GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Bucarest, le 28 octobre 2016

Priorités stratégiques pour la coopération en matière de cybercriminalité et de preuve électronique dans les États participants au projet GLACY

[Adoptées à la conférence de clôture du projet GLACY –
Action globale sur la cybercriminalité
Bucarest, 26-28 octobre 2016]

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Table des matières

Contact
Bureau de Programme du Conseil de l'Europe sur la cybercriminalité (C-PROC)
Téléphone : +33-3-9021-4506
Mail : alexander.seger@coe.int

Déclaration sur les priorités stratégiques pour la coopération en matière de cybercriminalité

Nous, représentants de l'Ile Maurice, Maroc, Philippines, Sénégal, Afrique du Sud, Sri Lanka et Tonga participant à l'Action globale sur la cybercriminalité (GLACY)

- Réunis à la Conférence de clôture du projet GLACY, à Bucarest, en Roumanie, le 28 octobre 2016 ;

- Soulignant l'importance de la Convention de Budapest sur la cybercriminalité en tant que ligne directrice pour l'élaboration d'une législation nationale et d'un cadre de coopération internationale en matière de cybercriminalité et de preuve électronique ;

- Conscients des avantages que présentent les technologies de l'information et de la communication (TIC) qui sont en train de transformer notre société ;

- Préoccupés par les dangers de la cybercriminalité en ce qu'elle mine la confiance dans les TIC et pose une menace pour les droits de l'homme et la sécurité des personnes ;

- Conscients de la valeur du Protocole additionnel à la Convention de Budapest sur la cybercriminalité, relatif au racisme et à la xénophobie pour lutter contre les discours de haine contribuant à la radicalisation et à l'extrémisme violent ;

- Reconnaissant l'obligation positive des gouvernements de protéger les personnes contre la cybercriminalité et autres infractions liées à la preuve électronique ;

- Soucieux du respect des droits et libertés fondamentales ainsi que du droit à la vie privée, en particulier à l'égard du traitement des données à caractère personnel**,** dans la lutte contre le crime ;

- Considérant la nécessité de la coopération entre secteur public et secteur privé pour prévenir et maîtriser la cybercriminalité et protéger les systèmes informatiques ;

- Convaincus que, pour pour être efficaces, les mesures en matière de cybercriminalité et de preuve électronique exigent une coopération régionale et internationale efficace ;

- Reconnaissants de l'appui fourni par l'Union européenne et le Conseil de l'Europe par le biais du projet GLACY – Action globale sur la cybercriminalité ;

- Nous appuyant sur les progrès réalisés et sur les mesures déjà prises par nos États contre la cybercriminalité, tout en soulignant la nécessité des efforts supplémentaires ;

Nous adoptons

les priorités stratégiques sur la coopération en matière de cybercriminalité présentées à cette conférence et nous engageons à

- Mener en matière de cybercriminalité des stratégies permettant d'opposer une réponse efficace aux infractions commises sur et au moyens des ordinateurs et aux infractions impliquant des preuves électroniques ;

- Adopter une législation complète et efficace sur la cybercriminalité, compatible avec les exigences de l'Etat de droit et des droits de l'homme ;

- Renforcer la spécialisation des services de répression et de poursuite dans le domaine de la cybercriminalité et de la preuve électronique ;

- Mettre en œuvre des stratégies durables de formation des services répressifs ;

- Encourager la formation des juges et des procureurs dans le domaine de la cybercriminalité et de la gestion des preuves électroniques en relation avec tout crime ;

- Mener des stratégies complètes de protection des enfants contre les abus et l'exploitation sexuelle en ligne ;

- Renforcer la coopération avec le secteur privé, notamment entre les services répressifs et les fournisseurs de services Internet et/ou autres fournisseurs de services de communication ;

- Coopérer de façon efficace aux niveaux régional et international ;

- Partager notre expérience avec d'autres régions du monde, en vue de renforcer les capacités de lutte contre la cybercriminalité ;

- Développer la prise de conscience à la Convention de Budapest sur la cybercriminalité au niveau mondial.

Déclaration adoptée par acclamation à

Bucarest, Roumanie, le 28 octobre 2016

Annexe : priorités stratégiques pour la coopération en matière de cybercriminalité

Priorité stratégique 1 : Intégrer la cybercriminalité et la preuve électronique à tous les échelons du système de justice pénale

Dans une société que les TIC sont en train de transformer, la sécurité informatique est devenue une priorité politique pour de nombreux gouvernements, conscients de l'obligation positive de protéger les personnes et leurs droits contre la cybercriminalité et de traduire les délinquants en justice. L'ampleur du phénomène de la cybercriminalité et le recours croissant à la preuve électronique dans les enquêtes et les poursuites liées aux formes traditionnelles de criminalité nécessitent donc de relever les défis posés par la lutte contre la cybercriminalité, au même titre que celle menée contre les autres formes de criminalité et qui portent atteinte à la sûreté de l'état, à la stabilité économique et au bien-être des personnes et de la société.

