Version 5 juillet 2024

Adhérer à la Convention sur la cybercriminalité : les avantages

La Convention sur la cybercriminalité

La Convention sur la cybercriminalité (« Convention de Budapest ») est considérée comme la norme internationale la plus complète à ce jour puisqu'elle offre un cadre complet et cohérent en matière de cybercriminalité et de preuves électroniques. Elle fait office de ligne directrice pour tout pays élaborant une législation exhaustive en matière de lutte contre la cybercriminalité, mais aussi de cadre pour la coopération internationale entre ses États parties.

La Convention de Budapest prévoit : i) l'incrimination des actes de cybercriminalité, y compris l'accès illégal, l'atteinte à l'intégrité des données et du système, la fraude informatique et la pornographie enfantine ; ii) des outils de droit procédural visant à améliorer l'efficacité des enquêtes en matière de cybercriminalité et à obtenir plus aisément des preuves électroniques ; iii) des procédures de coopération internationale efficaces. La Convention est ouverte à l'adhésion de tous les États.

La Convention est complétée par un premier Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189) et un deuxième Protocole additionnel sur le renforcement de la coopération internationale et de la divulgation de preuves électroniques (CETS 224).

Les États qui ont participé aux négociations de la Convention (les membres du Conseil de l'Europe, l'Afrique du Sud, le Canada, les États-Unis et le Japon) peuvent la signer et la ratifier. En vertu de l'article 37, tout autre État peut devenir partie en « adhérant » à la Convention s'il est prêt à l'appliquer.

La procédure d'adhésion se décompose comme suit :

1. Une fois qu'une loi ou qu'un projet de loi indique qu'un État a déjà transposé les dispositions de la Convention de Budapest dans son droit interne ou qu'il est susceptible de le faire, le ministre des Affaires étrangères (ou tout autre représentant habilité) envoie une lettre au Secrétaire général du Conseil de l'Europe pour faire part de la volonté de son État d'adhérer à la Convention.
2. Une fois que les États actuellement parties à la Convention sont parvenus à un consensus, l'État concerné est invité à y adhérer.
3. Les autorités de l'État concerné mènent à leur terme les procédures internes comme pour toute autre ratification de traité international avant de déposer l'instrument d'adhésion près le Conseil de l'Europe.

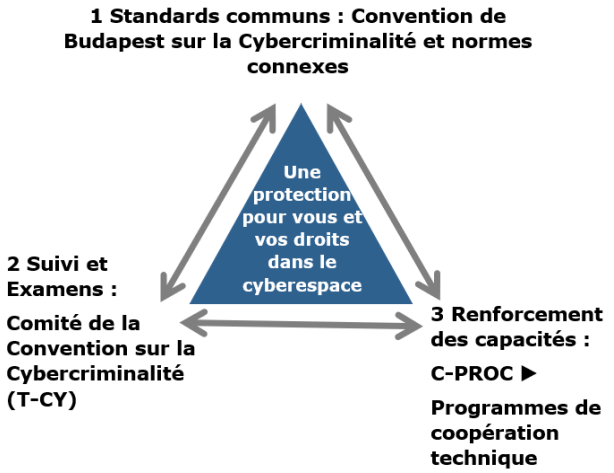
Que l'on devienne Partie par ratification ou par adhésion, le résultat final est le même. Les Parties à la Convention peuvent également devenir Parties aux deux Protocoles sans qu'il soit nécessaire de présenter une nouvelle demande d'adhésion.

En juin 2024, 75 États étaient parties à la Convention (des États européens ainsi que l'Argentine, l'Australie, le Bénin, le Brésil, le Cameroun, le Canada, le Cap Vert, le Chili, la Colombie, le Costa Rica, les États-Unis, les Fidji, le Ghana, la Grenade, Israël, le Japon, le Kiribati, l'Ile Maurice, le Maroc, le Nigeria, le Panama, le Paraguay, le Pérou, les Philippines, la République dominicaine, le Sénégal, le Sierra Leone, le Sri Lanka et les Tonga), deux autres l'avaient signée (l'Irlande et l'Afrique du Sud) et 16 pays avaient été invités à y adhérer (le Burkina Faso, la Côte d'Ivoire, l'Equateur, le Guatemala, le Kazakhstan, la république de Corée, la Nouvelle Zélande, le Mexique, le Mozambique, la République du Niger, le Rwanda, la Sierra Léone, le Timor oriental, Trinité-et-Tobago, la Tunisie, Sao Tomé-et-Principe, l'Uruguay et Vanuatu).

Ces 93 États sont des membres (pour les Parties) ou des observateurs (les signataires et les invités) du Comité de la Convention sur la cybercriminalité (T-CY).

Le T-CY est notamment chargé d'évaluer l'application de la Convention par les Parties, d'adopter des notes d'orientation et d'élaborer d'autres instruments juridiques.

Les programmes de renforcement des capacités, qui sont gérés par le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) en Roumanie, aident les pays du monde entier à se doter des capacités nécessaires pour appliquer la Convention de Budapest ou donner suite aux recommandations du Comité.



