

**Contribution du Royaume de Belgique à la Discussion thématique**

**Renforcement de l'utilisation de la preuve informatique en matière de justice pénale**

1. La Belgique a fait de la cybermenace un de ses objectifs prioritaires. Notre stratégie se concentre sur plusieurs objectifs dont la prévention qui est pour nous primordiale. Elle permet de s'attaquer aux causes profondes du phénomène et de diminuer l'afflux de dossiers criminels. A cet effet, le Centre pour la Cybersécurité en Belgique (CCB) mis sur pied en 2014, supervise, coordonne et veille à la mise en œuvre de la stratégie belge en matière de cybercriminalité.
2. Outre la prévention, la Belgique met un point d'honneur à augmenter ses moyens disponibles pour la détection et la répression afin notamment de pouvoir identifier et appréhender les auteurs de criminalité informatique, de collecter les preuves électroniques, de cartographier et de démanteler les infrastructures criminelles, de saisir et confisquer les actifs illégaux et de poursuivre et sanctionner justement les « *suspects* ».
3. Parmi les initiatives déjà entreprises par la Belgique, il y a notamment l'investissement supplémentaire dans certaines techniques d'enquêtes spéciales comme l'interception des communications électroniques, qui reste un élément crucial de la lutte contre la criminalité organisée. La Belgique est également en train de revoir son cadre juridique relatif à la conservation des données.
4. D'un point de vue moral et politique, la Belgique s'attèle à trouver le juste équilibre entre, d'une part, l'efficacité des moyens d'investigation, le traitement des preuves électroniques à des fins de détection, de répression ainsi qu'à des fins judiciaires et, d'autre part, le respect et la protection des droits humains, dont la garantie est pour nous essentielle et inviolable.
5. En ce qui concerne les infractions informatiques, notre législateur a fait en sorte d'utiliser une terminologie technologiquement neutre de façon à ce que les infractions puissent s'appliquer aux technologies tant actuelles que futures. Ainsi, en principe, notre droit pénal matériel devrait couvrir les nouvelles formes de criminalité dans ce domaine.
6. Au niveau des bonnes pratiques de récolte de preuves électroniques, nous pouvons mentionner l'affaire SKY-ECC, qui est une parfaite illustration de l'importance des preuves électroniques dans les enquêtes criminelles et des défis auxquels la police et les autorités judiciaires sont aujourd'hui confrontés face à une criminalité organisée qui évolue sans cesse et surfent sur les progrès techniques et technologiques pour gagner en efficacité et se spécialiser dans certaines activités.

