Le
Projet sur la cybercriminalité
www.coe.int/cybercrime

et le
Réseau de Lisbonne
www.coe.int/lisbon-network

Service de la Société de l'information et de la lutte contre la criminalité
Direction générale des droits de l'homme et des affaires juridiques
Strasbourg, France

8 octobre 2009

Formation des juges et des procureurs en matière de cybercriminalité : un concept

Projet financé par des contributions de la Roumanie, de Microsoft et McAfee et du Conseil de l'Europe

Ce document a été élaboré par un groupe de travail multilatéral dans le cadre du Projet sur la cybercriminalité et du Réseau des institutions de formation judiciaire – dit « Réseau de Lisbonne » – du Conseil de l'Europe.

Service à contacter :

Pour plus d'informations, veuillez contacter :

Service de la Société de l'information et de la lutte contre la criminalité
Direction générale des droits de l'homme et des affaires juridiques
Conseil de l'Europe
Strasbourg, France

Tél. : +33-3-9021-4506
Fax : +33-3-9021-5650
E-mail : alexander.seger@coe.int

Clause de non-responsabilité :

Table des matières

1 Résumé

Compte tenu de la dépendance des sociétés du monde entier à l'égard des technologies de l'information et de la communication, les juges et les procureurs doivent être préparés à faire face à la question de la cybercriminalité et de la preuve électronique. Cependant, alors que dans de nombreux pays, les forces de l'ordre sont parvenues à renforcer leurs capacités à enquêter sur la cybercriminalité et à recueillir des preuves électroniques, il ne semble pas en être de même des juges et des procureurs. En effet, l'expérience a montré que dans la plupart des cas, ces derniers avaient des difficultés à s'adapter aux nouvelles réalités du monde virtuel. Des efforts particuliers doivent donc être déployés pour donner aux juges et aux procureurs la capacité de poursuivre les auteurs d'actes de cybercriminalité, de statuer sur de tels actes et d'utiliser les preuves électroniques, en développant la formation, le travail en réseau et la spécialisation.

Le présent concept vise à accompagner ces efforts. Il a été élaboré au cours de l'année 2009 par le Projet sur la cybercriminalité et le Réseau de Lisbonne du Conseil de l'Europe, en coopération avec un groupe de travail multilatéral.

Il s'agit, dans le cadre de ce concept, d'aider les institutions de formation judiciaire à élaborer des programmes de formation sur la cybercriminalité et la preuve électronique destinés aux juges et aux procureurs et à les intégrer aux formations initiales et en cours d'emploi ordinaires (c'est-à-dire à les institutionnaliser). Il s'agit également de faciliter le travail en réseau des juges et des procureurs, afin de favoriser le développement de leurs connaissances en la matière, et d'apporter un soutien systématique – et non plus ponctuel – aux initiatives de formation proposées par les partenaires intéressés.
Le concept recouvre les éléments suivants :

Objectifs

En règle générale, les formations initiales et en cours d'emploi actuelles n'apportent pas aux juges et aux procureurs les connaissances nécessaires pour aborder la question de la cybercriminalité et de la preuve électronique.

C'est pourquoi, le concept de formation des juges et des procureurs a pour objectif :

- de faire en sorte que les institutions de formation judiciaire soient en mesure de dispenser une formation – initiale et en cours d'emploi – en matière de cybercriminalité fondée sur les normes internationales
- de faire en sorte que le plus grand nombre possible d'auditeurs de justice ainsi que de juges et de procureurs en exercice acquièrent des connaissances élémentaires en matière de cybercriminalité et de preuve électronique
- de faire en sorte que des formations de niveau avancé soient proposées à un nombre conséquent de juges et de procureurs
- d'encourager la spécialisation et la formation technique permanente des juges et des procureurs
- de contribuer à l'enrichissement des connaissances des juges et des procureurs par le travail en réseau
- de faciliter l'accès à différents réseaux et initiatives de formation.