A cet égard, les autorités compétentes sont invitées à envisager les mesures suivantes :

- **Adopter des politiques et des stratégies en matière de cybercriminalité et de cybersécurité visant à garantir l'efficacité de la réponse du système de justice pénale** aux attaques commises contre et par les TIC et à toute infraction impliquant des preuves électroniques. Envisager comme composants de ces politiques et stratégies des éléments tels que les mesures de prévention, lois, unités spécialisées au sein des services répressifs et de poursuite, coopération interinstitutionnelle, formation de la police et des juges, coopération entre les secteurs public et privé, coopération internationale efficace, investigations financières, lutte contre la fraude et le blanchiment d'argent et protection des enfants contre la violence sexuelle.

- **Sensibiliser aux défis de la cybercriminalité et de la preuve électronique et promouvoir des mesures de prévention** à tous les niveaux. Notamment sensibiliser les responsables gouvernementaux et parlementaires à la preuve électronique en tant que défi transversal.

- **Garantir la compatibilité avec les droits de l'homme et l'Etat de droit** de toute mesure prise en matière de lutte contre la cybercriminalité.

- **Créer des plates-formes de signalement public** et intégrer le signalement de la cybercriminalité dans les plates-formes et systèmes de signalement existants. Le but est de mieux comprendre les menaces et les tendances de la cybercriminalité et de faciliter les mesures de justice pénale. Ces plates-formes permettront également d'informer le public et de lancer des alertes.

- **S'engager dans une coopération public-privé**, notamment entre les autorités répressives et les fournisseurs de service.

- **S'engager dans une coopération internationale aussi étendue que possible.** Il conviendra notamment de mettre pleinement à profit les accords bilatéraux et multilatéraux régionaux existants, en particulier la Convention de Budapest sur la cybercriminalité. Participer activement aux travaux du Comité de la Convention Cybercriminalité (T-CY).

- **Évaluer régulièrement l'efficacité des mesures de justice pénale contre la cybercriminalité et établir des statistiques**. Ces analyses aideront à évaluer et à améliorer les résultats des mesures de justice pénale et à affecter les ressources de manière efficace.

Priorité stratégique 2 : Réformes et développement législatifs continus

L'adoption d'une législation adéquate est fondamentale en ce qui concerne les mesures de justice pénale contre la cybercriminalité et l'utilisation des preuves électroniques dans les procédures. Les États participant au projet GLACY ont considérablement progressé dans l'harmonisation de leur législation avec la Convention de Budapest ; cependant, il reste beaucoup à faire pour garantir le développement continu de la législation en réponse aux nouvelles menaces et nouveaux défis que pose le cyberespace et pour mettre en œuvre les normes et garanties en la matière, telles que les normes de protection des données reconnues à l'échelle mondiale, les réglementations concernant la protection des enfants contre la violence sexuelle ou encore les mesures de lutte contre les produits de l'activité criminelle et le blanchiment de capitaux.

L'adoption d'une législation efficace respectueuse des droits de l'homme et de l'Etat de droit et son réexamen et sa mise à jour continus doivent constituer une priorité stratégique.

Les autorités compétentes sont invitées à envisager les mesures suivantes :

- **Adopter et/ou améliorer les dispositions du droit procédural afin de permettre la collecte de preuves électroniques par les services répressifs**. Ceci concerne en particulier les dispositions juridiques nationales et la mise en œuvre des réglementations sur l'injonction de produire (article 18) et la conservation rapide de données (articles 16, 17, 29 et 30) tels que prescrits par la Convention de Budapest afin de permettre un accès légal aux données détenues par des entités du secteur privé.

- **Évaluer l'efficacité de la législation.** La mise en œuvre de la législation et des réglementations dans la pratique doit être évaluée régulièrement. Les données relatives aux enquêtes, aux poursuites et aux jugements doivent être recueillies et les procédures appliquées doivent être documentées.

- **Garantir que les services répressifs sont soumis à des conditions et garanties conformes à l'article 15 de de la Convention de Budapest.** Il s'agit notamment d'instaurer un contrôle judiciaire relativement à l'ingérence mais aussi de veiller au respect des principes de proportionnalité et de nécessité.

