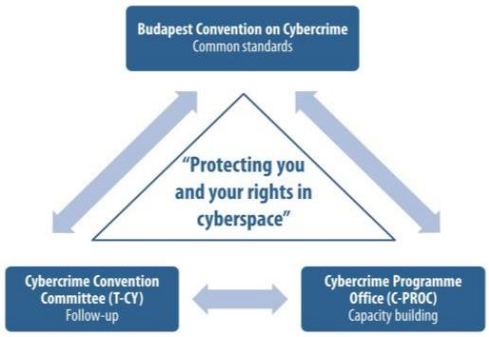
Version 14 avril 2021

**Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques :**

# Vers un protocole à la Convention de Budapest

La Convention de Budapest sur la Cybercriminalité a été ouverte à la signature en 2001. Depuis, le nombre des États Parties ne cesse de croître et tout pays en mesure d'en appliquer les dispositions peut demander à y adhérer. En avril 2021, 65 États étaient devenus parties à la Convention, et 12 autres l'avaient signée ou avaient été invités à y adhérer. En plus de ces 72 États, 30 autres sont considérés comme ayant une législation quasiment alignée à ce Traité et, de plus, 50 autres états ont partiellement adaptée leur législation à ce dernier. La Convention de Budapest est complétée par un Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.




La qualité de la mise en œuvre de la Convention de Budapest est évaluée par le Comité de la Convention sur la cybercriminalité (T-CY) représentant les Parties à cette Convention, avec la participation des signataires et des États invités à y adhérer en qualités d'observateurs.

Les États qui se sont engagés à coopérer au titre de cette Convention bénéficient en outre d'un soutien dans le cadre de projets de consolidation de capacités gérés par le Bureau du Conseil de l'Europe pour le Programme sur la cybercriminalité (C-PROC) en Roumanie.

L'évolution des technologies de l'information et de la communication, si elle a ouvert des possibilités inouïes pour l'humanité, pose également des défis, notamment pour la justice pénale et donc pour l'État de droit dans le cyberespace. Alors que prospèrent la cybercriminalité et les autres infractions impliquant des preuves électroniques sur des systèmes informatiques, et que ces preuves sont de plus en plus stockées sur des serveurs hébergés dans des juridictions étrangères, multiples, fluctuantes ou inconnues, autrement dit dans le Cloud (« Nuage »), les pouvoirs des services répressifs sont limités par les frontières territoriales. Par conséquent, seule une très faible part des actes de cybercriminalité signalés aux autorités de justice pénale donne lieu à des décisions de justice, et le plus souvent, les victimes n'obtiennent pas justice.

Les Parties à la Convention de Budapest Convention cherchent depuis quelque temps déjà des solutions dans ce domaine : de 2012 à 2014, un groupe de travail sur l'accès transfrontière aux données a travaillé sur la question, puis de 2015 à 2017, le flambeau a été repris par le Groupe sur les preuves dans le Nuage. En 2014, ils ont également adopté une série de Recommandations visant à renforcer l'efficacité de l'entraide judiciaire et, en 2017, une Note d'orientation sur l'article 18 de la Convention de Budapest concernant les ordonnances de production relatives aux informations sur les abonnés. Cette Note explique comment les injonctions de produire nationales pour des informations relatives aux abonnés

peuvent être émises à l'intention d'un fournisseur de services national indépendamment du lieu où se trouvent les données (article 18.1.a) et à l'intention de fournisseurs offrant un service sur le territoire d'une Partie (article 18.1.b).

En 2017, le Groupe sur les preuves dans le Nuage a recommandé la préparation d'un nouveau deuxième protocole additionnel à la Convention de Budapest. En juin 2017, le T-CY s'est entendu sur un Mandat pour la préparation du protocole et les négociations ont commencé en septembre 2017. Depuis lors, le T-CY a tenu 9 plénières de rédaction du protocole et 16 sessions du "Groupe de rédaction du Protocole" pour préparer le texte du projet de protocole. Suite aux restrictions liées à COVID-19, entre avril 2020 et avril 2021, plus de 50 réunions de sous-groupes du Groupe de rédaction du Protocole se sont tenues en format virtuel.

Chaque fois que des projets d'articles avaient été provisoirement approuvés par la plénière de rédaction du protocole, ils étaient rendus publics et les parties prenantes de la société civile, de la protection des données et du secteur du Net étaient invitées à soumettre des commentaires ou à participer à des auditions. Cinq cycles de consultations de ce type ont eu lieu entre juillet 2018 et décembre 2020. Bon nombre des contributions reçues ont été prises en compte dans le texte du dispositif ou ont donné lieu à des clarifications supplémentaires dans le rapport explicatif.

Le 12 avril 2021, la Plénière de rédaction du protocole a convenu de publier un projet complet du protocole et d'inviter les parties prenantes à fournir des commentaires supplémentaires et à participer à une réunion en ligne le 6 mai 2021.

Le projet de "Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et à la divulgation des preuves électroniques" prévoit :

- Une coopération directe avec les fournisseurs de services (article 6) et les entités fournissant des services d'enregistrement de noms de domaine (article 7) dans d'autres Parties pour la divulgation d'informations permettant d'identifier des suspects ;
- Des formes accélérées de coopération entre les Parties pour la divulgation d'informations sur les abonnés et de données relatives au trafic (article 8) ;
- La coopération et la divulgation accélérées dans les situations d'urgence (articles 9 et 10) ;
- Des outils supplémentaires d'entraide (articles 11 et 12) ;
- La protection des données et d'autres garanties de l'État de droit (articles 13 et 14).

Le champ d'application de ce Protocole - comme celui de la Convention sur la cybercriminalité - est limité "aux enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des systèmes et des données informatiques, et à la collecte de preuves sous forme électronique d'une infraction pénale" (article 2).

Outre les articles 13 et 14, une série d'autres garanties ont été intégrées dans les dispositions individuelles, et les Parties au Protocole peuvent faire usage de réserves et de déclarations si leur droit interne l'exige. Par exemple, elles peuvent exiger une notification simultanée lorsqu'une commande est envoyée directement à un prestataire de services sur leur territoire (voir article 7, paragraphe 5).

En conséquence, le projet actuel concilie (a) la nécessité d'une réponse efficace de la justice pénale pour renforcer l'État de droit et protéger les victimes et leurs droits en ligne, et (b) la nécessité de solides garanties en matière de droits de l'homme et d'État de droit, notamment pour la protection des données à caractère personnel.

Les dispositions de ce protocole seront utiles sur le plan opérationnel et politique et permettront à la Convention de Budapest de continuer à défendre un Internet libre où les gouvernements s'acquittent de leur obligation de protéger les personnes et leurs droits dans le cyberespace.

**Pour de plus amples informations, veuillez contacter :**


Le Secrétariat du Comité de la Convention sur la cybercriminalité
Division Cybercriminalité, DGI
Conseil de l'Europe

Strasbourg, France
Email cybercrime@coe.int


**www.coe.int/cybercrime**