Les mesures suivantes devraient permettre d'atteindre ces objectifs :

1. L'institutionnalisation de la formation initiale

- Dans les pays où la formation initiale consiste en une formation pratique sur le lieu de travail, il est recommandé qu'une partie au moins de cette formation soit consacrée à la cybercriminalité et à la preuve électronique.
- Dans les pays où la formation initiale est assurée par des institutions de formation judiciaire, les programmes devraient comporter au moins un module de niveau élémentaire portant sur la cybercriminalité et la preuve électronique. Ces questions devraient en outre être abordées dans le cadre des modules obligatoires de droit matériel et de droit procédural. Des modules facultatifs de niveau avancé axés sur la cybercriminalité et la preuve électronique devraient en outre être proposés.
- Les modules de formation spécifiques devraient être standardisés de manière à être reproductibles et à assurer une progression des candidats entre le niveau élémentaire et le niveau avancé.

2. L'institutionnalisation de la formation en cours d'emploi

- Les institutions de formation en cours d'emploi devraient proposer au moins un module de niveau élémentaire sur la cybercriminalité et la preuve électronique afin que les juges et les procureurs en exercice puissent accéder aux connaissances de base qu'ils n'ont pas pu acquérir lors de leur formation initiale.
- Elles devraient également proposer des formations de niveau avancé.

3. Des formations/modules standardisés et reproductibles

- Des formations ou des modules standards pouvant être reproduits à grande échelle, à un coût avantageux et permettant d'assurer aux auditeurs de justice ainsi qu'aux juges et aux procureurs en exercice une progression entre le niveau de base et le niveau avancé devraient être élaborés.
- Les formations de niveau élémentaire existantes pouvant être intégrées aux programmes de formation initiale ou en cours d'emploi devraient être évaluées. Une formation standard pourrait par la suite être recommandée aux institutions de formation initiale et en cours d'emploi.
- Une évaluation similaire pourrait être effectuée pour les formations de niveau avancé et une formation de niveau avancé standard pourrait ensuite être recommandée.
- Des formateurs locaux devraient être formés afin d'être en mesure de dispenser ces formations en langue locale et de limiter ainsi le recours à des formateurs internationaux.

4. L'accès aux matériels de formation ou d'autoformation

- Des matériels de formation mettant en évidence les normes internationales communes et les bonnes pratiques en ce domaine devraient être élaborés et mis à la disposition des institutions de formation à un coût avantageux, afin de pouvoir être utilisés localement.
- S'il est vrai que les juges et les procureurs doivent avant tout être formés à l'application de leur législation nationale, il est toutefois possible de mettre au point des matériels de formation standardisés laissant suffisamment de place pour l'étude des législations et des systèmes nationaux.
- Des formations en ligne devraient être élaborées et mises à disposition.

5. Les centres pilotes de formation élémentaire et avancée

- Plusieurs centres pilotes spécialisés dans la formation élémentaire et avancée des juges et des procureurs dans le domaine de la cybercriminalité et de la preuve électronique devraient être mis en place afin de tester et d'améliorer les formations et les matériels standardisés, de

diffuser de bonnes pratiques, de mener des recherches sur la formation, de tenir un registre des formateurs, de former des formateurs et de proposer des formations à d'autres pays utilisant des systèmes et des langues similaires.
- Il serait souhaitable que les centres pilotes coordonnent leurs travaux, avec l'aide du Conseil de l'Europe.
- Les juges et les procureurs qui souhaitent devenir spécialistes en la matière devraient envisager de participer aux formations proposées par les centres d'excellence et destinées aux forces de l'ordre et au secteur privé.

6. L'enrichissement des connaissances par le travail en réseau

- Outre la formation, la coopération entre pairs et le travail en réseau entre juges et procureurs, mais aussi avec différentes parties prenantes, seront extrêmement importants.
- Les juges et les procureurs devraient utiliser les réseaux de juges et de procureurs existants (tels que le GPEN).
- La possibilité de créer un réseau international de juges spécialisés dans la cybercriminalité ou la criminalité électronique (semblable au GPEN pour les procureurs) devrait être examinée par le Conseil de l'Europe.
- Le Conseil de l'Europe et le Réseau européen de formation judiciaire devraient soutenir le travail en réseau entre les institutions européennes proposant des formations en matière de cybercriminalité et de preuve électronique.
- Afin de faciliter l'accès des juges et des procureurs à ces réseaux de juges et procureurs ainsi qu'aux différents réseaux touchant à la cybercriminalité, le Conseil de l'Europe devrait recenser ces derniers ainsi que les initiatives s'y rapportant et créer un portail présentant des liens, de brèves informations et les coordonnées des personnes à contacter pour chaque réseau. Un tel portail pourrait également faciliter la coordination entre les réseaux ainsi que l'accès aux initiatives et aux matériels de formation existants.