- **Renforcer la législation relative à la protection des données** de manière conforme aux normes internationales et européennes. Les gouvernements sont encouragés à garantir que leur législation nationale de protection des données respecte les principes de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n°108) ou autres normes reconnues et applicables.

- **Compléter la législation et prendre des mesures préventives et de protection des enfants contre la violence sexuelle sur Internet**, conformément aux dispositions de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote).

- Examiner la législation en conformité avec le **Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe** commis par le biais de systèmes informatiques.

- **Adapter la législation sur les enquêtes financières, la confiscation des produits de la criminalité et du blanchiment et sur le financement du terrorisme**. Les règles et réglementations, tant générales que spécifiques au secteur, doivent notamment permettre un échange d'informations national et international rapide.

Priorité stratégique 3 : Renforcer les capacités en matière de cybercriminalité et de preuves électroniques

La cybercriminalité et le traitement des preuves électroniques requièrent une réponse spécialisées de la part des autorités de justice pénale. Les services répressifs et les autorités de poursuite doivent être à même de mener des investigations et de poursuivre les infractions commises contre des systèmes et données informatiques, les infractions commises au moyen d'ordinateurs et les infractions impliquant des preuves électroniques. Il est essentiel de comprendre que la technologie évolue tous les jours et que la charge de travail des unités spécialisées en cybercriminalité et en informatique forensique ne cesse d'augmenter. La gestion des ressources (personnels, matériel et logiciel), le maintien des compétences spécialisées et l'adaptation de ces unités aux défis émergents constituent un défi de tous les instants.

Le renforcement des unités spécialisées et leur compétence en matière de preuve électronique dans les affaires pénales doit être une priorité stratégique.

Les autorités compétentes sont invitées à envisager les mesures suivantes :

- **Créer, au sein de la police judiciaire, si ce n'est déjà fait, des unités spécialisées dans le domaine de la cybercriminalité**. Les caractéristiques et les fonctions exactes de ces unités devraient résulter d'une analyse rigoureuse des besoins et être fondées sur une base légale. Elles devraient être aisément modifiables, afin de pouvoir s'adapter aux nouveaux défis et à la demande croissante.

- **Renforcer la spécialisation des procureurs**. Envisager la création d'unités spécialisées ou d'un groupe de procureurs spécialisés dont la fonction serait de guider et d'aider les autres procureurs dans les affaires liées à la cybercriminalité et à la preuve électronique.

- **Assurer le renforcement continu des capacités en matière de criminalistique et de formation des experts,** soit dans les unités d'enquête spécialisées dans la lutte contre la cybercriminalité, soit au sein d'autres autorités compétentes.

- **Faciliter la coopération et l'échange de bonnes pratiques** entre unités spécialisées tant au niveau régional qu'international.

- **Améliorer les procédures relatives aux enquêtes en matière de cybercriminalité et de preuve électronique**. Examiner et envisager la mise en œuvre de normes et bonnes pratiques nationales et internationales, notamment les normes et directives élaborées par le Conseil de l'Europe et autres documents pertinents.

Priorité stratégique 4 : Formation des services répressifs

Les services répressifs doivent être en mesure non seulement d'enquêter sur les infractions commises sur et par les TIC mais aussi de traiter la question de la preuve électronique liée à une infraction donnée. La croissance exponentielle de l'utilisation des technologies de l'information par la société entraîne une intensification parallèle des défis posés aux autorités chargées de l'application de la loi. Il importe que tous les membres des services répressifs – des premiers intervenants aux enquêteurs experts en informatique forensique – puissent aborder la lutte contre la cybercriminalité et la question de la preuve électronique à leur niveau respectif. Des éléments de stratégie de formation ont été identifiés mais aucune stratégie cohérente n'a encore été adoptée.

L'élaboration et la mise en œuvre de stratégies de formation durables permettant d'assurer une formation des forces répressives au niveau approprié doit être une priorité stratégique.

Les autorités compétentes sont invitées à envisager les mesures suivantes :

- **Mettre en œuvre une stratégie de formation nationale.** Il s'agit de garantir que les institutions d'application des lois se dotent des compétences nécessaires pour enquêter sur les infractions de cybercriminalité, recueillir les preuves électroniques et effectuer des expertises d'informatique forensique dans le cadre de procédures pénales, coopèrent activement au niveau interinstitutionnel et contribuent à la sécurité du réseau. L'investissement dans cette formation se justifie compte tenu de la dépendance de la société aux technologies de l'information et des risques associés.

