Annexe II – Termes de référence– tel qu'amendés le 12 décembre 2023

Réseau international de formateurs judiciaires sur la cybercriminalité et les preuves électroniques

I. Contexte et justification

Comme les sociétés du monde entier dépendent des technologies de l'information et de la communication, tout type de crime - et pas seulement la cybercriminalité - peuvent inclure des preuves sur un système informatique, c'est-à-dire des preuves électroniques. Cela signifie que tout juge ou **procureur** peuvent être assignés à des affaires impliquant de telles preuves. Des efforts importants sont donc nécessaires pour que les juges et les procureurs disposent des compétences nécessaires, notamment par la formation et « networking »/la mise en réseau.

Un concept[1] visant à soutenir ces efforts a été développé par le Conseil de l'Europe en coopération avec le Réseau de Lisbonne d'institutions de formation judiciaire. Le but de ce concept est d'aider les institutions de formation judiciaire à développer des programmes de formation sur la cybercriminalité et les preuves électroniques pour les juges et les procureurs et d'intégrer cette formation dans la formation initiale et continue régulière. En outre, un ensemble de principes de formation judiciaire sur la cybercriminalité et les preuves électroniques a été adopté et constitue un set de recommandations à considérer pour définir une stratégie nationale de formation judiciaire sur la cybercriminalité et les preuves électroniques.

Des projets communs de l'Union Européenne et du Conseil de l'Europe sur la cybercriminalité soutiennent la formation par des matériels de formation sur la cybercriminalité, les preuves électroniques, la coopération internationale et les procédés criminels en ligne[2]. Dans les pays prioritaires, un groupe de formateurs nationaux a été formé pour organiser des cours de formation au sein des institutions de formation judiciaire.

En 2019, le Conseil de l'Europe a poussé l'initiative plus loin en discutant de la faisabilité et de la viabilité d'un réseau international de formateurs judiciaires nationaux sur la cybercriminalité et la preuve électronique. L'objectif est de permettre aux formateurs formés dans le cadre de ces projets de se connecter, de partager leur expérience et de se tenir à jour.

En 2020, une deuxième réunion visant à définir la mission et les fonctions de la future communauté des formateurs judiciaires a eu lieu. À cette occasion, la nécessité d'une approche coordonnée de la formation judiciaire en matière de cybercriminalité et de preuve électronique a été renforcée et les participants ont à nouveau exprimé leur soutien à la mise en place d'un mécanisme de soutien au futur Réseau international de formation judiciaire et leur volonté de se joindre à l'initiative.

II. Mission et domaine d'application

Le réseau devrait viser à être une entité de coordination des initiatives de formation judiciaire sur la cybercriminalité et les preuves électroniques dans les régions d'intérêt prioritaire. Sa mission pourrait donc être définie comme suit :

Faciliter une approche commune et coordonnée de la formation judiciaire en matière de cybercriminalité et de preuves électroniques et renforcer la constitution de networking professionnel des formateurs.

---

[1] Conseil de l'Europe Formation à la cybercriminalité pour les juges et les procureurs : un concept (autres langues), octobre 2009 : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c3

[2] Les modules de formation sont disponibles sur la page web Octopus du CdE : https://www.coe.int/en/web/octopus/training-materials

Il faut donc poursuivre dans cette voie par:

- Établir et maintenir une réserve de formateurs qualifiés (et certifiés) en matière de cybercriminalité et de preuves électroniques, disponibles pour la présentation des cours de formation judiciaire aux niveaux national, régional et international ;
- Offrir des orientations sur les stratégies nationales de formation judiciaire dans les pays représentés dans sa région, en intégrant la Convention de Budapest sur la cybercriminalité et les normes connexes dans les programmes nationaux des établissements de formation des juges et des procureurs;
- Soutenir et intégrer les cours de formation judiciaire du Conseil de l'Europe sur la cybercriminalité et les preuves électroniques, en donnant des conseils sur les besoins de formation, les méthodes de présentation et les sujets pertinents dans ce domaine, et en fournissant ainsi un retour d'information et des mises à jour de la stratégie de formation judiciaire du Conseil de l'Europe ;
- Faciliter les possibilités de networking et le partage d'informations entre les membres, à travers des réunions internationales, des ateliers de praticiens à praticiens, des groupes de discussion, des réunions virtuelles et des outils communautaires en ligne.

