COMMISSION EUROPÉENNE

Bruxelles, le 15.10.2020
C(2020) 7204 final

M. Jean-François RAPIN
Président de la Commission
des affaires européennes du Sénat
Palais du Luxembourg
15, rue de Vaugirard
F – 75291 PARIS Cedex 06

cc. M. Gérard LARCHER
Président du Sénat
Palais du Luxembourg
15, rue de Vaugirard
F – 75291 PARIS Cedex 06

Monsieur le Président,

La Commission tient à remercier le Sénat pour son avis concernant la lutte contre la cybercriminalité du 9 juillet 2020.

La Commission reconnaît que la cybercriminalité continue de constituer une menace considérable pour notre société et notre économie. Des enquêtes montrent que les Européens la considèrent comme un problème majeur pour la sécurité de l'Union européenne et sont de moins en moins confiants quant à leur capacité à préserver leur sécurité en ligne[1]*. Il est probable que la pandémie de COVID-19 a exacerbé la menace que représente la cybercriminalité, les criminels profitant de vulnérabilités accrues*[2]*. L'amélioration de la lutte contre la cybercriminalité figure donc en bonne place parmi les priorités politiques de la Commission.*

Dans ses orientations politiques[3] *pour la Commission 2019-2024, la présidente von der Leyen souligne l'importance de la sécurité intérieure de l'Union européenne, notamment*

---

[1] Voir le rapport Eurobaromètre spécial 464b de 2017 sur l'attitude des Européens à l'égard de la sécurité, disponible à l'adresse https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/80698 et le rapport Eurobaromètre spécial 499 de 2019 sur les attitudes des Européens à l'égard de la cyber sécurité, disponible à l'adresse https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/89100

[2] Voir le rapport d'Europol d'avril 2020 intitulé «Catching the virus cybercrime, disinformation and the COVID-19 pandemic», disponible à l'adresse https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

[3] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_fr.pdf

la nécessité d'intensifier la coopération transfrontière pour combler les failles de la lutte menée contre les formes graves de criminalité et le terrorisme. Récemment, la Commission s'est engagée à prendre des mesures concrètes dans le cadre de la stratégie pour l'union de la sécurité de 2020[4]*, notamment pour faire face à la menace de la cybercriminalité, qui évolue sans cesse. La communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide»*[5] *fournit un cadre complet pour bâtir une cybersécurité solide et lutter efficacement contre la cybercriminalité.*

Dans la stratégie pour l'union de la sécurité de 2020, la Commission reconnaît la nécessité d'une approche qui englobe l'ensemble de la société et associe toutes les parties prenantes concernées. La Commission partage donc l'avis du Sénat concernant le rôle important que les autorités répressives et judiciaires des États membres ont à jouer dans la lutte contre la cybercriminalité. Elle convient également que la coopération entre les autorités répressives et judiciaires est indispensable pour apporter une réponse efficace à la cybercriminalité, et que, pour cela, les agences et initiatives de l'Union européenne, tel le réseau judiciaire européen en matière de cybercriminalité, sont essentielles. La Commission salue l'avis du Sénat concernant le rôle d'Europol et de son Centre européen de lutte contre la cybercriminalité.

La Commission apporte un soutien constant à Europol et Eurojust en faisant en sorte qu'ils obtiennent des ressources suffisantes pour être en mesure d'avancer dans la réalisation de leurs objectifs prioritaires. Le projet de budget général de l'UE pour 2021 propose de nouveau une augmentation notable du budget des deux agences. En outre, le renforcement du rôle d'Europol en matière de recherche et d'innovation dans le domaine de la répression constitue un des objectifs de la révision à venir du règlement Europol[6]*.*

La Commission salue la reconnaissance de l'importance de l'unité de l'UE chargée du signalement des contenus sur Internet (IRU) pour l'évaluation et la suppression de contenus à caractère terroriste en ligne. Cette unité détecte et signale déjà des contenus relatifs au trafic de migrants et, en réaction à la menace grandissante que constitue l'extrémisme de droite violent, le Centre européen de lutte contre le terrorisme s'emploie à garantir une capacité d'action dans ce domaine. La Commission convient également que la base de données européenne de contenus illicites doit encore être développée et note qu'Europol a prévu une mise à niveau du système au cours de l'année 2021. La Commission prend acte de la suggestion concernant une nouvelle extension de la portée des travaux à d'autres types de contenus illicites.

---

[4] COM(2020) 605 final du 24.7.2020.

[5] JOIN(2017) 450 final du 13.9.2017.

[6] Analyse d'impact initiale (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate).

La Commission convient de la nécessité d'améliorer encore le signalement de la cybercriminalité et des infractions facilitées par les technologies de l'information et de la communication, comme la fraude en ligne, et de fournir une aide aux victimes. Elle reconnaît que le développement de plateformes facilitant les signalements, telles que celles mises en place par les autorités françaises[7], devrait être encouragé dans le respect, également, des dispositions particulières des instruments juridiques de l'UE applicables[8]. La Commission est disposée à soutenir la mise en place ou le renforcement de telles initiatives (y compris transfrontières) par un financement spécifique[9].