- **Inclure des règles et des protocoles pour le traitement de la preuve électronique à tous les niveaux de formation nationale.** Il est important de reconnaître que la preuve électronique joue un rôle dans toutes les activités de la cybercriminalité, de sorte que la formation permettant d'identifier et de traiter la preuve électronique représente une nécessité pour tous les agents des services répressifs et pas uniquement pour les unités spécialisées.

- **Envisager l'élaboration de programmes individuels de formation à l'intention des enquêteurs spécialisés.** L'évolution technologique et la manière dont les cyberdélinquants en abusent signifient qu'un personnel suffisamment nombreux de spécialistes hautement qualifiés est nécessaire pour effectuer des enquêtes et des examens de preuves numériques au plus haut niveau. Cela renforcerait également la position de ces experts au sein du système de justice pénale.

- **Envisager la mise en œuvre de procédures en vue de garantir l'optimisation de l'investissement en formation**. La formation d'experts en matière de lutte contre la cybercriminalité et d'informatique forensique est coûteuse. Afin d'obtenir un retour adéquat sur l'investissement en formation, les États doivent s'assurer que le personnel soit affecté – et demeure – à des postes adaptés à son niveau de connaissances et de compétences. A cette fin, il est indispensable d'élaborer des stratégies de développement des ressources humaines complémentaires des stratégies de formation.

Priorité stratégique 5 : Formation des juges

Outre les infractions commises sur et par des ordinateurs, un nombre croissant d'autres infractions impliquent des preuves stockées sur des systèmes informatiques ou autres systèmes de stockage de données, ce qui signifie que tous les juges et les procureurs devront se familiariser avec le traitement de la preuve électronique. Il existe un besoin évident de formation systématique et durable pour les juges et les procureurs en matière de cybercriminalité et de preuve électronique.

Former les juges et les procureurs à l'instruction et au jugement d'affaires liées à la cybercriminalité et à la preuve électronique doit rester une priorité stratégique.

Les autorités compétentes sont invitées à envisager les mesures suivantes :

- **Créer des programmes de formation des juges en matière de cybercriminalité et de preuve électronique.** Les institutions nationales de formation des juges et des procureurs doivent intégrer des modules de formation avancés sur la cybercriminalité et le traitement de la preuve électronique tant dans leurs programmes de formation initiale que de formation continue.

- **Adopter des mesures afin de garantir que la formation des juges en matière de cybercriminalité et de preuve électronique soit obligatoire.** Il est apparu au cours du projet que pour de nombreux modules, la formation des juges et des procureurs s'effectuait sur une base volontaire. En conséquence, il s'est fréquemment produit que les participants ne suivaient la formation que sur de brèves périodes et donc qu'ils n'en bénéficiaient pas pleinement.

- **Adapter les supports de formation existants et former les formateurs.** Des concepts et matériels pédagogiques ayant déjà été élaborés par le Conseil de l'Europe et d'autres organisations, ils pourraient être adaptés aux besoins des institutions de formation nationales. Il conviendrait de former des formateurs à la présentation des matériels.

- **Fournir aux juges des documents de référence qui pourront être utilisés lors de l'arbitrage des questions liées à la cybercriminalité**. Afin d'intégrer les connaissances en matière de cybercriminalité, un livre de référence devrait être élaboré pour accélérer le traitement des questions liées à la cybercriminalité et aux preuves électroniques.

- **Créer des dossiers de formation pour les juges et les procureurs.** Afin de garantir la meilleure utilisation possible de la formation dispensée aux juges et aux procureurs, il serait souhaitable de créer des dossiers individuels où consigner tous les cours suivis par chacun, de manière à évaluer les besoins de perfectionnement et à garantir que les bonnes formations soirent dispensées aux bonnes personnes, et leurs compétences utilisées de manière appropriée.

Priorité stratégique 6 : Coopération entre les services répressifs et les fournisseurs de services Internet

Il est essentiel que les services répressifs coopèrent avec les FSI et autres entreprises du secteur privé afin de préserver les droits des utilisateurs d'Internet et protéger ces derniers des cybercriminels. Les enquêtes sur les infractions liées à la cybercriminalité et autres infractions impliquant la preuve électronique sont souvent impossibles sans la coopération des fournisseurs d'accès. Cependant, cette coopération doit prendre en compte les différences de rôle entre les services répressifs et les fournisseurs d'internet.

La coopération renforcée entre les services répressifs et les fournisseurs de services Internet et le partage d'informations entre les secteurs privé et public dans le respect de la réglementation sur la protection des données doivent devenir une priorité stratégique.

