représentante de l'UE recenseront les actions nécessaires pour apporter une réponse européenne efficace à ces menaces, dans le prolongement de la stratégie de cybersécurité de l'UE de 2013.

V. PROTÉGER LES DONNÉES À CARACTÈRE PERSONNEL TOUT EN CONCOURANT À L'EFFICACITÉ DES ENQUÊTES PÉNALES

La directive relative à la protection des données destinées à la police et à la justice pénale[9] est un élément constitutif de la lutte contre le terrorisme et les formes graves de

---

6 JOIN (2018)18.

7 Annoncé dans la communication sur la cyber-résilience de 2016, COM (2016) 410 final.

8 Par exemple: des lignes directrices internationales comme celles élaborées par l'Organisation maritime internationale ou une résolution que l'OACI a récemment adoptée, à l'initiative commune de l'UE et des États-Unis; une notification des incidents dans le cadre de laquelle un mode plus réactif est actuellement mis au point par l'Agence européenne de la sécurité aérienne, et la cybersécurité dès la conception, applicable aux nouveaux systèmes en cours de développement, tels que le plan directeur européen de gestion du trafic aérien conçu par l'entreprise commune SESAR.

9 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de

criminalité. Sur la base d'une norme commune de protection des données établie dans la directive, les autorités répressives des États membres pourront échanger sans heurts les données pertinentes, tandis que les données concernant les victimes, les témoins et les suspects d'infractions seront dûment protégées.

En outre, afin d'assurer un niveau élevé de confidentialité des communications, tant pour les citoyens que pour les entreprises, et des conditions de concurrence équitables pour tous les acteurs du marché, comme indiqué dans la stratégie pour le marché unique numérique d'avril 2015, la Commission a adopté, ce 11 janvier, la proposition de **règlement «vie privée et communications électroniques»** (qui remplace la directive 2002/58/CE)[10]. À l'instar de l'actuelle directive, le nouveau règlement «vie privée et communications électroniques» précise le règlement général sur la protection des données[11] et instaure un cadre régissant la protection de la vie privée et des données à caractère personnel dans le secteur des communications électroniques.

Cette révision a pour conséquence que l'ensemble des données de communications électroniques, même lorsque la communication est accessoire, sont considérées comme confidentielles/respectées — qu'elles soient transmises par des services de télécommunications traditionnels ou d'autres services par contournement (OTT) qui sont équivalents sur le plan fonctionnel (par exemple, Skype et WhatsApp), devenus souvent interchangeables avec les opérateurs de télécommunications normaux pour de nombreux utilisateurs[12]. Parmi les obligations imposées aux fournisseurs de services — outre celle de respecter les choix relatifs à la vie privée de leurs clients concernant l'utilisation, le stockage et le traitement de leurs données — figure l'obligation pour les fournisseurs de services établis en dehors de l'Union de désigner un représentant dans un État membre. Cette obligation permettra aussi aux États membres de faciliter la coopération des autorités répressives et judiciaires avec les fournisseurs de services afin d'accéder à des preuves électroniques (voir ci-dessous).

Comme dans le cadre des actuelles règles sur la vie privée et les communications électroniques, l'accès des autorités répressives et judiciaires à des informations électroniques pertinentes, nécessaires dans les enquêtes pénales, sera régi par l'exception prévue à l'article 11 de la proposition de règlement «vie privée et communications électroniques»[13]. Cette disposition offre la possibilité en droit de l'Union ou en droit

---

poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil. La directive, entrée en vigueur le 5 mai 2016, doit être transposée par les États membres au plus tard le 6 mai 2018. La Commission a créé un groupe d'experts avec les États membres afin qu'ils puissent échanger leurs points de vue sur la transposition de cette directive.

10 Règlement «vie privée et communications électroniques», COM(2017) 10.

11 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), qui sera applicable à partir du 25 mai 2018.

12 Elle suit l'approche adoptée dans la proposition de directive établissant le code des communications électroniques européen, présentée le 14 septembre 2016 par la Commission (le paquet «Télécoms»), COM(2016) 590 final.