III. Modèle de gouvernance

Le modèle de gouvernance du réseau est organisé autour de trois entités permanentes :

IV. Plénière du réseau

La Plénière est composée de tous les membres du Réseau et il est prévu qu'elle se réunisse une fois par an, afin de :

- approuver la stratégie annuelle et les plans de priorités
- mettre en place des groupes de travail pour les rationalisations prioritaires
- adopter un plan de travail annuel et des rapports annuels
- assurer un effort coordonné en matière de formation judiciaire sur la cybercriminalité et les preuves électroniques en s'engageant dans une coopération et une collaboration avec d'autres initiatives/réseaux de formation judiciaire

V. Comité de pilotage

Le comité de pilotage est un sous-ensemble de la plénière où sont prises les décisions concernant la définition du plan de travail, les stratégies de développement et les règles d'engagement/désengagement.

Le **comité de pilotage** devrait:

- Offrir des orientations à la plénière et superviser les travaux des groupes de travail
- Proposer des méthodes de travail
- Assurer la mise en œuvre de la stratégie globale adoptée par la plénière, en préparant le plan de travail annuel et les rapports d'activité annuels qui doivent être approuvés par la plénière
- Préparer le rapport du progrès trimestriel à partager avec la plénière.

Il est prévu d'inclure :

- Deux représentants par pays participant
- Deux représentants des experts judiciaires du Conseil de l'Europe
- Représentants du Conseil de l'Europe

VI. <u>Secrétariat</u>

Le secrétariat du réseau sera assuré par le Conseil de l'Europe, a travers de ses projets de renforcement des capacités en matière de cybercriminalité, et il devrait de:

- Maintenir et mettre à jour la liste des membres
- Assurer la coordination entre le Comité de pilotage et la plénière du réseau
- Offrir tout autre soutien administratif jugé nécessaire

L'implication et le soutien du Conseil de l'Europe seront réévalués après une phase de lancement de trois ans.

Outre ses organes permanents, il est prévu que le réseau fonctionne également aider par des groupes de travail ad hoc créés pour assurer les progrès sur divers sujets considérés comme des volets hautement prioritaires. Le mandat et la portée des groupes de travail sont décidés par la plénière et leur activité et leurs méthodes de travail sont supervisées par le Comité de pilotage.

VII. Adhésion

Le réseau est constitué par les parties concernées suivantes :

- Juges, magistrats, procureurs (et représentants de la communauté des forces de l'ordre) qui ont été formés comme formateurs judiciaires dans le cadre des programmes de renforcement des capacités du Conseil de l'Europe en matière de cybercriminalité et de preuves électroniques ;
- Juges, magistrats et procureurs qui sont approuvés par les institutions nationales de formation selon des procédures cohérentes qui certifient les aptitudes et les compétences en matière de formation sur la cybercriminalité et les preuves électroniques ;
- Représentants des écoles de formation des juges et des procureurs ;
- Les experts en formation judiciaire qui ont été approuvés par le Conseil de l'Europe selon des procédures cohérentes qui certifient les aptitudes et les compétences en matière de formation sur la cybercriminalité et les preuves électroniques.

Tous les pays qui sont soutenus par les activités de renforcement des capacités développées par le Bureau du programme sur la cybercriminalité du Conseil de l'Europe sont invités à participer au réseau. Les pays intéressés et les organisations ou institutions internationales concernées peuvent devenir membres observateurs jusqu'à ce que la décision d'adhérer au réseau soit officiellement prise, après approbation de la plénière.

L'adhésion est reconfirmée chaque année sur la base de critères qui seront établis par le Comité de pilotage et qui tiendront compte de la participation active aux activités du réseau, ainsi que de l'organisation effective de cours sur la cybercriminalité et la preuve électronique au cours de l'année.

