

CONSEIL DE L'EUROPE

**LUTTE CONTRE LA
CYBERCRIMINALITÉ**



La convention sur la cybercriminalité

La Convention sur la cybercriminalité, également connue sous le nom de "Convention de Budapest", est considérée comme l'accord international le plus complet et le plus cohérent à ce jour en matière de cybercriminalité et de preuves électroniques. Elle sert de ligne directrice à tout pays qui élabore une législation nationale sur la cybercriminalité et de cadre à la coopération internationale entre les États parties à ce traité.

La **Convention de Budapest** prévoit :

- la criminalisation des comportements ;
- des pouvoirs procéduraux pour enquêter sur la cybercriminalité et obtenir des preuves électroniques en rapport avec tout délit ;
- une coopération internationale efficace.

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** relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE N° 224).

Le traité est ouvert à l'adhésion de tout pays. En effet, en vertu de l'article 37, tout État peut devenir partie par "adhésion" s'il est prêt à mettre en œuvre les dispositions du traité. En outre, un État peut devenir partie par "ratification" : qu'il devienne partie par ratification ou par adhésion, la finalité est la 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, 2 pays l'avaient signée et 16 pays avaient été invités à y adhérer. Ces États participent en tant que membres (Parties) ou observateurs (signataires ou invités) au Comité de la Convention sur la cybercriminalité (T-CY).

Le **T-CY (Comité de la Convention sur la cybercriminalité)** évalue notamment la mise en œuvre de la Convention par les Parties, adopte des notes d'orientation ou prépare des instruments juridiques supplémentaires.

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

Avantages pour les parties

Tout pays peut utiliser la Convention sur la cybercriminalité comme une ligne directrice, une liste de contrôle ou une loi modèle, et un grand nombre d'entre eux l'ont déjà. 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** ; Les Parties sont membres du T-CY et partagent des informations et des expériences, évaluent la mise en œuvre de la Convention, ou interprètent la Convention par le biais de notes d'orientation ; chaque État membre est en mesure de participer à la négociation de futurs instruments et à l'évolution de la Convention ; les Parties à la Convention s'engagent les unes avec les autres dans une coopération fiable et efficace.

En outre, les **entités du secteur privé** sont également plus susceptibles de coopérer avec les autorités de justice pénale des Parties à la Convention, puisque les Parties doivent disposer d'un cadre juridique national sur la cybercriminalité et les preuves électroniques, qui comprend également les garanties de l'article 15.

En outre, les États qui demandent à adhérer ou qui ont adhéré peuvent devenir des pays

prioritaires pour les **programmes de renforcement des capacités**. Cette assistance technique vise à faciliter la pleine mise en œuvre de la Convention et à renforcer la capacité à coopérer au niveau international.

Le premier protocole additionnel

Le Premier Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE N°189) entraîne une extension du champ d'application de la Convention sur la cybercriminalité, y compris de ses dispositions matérielles, procédurales 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 ce type de comportement, le protocole vise à améliorer la capacité des parties à utiliser les moyens et les voies de coopération internationale prévus par la convention dans ce domaine.

Les avantages pour les signataires sont nombreux :

- **Un cadre juridique solide** pour lutter contre la xénophobie et le racisme dans le cyberspace en fournissant un ensemble de lignes directrices claires pour les enquêtes et les poursuites relatives à ces crimes.
- **Renforcement de la coopération internationale** dans les enquêtes et les poursuites relatives aux crimes liés à la xénophobie et au racisme en ligne, ce qui est particulièrement important compte tenu de la nature transfrontalière de bon nombre de ces infractions.
- **Une protection accrue des victimes** de la xénophobie et du racisme en ligne, et des mesures efficaces pour veiller à ce qu'elles puissent accéder à la justice et bénéficier d'un soutien.
- **une meilleure sensibilisation** et éducation aux méfaits des actes xénophobes et racistes commis par le biais de systèmes

informatiques. En outre, le protocole encourage la mise en œuvre de mesures visant à prévenir ces formes de haine.

Le Premier Protocole additionnel a été ouvert à la signature le 23 janvier 2023. En juin 2024, 10 États l'avaient signé et 36 États au total y avaient adhéré.

Le deuxième protocole additionnel

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 petite partie 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 afin d'obtenir des informations sur les abonnés**, des moyens efficaces pour obtenir des informations sur les abonnés et des données relatives au trafic, une coopération immédiate en cas d'urgence, des outils d'assistance mutuelle, ainsi que des garanties en matière de protection des données à caractère personnel.

Les principales caractéristiques du protocole sont, entre autres, la demande directe aux bureaux d'enregistrement d'autres juridictions d'obtenir des informations sur l'enregistrement des noms de domaine ; la coopération directe avec les fournisseurs de services d'autres juridictions afin d'obtenir des informations sur les abonnés ; la coopération entre gouvernements et la coopération rapide dans les situations d'urgence ; les équipes d'enquête conjointes et les enquêtes conjointes.

Le Deuxième Protocole additionnel a été ouvert à la signature le 12 mai 2022. En juin 2024, 46 États l'avaient signé et 2 États l'avaient ratifié.

- La Convention sur la cybercriminalité,

également connue sous le nom de "Convention de Budapest", est considérée comme l'accord international le plus complet et le plus cohérent à ce jour en matière de cybercriminalité et de preuves électroniques.

La Convention est complétée par le 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 le Deuxième Protocole additionnel relatif au renforcement de la coopération internationale et de la divulgation de preuves électroniques (STCE N°224).

CONSEIL DE L'EUROPE

**GOUVERNANCE
NUMÉRIQUE**

Protéger les
droits humains,
la démocratie
et l'État de
droit dans
l'environnement
numérique

Médias sociaux



Council of Europe
Digital Governance

FRA