7. Les autorités judiciaires et les polices belges, néerlandaises et françaises ont mené avec succès des enquêtes conjointes sur le fournisseur de service SKYE CC, société canadienne, qui vendait des cryptophones dans le monde entier à des organisations criminelles, utilisés principalement pour le trafic international de cocaïne. Grâce aux interceptions effectuées et à des efforts technologiques exceptionnels, plus de la moitié des communications ont pu être rendues lisibles. Pratiquement toutes les communications échangées étaient d'origine criminelle, et pas moins d'un quart des utilisateurs criminels étaient actifs en Belgique et aux Pays-Bas.
8. La police et la justice belges ont dû se réorganiser et se réinventer en urgence afin de pouvoir poursuivre et traiter cet immense dossier, où elles font face à une montagne de données et de preuves numériques. La police judiciaire fédérale a dû élaborer un plan de réforme, de recrutement et d'investissement afin de se préparer aussi structurellement aux enquêtes dans le monde numérique, impliquant le big data. Plus de 600 équivalents temps plein travaillent sur ce dossier. Par ailleurs, les forces de l'ordre ont notamment du coopérer avec le secteur privé (des opérateurs mais aussi avec une spin-off d'une université belge afin de développer des algorithmes pour aider les analystes de la police à exploiter les données SKY).
9. Ainsi, c'est notamment grâce à une bonne coopération policière internationale, à une coopération avec le secteur privé, au recours à de nouvelles techniques d'enquêtes se basant notamment sur l'IA, ainsi qu'à une réforme dans la manière de procéder de la police judiciaire et des autorités judiciaires que dans le cadre de cette enquête SKY-ECC, plus de 90 tonnes de cocaïne ont pu être saisies, ainsi que de l'argent en espèces et des biens d'une valeur totale de près de 60 millions d'euros. Plusieurs dizaines de cas de corruption ont également été mis au jour. À ce jour, plusieurs centaines de millions de messages ont déjà été déchiffrés sur les milliards de messages qui avaient été interceptés. Et les informations obtenues ont été partagées par la Belgique avec 22 pays.
10. Au niveau des bonnes pratiques ciblant les abus d'enfants, la Belgique observe que l'exploitation sexuelle des enfants en ligne a pris des proportions encore plus alarmantes depuis le début de la crise du Covid.
11. En effet, Child focus, fondation belge créée en 1998, qui traite les disparitions et l'exploitation sexuelle d'enfants, a reçu un nombre record de 2 147 signalements d'images d'abus sexuels sur mineurs. Une augmentation de plus de 50 % par rapport à 2019. Pendant la période de confinement en 2020, le nombre de cas signalés a même triplé. Par ailleurs, Child Focus a traité 129 dossiers de sexting non consensuel, 91 cas de sextorsion (une pratique consistant à extorquer des faveurs sexuelles ou de l'argent en menaçant la victime de diffuser un contenu personnel sexuellement explicite) et 43 signalements de grooming (ou "pédopiégeage", soit le fait pour un adulte de construire une relation avec un enfant, en ligne ou hors ligne, dans le but de faciliter un contact sexuel avec cet enfant).
12. L'innovation et la technologie jouent un rôle majeur dans la lutte contre l'exploitation sexuelle des enfants en ligne. L'identité des auteurs ou des victimes est souvent inconnue. Dans certains cas, les auteurs ont déjà été arrêtés ou condamnés, mais les images d'abus sexuels sur mineurs continuent malgré tout de circuler.

13. Pour faire face à ce phénomène, la Belgique vient de revoir son cadre légal. Une loi sur la réforme du droit pénal sexuel vient d'être adoptée en mars 2022, elle comprend une nouvelle section sur l'exploitation sexuelle des mineurs, qui regroupe la plupart des infractions à caractère sexuel dont la victime mineure est un élément constitutif. Les constats de la Convention de Lanzarote ont servi de point de départ à cette section.
14. De plus, la Belgique et participe à l'élaboration d'instruments régionaux et international en la matière et elle se tient au courant des développements de bonne pratique en la matière.
15. Sur le terrain, les services compétents travaillent d'arrache-pied, entre autres, pour traiter les images d'abus sexuels sur mineurs rapidement, les mettre hors ligne et, si possible, identifier les auteurs et les victimes. Des outils numériques puissants tels qu'Arachnid peuvent leur être très utiles.. Arachnid traque automatiquement les images d'éventuels abus sexuels sur mineurs. Non seulement les victimes et les citoyens peuvent signaler directement le matériel, après quoi Arachnid parcourt l'Internet à la recherche de ces images, mais l'outil est également capable de filtrer de manière proactive les images sur l'open web et le dark web, les forums et les groupes de chats privés. Les images aboutissent dans ce que l'on appelle « Arachnid Orb », où des organisations et des services nationaux du monde entier, tels que Child Focus, les analysent. S'il s'avère que les images sont effectivement des images d'abus sexuels, nos autorités compétentes bloqueront le site web ou d'autres canaux et mettront les images hors ligne en coopération avec les fournisseurs et d'autres plateformes en ligne.
16. La coopération internationale est essentielle pour gagner cette bataille. Plus d'analyses signifie non seulement plus de suppression d'images d'abus, mais aussi plus de poursuites. Arachnid travaille en étroite collaboration avec Interpol et Europol, entre autres, qui transmettent des informations utiles sur les auteurs et les victimes aux parquets compétents du monde entier.