7. La coopération public-privé

- Le soutien du secteur privé à la formation des juges et des procureurs serait bénéfique, dans la mesure où le secteur privé possède une expertise intéressante en la matière. Dans le même temps, les juges et les procureurs doivent rester indépendants et impartiaux.
- Les institutions de formation judiciaire pourraient utiliser l'expertise du secteur privé dans le cadre de la conception des programmes de formation, de l'élaboration des matériels de formation et de la dispense des formations elles-mêmes.
- Cependant, le soutien du secteur privé aux institutions de formation ne doit pas être envisagé comme un moyen potentiel de s'assurer la faveur des tribunaux ou de faire des affaires : il s'agit de permettre aux juges et aux procureurs d'accéder aux informations appropriées et de prendre des décisions en connaissance de cause.
- Le secteur privé pourrait soutenir en toute transparence des organisations internationales ou nationales, des universités, des initiatives de formation et d'autres tierces parties qui pourront à leur tour offrir un appui à des structures de formation indépendantes.
- Si les juges et les procureurs doivent acquérir une vue d'ensemble de l'Internet et de la cybercriminalité, il est également important de leur fournir des informations relatives à certaines plates-formes informatiques spécifiques. Le secteur privé pourrait fournir des matériels pour certains modules (plutôt que pour l'ensemble d'une formation) expliquant le fonctionnement des plates-formes majeures.

Le Réseau de Lisbonne du Conseil de l'Europe a approuvé ce concept en septembre 2009 et a recommandé qu'il soit largement diffusé et mis en œuvre par les institutions de formation judiciaire. Il a décidé de le porter à l'attention du Conseil consultatif des juges européens, du Conseil consultatif des procureurs européens et de la Commission européenne pour l'efficacité de la justice (CEPEJ) afin de lui assurer un soutien le plus large possible.

2 Introduction

Ces dernières années, les sociétés du monde entier ont connu des avancées spectaculaires qui les ont transformées en sociétés de l'information. Les technologies de l'information et de la communication (TIC) sont aujourd'hui présentes dans quasiment tous les aspects de la vie des individus. Cependant, le recours croissant aux TIC et, de fait, la dépendance à l'égard de celles-ci, rend les sociétés vulnérables à des menaces telles que la cybercriminalité, c'est-à-dire aux infractions commises à l'encontre ou par le biais de données ou de systèmes informatiques.

Outre les multiples infractions commises à l'encontre ou par le biais des TIC, de plus en plus d'autres affaires traitées par les tribunaux ont un rapport avec des preuves électroniques stockées dans des systèmes informatiques ou dans d'autres dispositifs.

Par conséquent, les juges et les procureurs doivent être préparés à faire face à la question de la cybercriminalité et de la preuve électronique. Comme indiqué par le Conseil consultatif des juges européens[1], « une formation élaborée, approfondie et diversifiée des juges, sélectionnés à l'issue d'études juridiques complètes, est indispensable pour que ceux-ci exercent leur métier de manière compétente » (paragraphe 3), « elle est aussi une garantie de leur indépendance et de leur impartialité » (paragraphe 4) et elle « devrait aussi prendre en considération le besoin d'une sensibilité sociale et d'une compréhension étendue de différentes disciplines rendant compte de la complexité de la vie en société » (paragraphe 27). Compte tenu de l'importance des TIC dans les sociétés actuelles, les juges et les procureurs doivent au moins avoir une compréhension élémentaire de ces technologies et des problèmes s'y rapportant.

Alors que dans de nombreux Etats, les forces de l'ordre sont parvenues à renforcer leurs capacités à enquêter sur la cybercriminalité et à recueillir des preuves électroniques, il ne semble pas en être de même des juges et des procureurs, qui jouent pourtant un rôle essentiel dans le processus pénal. En effet, l'expérience a montré que bien souvent, ces derniers avaient des difficultés à s'adapter aux nouvelles réalités du monde virtuel.