Un minimum d'un et un maximum de deux points focaux par pays sont mis en place, un responsable de la formation des services judiciaires et un responsable de la formation des procureurs/des services du ministère public. Les points focaux nationaux seront reconfirmés chaque année, en janvier, par le Secrétariat.

Veuillez également consulter l'annexe 2 Déclaration de confidentialité.

VIII. Communication et sensibilisation

Le réseau disposera d'un espace en ligne dédié, où des informations seront partagées sur les derniers événements et les activités à suivre. L'administration du site web sera assurée par le secrétariat.

La communication avec les membres du réseau sera assurée par la création et l'utilisation d'une liste de distribution, mise à jour par les services du secrétariat.

Il est prévu que les ateliers de praticiens à praticiens bénéficient d'un site web dédié, mis en place et mis à jour par les services du Secrétariat.

IX. Coordination et coopération avec d'autres réseaux internationaux de formation

La coordination sera assurée avec d'autres réseaux internationaux de formation sur la cybercriminalité et les preuves électroniques, tels que le réseau de Lisbonne, CyberNet, le Réseau européen de formation judiciaire (REFJ), le Réseau européen de cybercriminalité judiciaire (RECJ), le Groupe européen de formation et d'éducation en matière de cybercriminalité (ECTEG), INTERPOL et toute autre initiative pertinente dans ce domaine.

Annexe 1

2021 Plan de travail du Réseau international des formateurs judiciaires en matière de cybercriminalité et de preuve électronique		
Activité	Responsable	Date
Identifier les sujets et les membres pour organiser des ateliers de praticiens à praticiens	Secrétariat	Avant le 15 janvier 2021
Établir et tenir à jour la liste des membres du réseau	Secrétariat	En permanence
Mise en place du Comité de pilotage	Secrétariat et pays participants	Avant le 28 février 2021
Premier appel/réunion de coordination du Comité de pilotage	Secrétariat et Comité de pilotage	Avant le fin du mars 2021
Ateliers de praticiens à praticiens	Membres du réseau avec le soutien du secrétariat	De janvier à décembre 2021
Rapport sur l'état d'avancement de la formation judiciaire en matière de cybercriminalité et de preuve électronique	Comité de pilotage	Avant le 30 juin 2021
Deuxième appel/réunion de coordination du Comité de pilotage	Secrétariat et Comité de pilotage	Avant le 15 juillet 2021
Identifier les angles de coopération avec les écoles et instituts nationaux de formation judiciaire	Secrétariat et écoles et instituts nationaux de formation judiciaire	Avant le 28 février 2021
Troisième réunion annuelle du Réseau international de formateurs judiciaires	Plénière	Avant le 30 octobre 2021

Annexe 2

Déclaration de confidentialité

1. Qui est responsable du traitement des données ?

Le Conseil de l'Europe est le "responsable du traitement" en ce qui concerne le traitement des données à caractère personnel en relation avec votre inscription et votre adhésion au Réseau international des formateurs judiciaires nationaux, ce qui signifie qu'il a le pouvoir de décision concernant le traitement des données. Le Réseau international des formateurs judiciaires nationaux ("**Réseau**") est une communauté de formateurs nationaux, ayant pour mission de faciliter une approche commune et coordonnée de la formation judiciaire en matière de cybercriminalité et de preuve électronique et de renforcer le réseau professionnel des formateurs.

2. Quelles données traitons-nous et dans quel but ?

Nous traitons les données personnelles que vous nous communiquez aux objectifs suivantes :

a) Processus d'inscription et administration des adhésions

Pour procéder à l'inscription au Réseau, nous avons besoin de votre prénom, nom, adresse électronique, le nom de votre organisation et de votre fonction et le pays d'origine.