La Commission reconnaît pleinement l'importance d'améliorer les activités de formation pour contribuer au développement des connaissances et de l'expertise nécessaires en matière de cybercriminalité au sein des autorités répressives de toute l'Europe. Dans ce contexte, la Commission continue de soutenir l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) dans les efforts qu'elle déploie dans ce domaine primordial, notamment grâce à la Cybercrime Academy créée en son sein en 2019. De plus, la Commission soutient l'élaboration de formations spécialisées dans le domaine de la cybercriminalité et de l'informatique légale par le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG)[10]. Pour maximiser et rationaliser encore les actions de renforcement des capacités, la Commission s'est engagée, dans la stratégie de l'UE pour l'union de la sécurité récemment adoptée, à étudier des mesures visant à renforcer les capacités répressives dans le cadre des enquêtes numériques, la manière de tirer le meilleur parti possible de la recherche et du développement pour créer de nouveaux outils répressifs et en précisant comment la formation peut permettre aux membres des services répressifs et aux juges de disposer du meilleur profil de compétences.

La Commission se réjouit que le Sénat soutienne l'action de l'Agence de l'Union européenne pour la cybersécurité (ENISA) en vue d'un cadre européen de certification en matière de cybersécurité tel qu'exposé dans le règlement européen sur la cybersécurité[11]. Elle confirme la signature du protocole d'accord de 2018 entre l'ENISA, le Centre européen de lutte contre la cybercriminalité d'Europol, l'Agence européenne de défense (AED) et CERT-EU[12], ainsi que le fait que la coopération entre l'ENISA et

---

[7] Comme la plateforme Perceval (https://www.interieur.gouv.fr/Actualites/Infos-pratiques/Perceval-un-teleservice-pour-signaler-en-ligne-une-fraude-a-la-carte-bancaire) ou la plateforme PHAROS (https://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Signaler-un-contenu-suspect-ou-illicite-avec-PHAROS).

[8] À titre d'exemples, voir l'article 15 (Signalement des infractions) et l'article 16 (Aide et soutien aux victimes) de la directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.FRA).

[9] Voir, par exemple, le programme de travail annuel du Fonds pour la sécurité intérieure – Police pour 2020, qui prévoit un appel à propositions ouvert concernant des projets relatifs à la cybercriminalité.

[10] https://www.ecteg.eu/

[11] Règlement (UE) 2019/881.

[12] Voir https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance cooperation

d'autres agences compétentes en matière de justice et d'affaires intérieures devrait être renforcée.

En ce qui concerne le Parquet européen, la Commission prend acte des suggestions concernant le rôle possible de celui-ci dans la lutte contre la cybercriminalité. Si, actuellement, la priorité est de veiller à ce que le Parquet européen soit opérationnel d'ici à la fin de novembre 2020, la Commission reconnaît que les compétences de ce dernier peuvent, dans les conditions énoncées à l'article 86, paragraphe 4, du TFUE, être étendues à d'autres formes de criminalité grave ayant une dimension transfrontière, ce qui a déjà été évoqué au sujet des infractions terroristes transfrontières[13].

La Commission convient de l'importance de l'accès aux preuves électroniques pour les enquêtes pénales, en particulier à la lumière de l'utilisation croissante des technologies des communications dans les infractions pénales liées à la cybercriminalité ou facilitées par les technologies de l'information et de la communication, et prend acte de la demande du Sénat concernant l'adoption d'un régime européen de conservation des données. Elle considère toutefois que ce type de régime soulève des questions quant à la protection de la vie privée et elle évaluera la marche à suivre en fonction de l'issue des affaires pertinentes actuellement examinées par la Cour de justice de l'Union européenne.

La Commission reconnaît que la lutte contre la cybercriminalité est un effort mondial nécessitant une perspective qui dépasse les frontières de l'Union européenne. Elle partage donc l'avis du Sénat concernant l'importance de la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest) et soutient son appel pour que tous les États membres de l'UE la ratifient. Depuis la décision du Conseil de juin 2019[14]*, la Commission participe à la négociation d'un second protocole additionnel à la convention, avec pour objectif de conclure les travaux d'ici à décembre 2020. La Commission entend poursuivre sa coopération avec le Conseil de l'Europe en ce qui concerne le renforcement des capacités dans le domaine de la cybercriminalité au moyen d'un certain nombre d'initiatives de financement, comme le projet Action mondiale de lutte contre la cybercriminalité élargie (GLACY+), dans le but de renforcer les capacités des pays partenaires du monde entier à appliquer la législation sur la cybercriminalité et les preuves électroniques et d'améliorer leurs capacités à coopérer efficacement au niveau international dans ce domaine*[15].

Les échanges entre l'UE et le Royaume-Uni dans le domaine de la lutte contre la cybercriminalité sont couverts par les négociations en cours sur l'avenir de notre relation, dans le cadre du vaste partenariat de sécurité, complet et équilibré, qui est envisagé. Ce partenariat tiendra compte de la proximité géographique et de l'évolution des menaces, notamment de la grande criminalité internationale, de la criminalité organisée, du terrorisme, des cyberattaques, des campagnes de désinformation, des menaces hybrides, etc.

---

[13] COM(2018) 641 final du 12.9.2018.

[14] Décision du Conseil de 2019.

[15] https://www.coe.int/fr/web/cybercrime/glacyplus

En espérant que ces précisions répondront aux questions soulevées par le Sénat, nous nous réjouissons, par avance, de la poursuite de notre dialogue politique.

Veuillez agréer, Monsieur le Président, l'expression de notre très haute considération.

Maroš Šefčovič
Vice-président

Ylva Johansson
Membre de la Commission

AMPLIATION CERTIFIÉE CONFORME
Pour la Secrétaire générale

Martine DEPREZ
Directrice
Prise de décision & Collégialité
COMMISSION EUROPÉENNE