Des efforts particuliers doivent donc être déployés pour donner aux juges et aux procureurs la capacité de poursuivre les auteurs d'actes de cybercriminalité, de statuer sur de tels actes et d'utiliser les preuves électroniques, en développant la formation, le travail en réseau et la spécialisation.

L'expertise du secteur privé en matière de nouvelles technologies a joué un rôle essentiel dans la formation des forces de l'ordre. Elle pourra aussi être mise à profit pour la formation judiciaire[2], bien que ce potentiel ait été jusqu'ici largement sous-exploité. Dans le même temps, l'indépendance et l'impartialité des juges et des procureurs doivent être préservées. Des approches innovantes sont par conséquent nécessaires pour garantir l'indépendance des juges et des procureurs tout en leur permettant d'accéder à l'expertise du secteur privé et de comprendre le fonctionnement des technologies et de l'industrie des TIC. Le concept ici présenté démontre comment le secteur privé et les universités pourraient apporter un soutien aux institutions de formation judiciaire par le biais de programmes de formation standardisés et par d'autres moyens.

Il s'agit, dans le cadre de ce concept, d'aider les institutions de formation judiciaire à élaborer des programmes de formation sur la cybercriminalité et la preuve électronique destinés aux juges et aux procureurs et à les intégrer aux formations initiales et en cours d'emploi ordinaires (c'est-à-dire à les institutionnaliser).

---

[1] Avis n°4 sur la formation initiale et continue appropriée des juges, aux niveaux national et européen (CCJE (2003) Op. n° 4).

[2] Voir l'étude publiée en mars 2009 : Co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel.

Le concept a été mis au point en tenant compte des informations communiquées par diverses institutions de formation basées en Belgique, en Croatie, en Géorgie, en Allemagne, en France, aux Pays-Bas, en Pologne, au Portugal, en Roumanie, en Espagne, dans « L'ex-République yougoslave de Macédoine » et au Royaume-Uni (réponses à un questionnaire reçues en juin 2009). Il s'appuie aussi sur les informations recueillies lors de deux ateliers, l'un organisé au Portugal en juillet 2009 avec la participation de représentants belges, irlandais, italiens, portugais, néerlandais et britanniques et du secteur privé et l'autre organisé à Strasbourg les 3 et 4 septembre 2009 avec la participation de représentants d'institutions de formation, de juges et de procureurs des pays précités et de représentants du secteur privé, du Réseau européen de formation judiciaire et du Réseau de Lisbonne du Conseil de l'Europe[3].

Ce processus multilatéral a conduit à l'élaboration – inédite – d'un concept de formation des juges et des procureurs en matière de cybercriminalité et de preuve électronique. Le caractère participatif de ce processus facilitera assurément la coopération entre les différentes parties prenantes et la convergence des connaissances et de l'expertise lors de la mise en œuvre du concept.

Le Réseau de Lisbonne du Conseil de l'Europe a approuvé ce concept en septembre 2009 et a recommandé qu'il soit largement diffusé et mis en œuvre par les institutions de formation judiciaire. Il a décidé de le porter à l'attention du Conseil consultatif des juges européens, du Conseil consultatif des procureurs européens et de la Commission européenne pour l'efficacité de la justice (CEPEJ) afin de lui assurer un soutien le plus large possible.

[3] Réseau européen d'échange d'informations entre les personnes et les entités chargées de la formation des juges.

3 Les institutions[4] et les systèmes de formation

En Europe – comme dans d'autres régions – les systèmes de formation des juges et des procureurs sont assez divers[5].

S'agissant de la formation initiale, les systèmes correspondent généralement à l'un ou à une combinaison des modèles suivants[6] :

- Système A : après avoir achevé leurs études supérieures de droit et, bien souvent, réussi un examen d'entrée, les candidats suivent une formation spécifique dans un centre de formation judiciaire en vue de devenir juges et/ou procureurs. Les futurs juges et procureurs peuvent être formés ensemble ou dans des institutions distinctes.
- Système B : après avoir achevé leurs études supérieures de droit, les candidats acquièrent une expérience pratique sur le tas (parfois dans le cadre d'un apprentissage formel) dans des services du ministère public, dans des tribunaux, dans des cabinets d'avocat ou dans d'autres institutions, avant d'être soumis à un examen qui leur permettra d'exercer les fonctions d'avocat, de procureur ou de juge. Ils ne passent par aucune institution de formation centralisée[7].