Les gouvernements sont invités à envisager les mesures suivantes :

- **Établir des règles et des procédures claires au niveau national relativement à l'accès des services répressifs aux données détenues par les fournisseurs de services et autres entités du secteur privé** en conformité avec le règlement sur la protection des données. Une base juridique claire, respectueuse du droit procédural et des garanties et conditions de la Convention de Budapest sur la cybercriminalité, contribuera à la préservation des droits de l'homme et de l'Etat de droit. Les lignes directrices adoptées lors de la Conférence Octopus du Conseil de l'Europe en 2008 aideront les forces répressives et les fournisseurs de services à organiser leur coopération et à la structurer. Les gouvernements doivent faciliter l'utilisation des dispositions relatives à la conservation rapide de données (articles 16, 17, 29 et 30) de la Convention de Budapest et s'assurer de l'application intégrale de l'article 18 sur l'injonction de produire.

- **Favoriser une culture de coopération entre les services répressifs et les fournisseurs d'accès Internet et autres entités du secteur privé**. Les protocoles d'accord entre services répressifs et entités du secteur privé constituent un outil fondamental à cet égard. La coordination régionale de ces protocoles renforcerait la capacité des services répressifs, conscientes de l'adoption de normes similaires par les autres États, de mener des enquêtes de part et d'autre des frontières. Les protocoles d'accord, conjugués avec des règles et des procédures clairement établies, faciliteraient également la coopération entre fournisseurs de services Internet multinationaux et autres entités du secteur privé dans la divulgation des données stockées dans un pays étranger ou sur des serveurs en nuage gérés par ces fournisseurs de services.

- **Faciliter le partage transfrontalier d'informations privées et publiques.** Les entités du secteur privé détiennent de grandes quantités de données sur les incidents de sécurité informatique. Le partage transfrontalier de ces informations améliorerait la sécurité des infrastructures et faciliterait les enquêtes sur les cybercriminels. Les gouvernements devraient proposer des lois, conclure des accords de partage d'informations entre les secteurs public et privé et élaborer des lignes directrices sur le partage de données au niveau national et international précisant des garanties de protection du point vue procédural, technique et juridique.

Priorité stratégique 7 : Renforcer la coopération régionale et internationale

La cybercriminalité et la preuve électronique étant internationales par nature, elles requièrent une coopération internationale efficace. Une action immédiate est essentielle pour recueillir des preuves dans un pays étranger et en obtenir la divulgation. Cependant, l'inefficacité de la coopération internationale, notamment de l'entraide judiciaire, reste considérée comme un obstacle majeur à la lutte efficace contre la cybercriminalité.

Rendre la coopération internationale en matière de cybercriminalité et de preuve électronique plus efficace doit être une priorité stratégique.

Les gouvernements sont invités à envisager les mesures suivantes :

- **Exploiter les possibilités de la Convention de Budapest sur la cybercriminalité et autres accords bilatéraux, régionaux et internationaux sur la coopération en matière pénale.** Il convient notamment d'appliquer pleinement les articles 23 à 35 de la Convention relatifs à la coopération policière et judiciaire, aux ajustements législatifs et à l'amélioration des procédures. Les gouvernements (États parties à la Convention et observateurs) devraient promouvoir la mise en œuvre des articles 29 et 30 relatifs aux demandes de conservation de données entre États.

- **Établir des points de contact joignables vingt-quatre heures sur vingt-quatre, sept jours sur sept (contacts 24/7), conformément à l'article 35 de la Convention, et renforcer leur efficacité** au moyen d'un niveau adéquat de ressources, de formations, de compétence judiciaire et de soutien à la coopération proactive tant entre institutions nationales qu'avec leurs homologues à l'étranger.

- **Affecter davantage de personnel, en particulier plus de personnel versé dans le domaine des technologies, et d'autres ressources** à l'entraide judiciaire non seulement au niveau central mais aussi au niveau des institutions chargées d'exécuter les demandes, notamment les services de poursuite.

- **Établir des procédures d'urgence** relatives à l'accès et à la divulgation des données dans des situations de risque pour la vie et autres situations extrêmes.

- **Utiliser la transmission électronique des demandes** de manière conforme à l'article 25.3 de la Convention relatif aux moyens rapides de communication.

- **Évaluer l'efficacité de la coopération internationale**. Les ministres de la Justice et de l'Intérieur et les services de poursuite devraient recueillir des statistiques sur les demandes de coopération internationale en matière de cybercriminalité et de preuve électronique, notamment sur le type des demandes d'entraide, les délais de réponse et les procédures employées. Ils contribueraient ainsi à l'identification des bonnes pratiques et à l'élimination des obstacles à la coopération. Avec leurs partenaires régionaux, ils sont invités à entreprendre l'analyse des problèmes affectant la coopération internationale.