# Synthèse

Plusieurs paramètres font de la lutte contre la cybercriminalité une tâche unique et difficile. Par nature, la cybercriminalité ne connaît pas de frontière et évolue rapidement, parfois avant même que les autorités nationales n'aient eu le temps de réagir. Son caractère horizontal ajoute un niveau de complexité supplémentaire: presque tous les types d'activités criminelles peuvent aujourd'hui être commis sur l'internet. En raison de la volatilité des données, il peut être difficile de recueillir des preuves électroniques de telles infractions, et des compétences spécifiques peuvent être nécessaires. La coopération judiciaire est essentielle pour garantir une conservation en temps utile des preuves électroniques et, ainsi, leur recevabilité dans les procédures judiciaires. Toutefois, la coopération judiciaire internationale peut être entravée par des différences significatives entre les cadres juridiques nationaux (par exemple concernant la pénalisation d'un comportement ou la législation en matière de conservation des données) et par des conflits de compétence juridique. Le phénomène de cybercriminalité dans son ensemble transforme la notion juridique traditionnelle du principe de territorialité en raison du caractère supranational des preuves requises pour faire aboutir les poursuites judiciaires à l'encontre des cyberdélinquants.

Par conséquent, pour répondre efficacement à la cybercriminalité au niveau national, il est souvent nécessaire de mettre en place une collaboration à plusieurs niveaux. Une coopération internationale renforcée est indispensable car le cyberespace est en soi international et transfrontière. La «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» vise à créer un cyberespace favorisant l'accès à l'internet et à assurer la croissance des marchés tout en s'efforçant de parvenir à la cyber-résilience et à lutter contre la cybercriminalité, grâce à un juste équilibre entre les droits fondamentaux des citoyens et l'État de droit ([1]). Cette communication encourage par ailleurs le recours aux outils de coopération internationale dans la lutte contre la cybercriminalité ainsi que la coopération judiciaire et policière qui y est liée dans les pays tiers à partir desquels les organisations cybercriminelles opèrent ([2]).

Les conclusions du Conseil sur la communication intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide» ([3]) complètent la stratégie de l'UE en matière de cybersécurité en insistant sur la nécessité de prévenir, dissuader et déceler les actes de cybermalveillance ainsi que d'y répondre. Elles soulignent que les autorités publiques doivent disposer des outils nécessaires pour déceler les actes de cybercriminalité, mener des enquêtes et engager des poursuites en la matière.

Eurojust s'attache à lutter contre la cybercriminalité dans le but de renforcer la coopération judiciaire dans ce domaine, en particulier en permettant un traitement plus rapide des requêtes judiciaires - élément crucial pour résoudre le problème de la volatilité des données et combler les écarts dus à l'application de règles nationales différentes en matière de conservation des données - et l'intervention du pouvoir judiciaire à un stade précoce dans les opérations de cybercriminalité afin de s'assurer que les données sont recueillies conformément aux règles applicables pendant la phase d'enquête et que, par conséquent, elles peuvent être présentées comme des preuves électroniques recevables dans le cadre de procédures judiciaires ultérieures. Par ailleurs, Eurojust assure la réalisation de produits stratégiques dans le domaine de la cybercriminalité, ou y contribue de manière significative, aidant ainsi les professionnels de ce domaine à continuer d'acquérir les compétences cyberspécifiques nécessaires ([4]).

---

([1]) Conseil de l'Union européenne, Conclusions du Conseil relatives à la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, Bruxelles, 22.7.2013 (12109/13)

([2]) Eurojust est engagée dans plusieurs projets de renforcement des capacités dans le domaine de la cybercriminalité, tels que le projet Sirius (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), le projet EuroMed Justice (https://www.euromed-justice.eu/fr/home) et le projet GLACY+ (https://www.coe.int/fr/web/cybercrime/glacyplus).

([3]) Conseil de l'Union européenne, Conclusions du Conseil sur la communication conjointe au Parlement européen et au Conseil: Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide, Bruxelles, 20.11.2017 (14435/17).

([4]) Pour plus informations, voir la partie de ce document intitulée «Publications et projets d'Eurojust dans le domaine de la

L'objectif de ce rapport est de donner une vue d'ensemble des activités d'Eurojust dans le domaine de la cybercriminalité. Les activités opérationnelles menées à bien par Eurojust apportent un excellent éclairage sur les difficultés communes auxquelles sont confrontés les professionnels de ce domaine, ainsi que sur les meilleures pratiques pour faire face à ces difficultés. Les études de cas d'Eurojust constituent une source d'information utile sur les obstacles spécifiques à la coopération judiciaire et sur la manière de les surmonter, enrichissant la discussion sur les meilleurs moyens de s'attaquer au phénomène de la cybercriminalité. Le rapport comporte ensuite un chapitre présentant des exemples concrets. Enfin, on y trouvera une liste des publications d'Eurojust et des projets présentant un intérêt dans le domaine de la cybercriminalité.

cybercriminalité».