Lorsque vous vous connectez au site web du Conseil de l'Europe (pour accéder aux documents que nous mettrons à disposition en relation avec le Réseau), certaines informations, telles que votre adresse numérique Internet (IP), les logiciels que vous utilisez, ainsi que certaines autres données sont stockées sur les serveurs du Conseil de l'Europe. Ces éléments n'identifient pas spécifiquement l'utilisateur. Vous pouvez trouver plus d'informations sur la collecte et l'utilisation de ces données dans la clause de non-responsabilité du Conseil de l'Europe en matière de protection des données.

c) Échange de coordonnées entre les participants et facilitation de l'accès aux activités du réseau, interaction avec les membres pairs

Nous établirons une liste de membres et nous pourrons la fournir aux membres pairs et aux points focaux des pays participants en vue de promouvoir le réseautage professionnel. La liste contiendra les mêmes données que celles qui sont requises pour votre inscription au forum, c'est-à-dire votre prénom, votre nom, votre adresse électronique, le nom de votre organisation, votre fonction et votre pays d'origine.

Vous pouvez vous opposer à l'inclusion de vos données dans la liste des participants ou préciser que certaines données ne doivent pas être incluses. Si tel est le cas, veuillez nous contacter lors de l'enregistrement de votre adhésion.

d) Utilisation de votre adresse électronique pour la transmission d'informations

Nous utiliserons votre adresse électronique pour vous fournir les informations pertinentes concernant les mises à jour des activités/événements du réseau.

e) Utilisation de votre image et de votre voix

Nous utiliserons votre image et votre voix afin de promouvoir les activités du réseau, dans les cas où les activités seront enregistrées, dans le but de les partager à l'avenir avec les membres du réseau.

Vous pouvez vous opposer à l'utilisation de ces données ou préciser que certaines données ne doivent pas être utilisées. Si tel est le cas, veuillez nous contacter lors de l'enregistrement de votre adhésion.

3. Quelle est la base juridique du traitement de vos données ?

Nous traitons vos données personnelles sur la base des instruments juridiques du Conseil de l'Europe et de ses règles internes afin de mener à bien les activités nécessaires à l'accomplissement des missions du Conseil de l'Europe.

4. Qui a accès à vos données ?

Seules les personnes qui, au sein du Conseil de l'Europe, soutiennent les activités du Réseau ont accès aux données personnelles que vous fournissez pour votre adhésion au Réseau.

5. Comment collectons-nous et stockons-nous vos données ?

Nous recueillons vos informations sur la base de vos contributions. Nous enregistrons ensuite vos informations sous forme électronique sur les serveurs du Conseil de l'Europe. Nous avons mis en place des mesures pour protéger la sécurité de vos informations, y compris des mesures de sécurité appropriées pour empêcher que vos informations personnelles ne soient accidentellement perdues, utilisées ou consultées de manière non autorisée, modifiées ou divulguées.

6. Combien de temps vos données seront-elles conservées ?

Nous traitons et conservons vos données personnelles pendant la période nécessaire pour faciliter votre adhésion au réseau, conformément aux objectifs mentionnés au point 2 "2. Quelles données traitons-nous et dans quel but ? ”.

7. Vos données sont-elles transférées vers un pays tiers ?

Vos données sont enregistrées au sein de l'Union Européenne et ne sont transférées à aucun pays en dehors de l'Union Européenne.

8. Quels sont vos droits en matière de protection des données ?

Vous en avez le droit :

- demander l'accès aux informations personnelles que nous détenons sur vous ;

- nous demander de corriger les informations personnelles incomplètes ou inexactes que nous détenons à votre sujet ;

- nous demander de supprimer ou de retirer vos informations personnelles lorsqu'il n'y a pas de raison valable de les conserver ;

- s'opposer au traitement de vos informations personnelles pour des raisons spécifiques liées à votre situation.

Si vous souhaitez exercer les droits ci-dessus, ou pour toute question, préoccupation ou demande que vous pourriez avoir en rapport avec la manière dont vos données sont collectées et utilisées, veuillez contacter le Conseil de l'Europe en envoyant un courriel au Délégué à la protection des données du Conseil de l'Europe à l'adresse dpo@coe.int.