13 Voir l'article 11, paragraphe 1 (clause sur la conservation des données), qui est identique à l'article 15 de la directive «vie privée et communications électroniques» et conforme aux exigences du règlement général sur la protection des données. Cette limitation doit respecter le contenu essentiel des droits fondamentaux et être nécessaire, appropriée et proportionnée.

national de restreindre la confidentialité des communications, lorsque cela est nécessaire et proportionné, afin de sauvegarder la sécurité nationale, la défense, la sécurité publique, et à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales. Elle revêt une importance particulière pour les règles nationales en matière de **conservation des données**, à savoir pour obliger les fournisseurs de services de télécommunications à conserver les données de communication pendant une durée précise en vue d'un éventuel accès à des fins répressives, à la suite de l'annulation en 2014 par la Cour de justice de l'Union européenne (CJUE) de la directive sur la conservation des données[14]. Depuis lors, il n'a été adopté aucun instrument de l'UE relatif à la conservation des données et certains États membres ont légiféré en la matière. Les législations suédoise et britannique sur la conservation des données ont été contestées devant la Cour, qui a rendu son arrêt le 21 décembre dernier dans l'affaire *Tele2*[15]. La Cour a déclaré incompatible avec le droit de l'Union une législation nationale qui prévoit, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs concernant tous les moyens de communication électronique. Les conséquences de cet arrêt sont en cours d'analyse et la Commission mettra au point des orientations concernant la manière dont les législations nationales relatives à la conservation des données peuvent être rédigées dans le respect de l'arrêt.

La criminalité laisse des traces numériques qui peuvent servir de preuves dans le cadre de procédures judiciaires; les communications électroniques entre les suspects sont souvent les seuls indices que peuvent recueillir les autorités répressives et les procureurs. Toutefois, obtenir l'accès aux **preuves électroniques**, en particulier si elles sont stockées à l'étranger ou sur un nuage, peut être à la fois techniquement et juridiquement complexe et impliquer souvent une procédure lourde, ce qui entrave le travail des enquêteurs qui doivent agir vite. Afin de s'attaquer à ces problèmes, la Commission examine actuellement des solutions pour permettre aux enquêteurs d'obtenir des preuves électroniques dans un contexte transfrontière, y compris en rendant l'entraide judiciaire plus efficace, en trouvant des moyens de coopération directe avec les fournisseurs de services internet, et pour proposer des critères aux fins de la détermination de la compétence d'exécution dans le cyberespace, dans le strict respect des règles applicables en matière de protection des données[16]. Le 9 décembre 2016, la Commission a fait rapport au Conseil «Justice et affaires intérieures» sur les progrès accomplis[17].

Un vaste processus de consultation d'experts (toujours en cours) a permis à la Commission de recenser les différents problèmes, souvent complexes, que pose l'accès aux preuves électroniques, de mieux comprendre les règles et pratiques actuelles dans les États membres et de définir les moyens d'action possibles. Le rapport d'étape donne un aperçu des idées qui ont déjà émergé au cours de la collecte d'informations et du

---

[14] Arrêt de la Cour du 8 avril 2014, *Digital Rights Ireland*, dans les affaires jointes C-293/12 et C-594/12.

[15] Arrêt de la Cour du 21 décembre 2016, *Tele2*, dans les affaires jointes C−203/15 et C−698/15.

[16] Comme elle s'y était engagée dans le programme européen en matière de sécurité, COM (2015) 185 final, et dans la communication de la Commission sur la mise en œuvre du programme européen en matière de sécurité pour lutter contre le terrorisme et ouvrir la voie à une union de la sécurité réelle et effective, COM (2016) 230 final.

[17] Dans ses conclusions sur 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.

processus de consultation d'experts; la Commission, en concertation avec les parties concernées, en fera une analyse plus approfondie dans les mois à venir. Comme l'a annoncé la Commission dans son programme de travail, elle présentera une initiative en 2017.

VI. CONCLUSION

Le prochain rapport qui devra être publié le 1er mars sera l'occasion de faire le point sur les progrès réalisés dans la mise en œuvre de ces axes de travail et d'autres axes de premier plan.