La formation en cours d'emploi, c'est-à-dire la formation continue des juges et des procureurs en exercice, est assurée soit par des institutions publiques de formation judiciaire, qui se chargent également de la formation initiale (par exemple, en France, en Géorgie, aux Pays-Bas, en Pologne, au Portugal, en Roumanie, en Espagne, dans « L'ex-République yougoslave de Macédoine » et en Croatie), soit par des institutions de formation spécialement créées à cette fin (par exemple, en Allemagne), soit par d'autres institutions publiques, des organisations non gouvernementales, des organisations internationales ou le secteur privé. Dans certains cas, la formation en cours d'emploi est prévue par des plans de formation annuels ou peut être dispensée au cas par cas. Elle est le plus souvent facultative, sauf lorsque les juges ou les procureurs exercent leurs fonctions dans le cadre de juridictions spécialisées (par exemple, en Roumanie).

---

[4] Aux fins du présent document, il faut entendre par « institution de formation » toute entité dispensant des formations.

[5] Comme indiqué par le Conseil consultatif des juges européens du Conseil de l'Europe en 2003 : « Il existe une grande diversité entre les différents pays d'Europe pour ce qui est de la formation initiale et en cours d'emploi des juges. Ces différences peuvent être en partie liées à des caractéristiques particulières de différents systèmes judiciaires, mais à certains égards elles ne semblent pas être inévitables ou nécessaires. Certains pays proposent une formation institutionnalisée de longue durée dispensée dans un établissement spécialisé et suivie d'une formation continue intensive. D'autres prévoient une sorte d'apprentissage sous la tutelle d'un juge expérimenté qui dispense connaissances et conseils professionnels sur des exemples concrets, en montrant la marche à suivre et en évitant toute forme de didactisme. Les pays de *common law* comptent beaucoup sur une longue expérience professionnelle, communément en tant qu'avocats. Entre ces possibilités, il existe toute une variété de pays dans lesquels la formation est plus ou moins organisée et plus ou moins obligatoire ».
AVIS N° 4 DU CONSEIL CONSULTATIF DE JUGES EUROPEENS (CCJE) A L'ATTENTION DU COMITE DES MINISTRES DU CONSEIL DE L'EUROPE SUR LA FORMATION INITIALE ET CONTINUE APPROPRIEE DES JUGES, AUX NIVEAUX NATIONAL ET EUROPEEN (CCJE (2003) Op. n° 4, novembre 2003).

[6] Voir annexe pour plus d'informations.

[7] Les spécificités des systèmes de « common law » méritent d'être mentionnées. Au Royaume-Uni, par exemple, les juges sont nommés parmi des praticiens expérimentés. Cependant, les praticiens qui ne sont pas juges à temps plein peuvent siéger à temps partiel, pendant au moins un mois par an. Après cette période, la majeure partie d'entre eux sont nommés à temps plein. En outre, de nombreux juges non professionnels peuvent siéger dans des tribunaux de première instance (« Tribunals » en matière civile et « Magistrates Courts » principalement en matière pénale). Des programmes de formation distincts sont prévus avant chaque nomination et pendant toute la durée du mandat.

Les programmes de formation initiale et en cours d'emploi nécessitent généralement un processus d'examen et d'adoption officiel, bien qu'il existe une plus grande souplesse à l'égard des formations en cours d'emploi facultatives. Par exemple :