Avantages pour les Parties

Tous les pays peuvent se servir de la Convention de cybercriminalité comme d'une ligne directrice, d'un aide-mémoire ou d'un modèle de loi et bon nombre d'entre eux le font déjà. Toutefois, devenir un État partie à la Convention offre d'autres avantages :

- La Convention offre un **cadre juridique pour la coopération internationale**, non seulement en ce qui concerne la cybercriminalité (infractions contre et au moyen d'ordinateurs), mais aussi en ce qui concerne toute infraction impliquant une preuve électronique.
- Les parties à la convention peuvent signer et ratifier le deuxième Protocole additionnel à la convention de Budapest, qui fournit des **outils supplémentaires et accélérés pour renforcer la coopération et la divulgation des preuves électroniques**, comme la coopération directe avec les fournisseurs de services au-delà des frontières ou la coopération dans les situations d'urgence.

- Les États parties sont **membres du Comité de la Convention sur la cybercriminalité (T-CY)** et échangent des informations et des données d'expérience, évaluent l'application de la Convention ou interprètent ses dispositions grâce aux notes d'orientation.
- Même si un État n'a pas pris part aux négociations de cette-dernière, il peut, s'il est nouvellement partie, participer aux **négociations des futurs instruments** et à l'évolution de la Convention de Budapest.
- Les États parties à la Convention s'engagent dans une **coopération loyale et efficace**. Il semble que les entités du secteur privé sont également plus susceptibles de coopérer avec les autorités de justice pénale des Parties à la Convention dans la mesure où celles-ci doivent mettre en place un cadre juridique interne sur la cybercriminalité et les preuves électroniques, y compris s'agissant des garanties prévues à l'article 15.
- Les États qui demandent à adhérer à la Convention ou qui y ont adhéré peuvent devenir des **pays prioritaires pour les programmes de renforcement des capacités**. Cette assistance technique vise à favoriser la pleine mise en œuvre de la Convention et à renforcer leurs capacités en matière de coopération internationale.

Les faits observés au cours des 20 années qui se sont écoulées depuis l'ouverture à la signature révèlent que l'adhésion à la Convention ne comporte aucun inconvénient.

Le premier protocole additionnel sur la xénophobie et le racisme

Le premier protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STCE 189) entraîne une extension du champ d'application de la Convention sur la cybercriminalité, y compris ses dispositions de fond, de procédure et de coopération internationale, afin de couvrir également les infractions de propagande raciste ou xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel de ces comportements, le protocole vise à améliorer la capacité des Parties à faire usage des moyens et des voies de coopération internationale prévus par la Convention dans ce domaine.

Les avantages pour les parties sont les suivants :

- Un cadre juridique plus solide : le protocole renforce le cadre juridique de la lutte contre la xénophobie et le racisme dans le cyberespace en fournissant un ensemble de lignes directrices claires pour a criminalisation de ces crimes.
- Une coopération internationale renforcée : le protocole encourage la coopération internationale dans les enquêtes et les poursuites des crimes liés à la xénophobie et au racisme en ligne, ce qui est particulièrement important étant donné la nature transfrontalière de nombre de ces infractions.
- Une protection accrue des victimes : la criminalisation de la xénophobie et du racisme en ligne permet aux victimes de demander justice et de bénéficier d'un soutien.

Le premier protocole additionnel a été ouvert à la signature le 23 janvier 2003. En juin 2024, 36 États étaient parties et 10 autres avaient signé le premier protocole.

Le deuxième protocole additionnel sur les preuves électroniques

Compte tenu de la prolifération de la cybercriminalité et de la complexité croissante de l'obtention de preuves électroniques qui peuvent être stockées dans des juridictions étrangères, multiples, mouvantes ou inconnues, les pouvoirs des services répressifs sont limités par les frontières territoriales. Par conséquent, seule une très faible part de la cybercriminalité signalée aux autorités de justice pénale donne lieu à des décisions de justice. En réponse, le deuxième protocole additionnel à la Convention sur la cybercriminalité (STCE 224) fournit une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaine et pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, une coopération immédiate dans les situations d'urgence, des outils d'assistance mutuelle, ainsi que des garanties en matière de protection des données personnelles.

Les principales caractéristiques du protocole sont les suivantes :

- Des demandes directes aux bureaux d'enregistrement dans d'autres juridictions pour obtenir des informations sur l'enregistrement des noms de domaine
- Des injonctions directes aux fournisseurs de services dans d'autres juridictions pour obtenir des informations sur les abonnés
- Des moyens plus efficaces d'obtenir des informations sur les abonnés et des données sur le trafic grâce à une coopération entre gouvernements
- Une coopération accélérée dans les situations d'urgence
- Des équipes d'enquête conjointes et d’enquêtes conjointes
- La vidéoconférence

Le deuxième protocole additionnel a été ouvert à la signature le 12 mai 2022. En juin 2024, 46 États avaient signé le deuxième protocole (Albanie, Allemagne, Andorre, Argentine, Arménie, Autriche, Belgique, Bulgarie, Canada, Cap Vert, Chili, Colombie, Costa Rica, Croatie, Espagne, Estonie, États-Unis d'Amérique, Finlande, France, Ghana, Grèce, Hongrie, Ile Maurice, Islande, Italie, Japon, Lituanie, Luxembourg, Malte, Maroc, Monténégro, Macédoine du Nord, Pays-Bas, Portugal, République de Moldova, République dominicaine, Roumanie, Royaume-Uni, Serbie, Sierra Leone, Slovénie, Sri Lanka, Suède, Tchéquie et Ukraine) et deux États l'ont également ratifié (Japon et Serbie).

Contact

Conseil de l’Europe
Division de la cybercriminalité, DG I

Strasbourg, France
cybercrime@coe.int

www.coe.int/cybercrime