RÉPUBLIQUE FRANÇAISE

SÉNAT

COMMISSION
DES
AFFAIRES EUROPÉENNES

Paris, le 9 juillet 2020

AVIS POLITIQUE

relatif à la lutte contre la cybercriminalité

La commission des affaires européennes du Sénat,

Vu les articles 67 et 82 à 89 du traité sur le fonctionnement de l'Union européenne,

Vu la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001, dite convention de Budapest,

Vu la stratégie de sécurité intérieure renouvelée pour l'Union européenne 2015-2020,

Vu la communication conjointe de la Commission et de la Haute Représentante de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil du 13 septembre 2017 intitulée « Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide », JOIN (2017) 450 final,

Vu la déclaration de la Haute Représentante, au nom de l'Union européenne, sur le respect de la primauté du droit dans le cyberespace du 12 avril 2019,

Vu la résolution européenne n° 117 (2018-2019) du Sénat du 21 juin 2019 sur la coopération judiciaire en matière pénale et la mise en œuvre du Parquet européen,

Vu le rapport stratégique, dit *Internet Organized Crime Threat Assessment*, 2019 du Centre européen de lutte contre la cybercriminalité d'Europol,

Vu les conclusions pertinentes du Conseil JAI du 9 juin 2016, du Conseil Affaires générales des 15 et 16 novembre 2016, du Conseil JAI du 18 mai 2017, du Conseil Affaires générales du 20 novembre 2017, du Conseil Affaires étrangères du 16 avril 2018, du Conseil Affaires générales du 26 juin 2018, du Conseil européen du 18 octobre 2018, du Conseil Affaires générales du 19 février 2019, du Conseil Affaires générales du 19 mars 2019, du Conseil Transports, télécommunications et énergie du 3 décembre 2019 et du Conseil Affaires générales du 10 décembre 2019,

Note que la forte croissance de la cybercriminalité constitue une menace affectant l'Union européenne et ses États membres, qui recouvre des formes variées aux conséquences potentiellement très lourdes ;

Observe que le cyberespace est dépourvu de frontières, ce qui constitue un défi pour les autorités répressives et judiciaires en matière d'enquêtes et de poursuites pénales, comportant un risque élevé d'impunité ; considère par conséquent que les cybercrimes doivent être traités dans le cadre de la coopération judiciaire en matière pénale, avec l'appui du réseau judiciaire européen en matière de cybercriminalité ;

Note que l'efficacité des enquêtes et poursuites pénales relatives aux cybercrimes est particulièrement tributaire de l'obtention et de la conservation de données aux fins de preuves numériques ; regrette l'absence de régime de conservation des données au niveau de l'Union européenne ; appelle par conséquent à l'adoption d'un régime européen de conservation des données permettant de répondre aux besoins opérationnels des services répressifs et judiciaires, prenant en compte les exigences de la jurisprudence de la Cour de justice de l'Union européenne et des tribunaux nationaux et respectueux des droits fondamentaux tels que le respect de la vie privée, la protection des données à caractère personnel, la non-discrimination et la présomption d'innocence ;

Juge nécessaire, pour mieux lutter contre la cybercriminalité et assurer la cybersécurité, d'allouer aux autorités répressives et

judiciaires des États membres, à Europol et à Eurojust des ressources financières et humaines suffisantes pour faire face aux nouveaux défis que constituent les avancées technologiques et l'évolution des menaces, y compris par le renforcement des partenariats avec le secteur privé ; souligne l'importance de la formation à la sécurité numérique et considère que les agences européennes compétentes ont un rôle à jouer en la matière ;

Souligne le rôle central d'Europol et de son Centre européen de lutte contre la cybercriminalité ; invite l'ensemble des États membres à coopérer au mieux avec cette agence et à alimenter ses bases de données avec des informations complètes et de qualité ; appelle au renforcement d'Europol dans la lutte contre la cybercriminalité grâce à l'extension du champ de compétences de l'unité de référencement Internet *EU IRU* au signalement de l'ensemble des contenus illicites en ligne et à l'adaptation en conséquence de la base de données européenne de contenus illicites *IRMa*, au développement d'une plateforme de signalement des transactions bancaires frauduleuses, ainsi qu'au soutien à la création de dispositifs nationaux d'assistance aux victimes et à leur mise en réseau ; demande la mise en place rapide au sein d'Europol du laboratoire d'innovation qui permettra d'associer en amont les autorités répressives aux évolutions et au développement technologiques ;

Soutient l'action de l'ENISA en vue d'un cadre européen de certification en matière de cybersécurité ; souhaite que cette agence rejoigne le réseau des agences relevant de l'espace de liberté, de sécurité et de justice ; invite l'ENISA à renforcer sa coopération opérationnelle avec les autorités répressives et judiciaires ;

Estime que la lutte contre la cybercriminalité exige une coopération internationale efficace permettant de promouvoir la sécurité et la stabilité du cyberespace ; considère que l'amélioration de cette coopération requiert la ratification de la convention de Budapest par l'ensemble des États membres de l'Union européenne et la conclusion dans les meilleurs délais des négociations sur le deuxième protocole additionnel à cette convention ; souhaite le renforcement de la coopération entre l'Union européenne et le Conseil de l'Europe dans la lutte contre la cybercriminalité, dans le respect de leur mandat respectif ;

Estime que le Royaume-Uni doit demeurer un partenaire indispensable dans la lutte contre la cybercriminalité ; demande par

conséquent que le nouveau partenariat entre le Royaume-Uni et l'Union européenne permette d'instaurer la coopération la plus étroite possible, dans le respect de l'autonomie de l'Union européenne et de la souveraineté du Royaume-Uni, dans les domaines de la cybersécurité et de la lutte contre la cybercriminalité, y compris pour ce qui relève de la coopération judiciaire ; considère que ce nouveau partenariat devra garantir les relations du Royaume-Uni avec Europol, Eurojust et l'ENISA, ainsi que les modalités d'extradition et d'entraide judiciaire, qui remplaceront le mandat d'arrêt européen ;

Estime que l'Union européenne doit s'organiser pour poursuivre plus efficacement les cybercriminels ; constate que la territorialité de la loi pénale constitue encore trop souvent un obstacle aux poursuites, en particulier lorsque les cybercrimes impliquent plusieurs États membres ; demande par conséquent la conduite d'une réflexion approfondie sur les voies et moyens d'une extension du champ de compétences du Parquet européen à la lutte contre la cybercriminalité ; est consciente qu'une telle évolution ne pourra intervenir, le cas échéant, que si plusieurs conditions sont réunies, en particulier l'unanimité au Conseil européen, le respect du principe de subsidiarité et le fonctionnement probant du Parquet européen dans son champ initial de compétences ; estime en effet que la centralisation au Parquet européen du traitement des affaires transfrontalières de cybercriminalité permettrait une plus grande intégration du fonctionnement de l'Union européenne face à des menaces grandissantes.