- En France, les programmes sont établis au terme de consultations avec des professionnels du droit et de la justice et les directions concernées du ministère de la Justice. Ils sont ensuite présentés au Conseil d'administration de l'Ecole nationale de la magistrature pour validation.
- En Allemagne, la Conférence des programmes de l'Académie allemande de la magistrature – rassemblant des représentants des différentes administrations judiciaires et des associations professionnelles de juges et de procureurs – est chargée d'élaborer les programmes de formation en cours d'emploi de l'Académie.
- En Pologne, des propositions doivent être déposées au plus tard le 30 avril de chaque année par les services du ministère de la Justice, les présidents des tribunaux et les services du ministère public. Sur la base de ces propositions, le directeur de l'Ecole nationale soumet le programme des activités de formation pour l'année suivante au Conseil des programmes, en vue de leur adoption avant le 30 juillet. Après adoption par le ministre de la Justice, le programme de formation est transmis aux services du ministère de la Justice concernés, aux présidents des cours d'appel et aux procureurs généraux des cours d'appel.
- En Roumanie, la stratégie de formation initiale et en cours d'emploi est approuvée par le Conseil scientifique de l'Institut national de la magistrature et le Conseil supérieur de la magistrature.
- En Espagne, les programmes de formation sont élaborés par une commission pédagogique composée d'experts juridiques, en consultation avec des associations de juges ou des juges individuels. Les programmes de formation initiale et en cours d'emploi pour les juges sont ensuite adoptés par le Conseil général de la magistrature.
- Au Portugal, un programme de formation est élaboré chaque année par le Centre d'études judiciaires. Alors que le programme de formation initiale est arrêté par une loi, le programme de formation en cours d'emploi change chaque année en fonction des besoins identifiés dans la pratique. Les programmes de formation sont établis après consultation du Conseil supérieur de la magistrature, des juridictions fiscales et administratives et du ministère public.
- En Belgique, des programmes de formation généraux ou plus spécifiques sont élaborés chaque année par, ou sous la supervision de l'Institut de formation judiciaire. Cet institut a été récemment institué par une loi (31/01/07) et a démarré ses activités début 2009. La cybercriminalité peut être abordée dans le cadre de la formation en cours d'emploi (souvent facultative).
- Aux Pays-Bas, le Conseil des juges et le Conseil des procureurs généraux (qui, ensemble, donnent des instructions au Centre de formation judiciaire néerlandais – le SSR) définissent les disponibilités budgétaires pour les formations proposées. Les propositions peuvent par exemple émaner de procureurs, de juges ou d'enseignants du SSR et si un budget est disponible et est accordé, la formation sera élaborée par les experts concernés du SSR, des représentants du ministère public, des juges et, le cas échéant, des tierces parties, pouvant être issues du secteur privé.
- En Croatie, les programmes de formation initiale et en cours d'emploi sont établis en coopération avec le Conseil consultatif et le Conseil des programmes de l'Ecole de la magistrature. Le Conseil des programmes définit les priorités de formation et présente des propositions pour le projet de programme annuel de formation professionnelle. Le Conseil consultatif adopte le document et établit des lignes directrices définissant la stratégie de formation professionnelle envisagée. Les deux conseils sont composés d'éminents experts juridiques et de représentants de l'ensemble des groupes visés par l'Ecole de la magistrature.

Les institutions de formation peuvent faire appel à des experts externes, notamment lorsque les sujets abordés sont très spécifiques et techniques, comme dans le cas de la cybercriminalité et de la preuve électronique. Par exemple :

- En Allemagne, l'Académie allemande de la magistrature fait largement appel à des intervenants extérieurs qui sont pour la plupart des juristes ou des chercheurs, mais aussi parfois des experts du secteur privé.
- Aux Pays-Bas, des consultants et des experts du secteur privé participent à l'élaboration des programmes de formation ainsi qu'à la dispense des formations elles-mêmes.
- En Roumanie, l'Institut national de la magistrature fait appel à des formateurs et à des intervenants extérieurs spécialisés dans des domaines tels que la cybercriminalité (par exemple, des experts du Conseil de l'Europe, du ministère de la justice des Etats-Unis, du FBI, des Services secrets américains ou du secteur privé – eBay, Visa, American Express, Amazon, PayPal, Microsoft), notamment dans le cadre de la formation des formateurs.
- En Espagne, le Conseil général de la magistrature a conclu des accords avec des entreprises du secteur privé (CYBEX, Logality) pour assurer des formations en matière de cybercriminalité et de cybercriminalistique. Des experts du secteur privé participent également à la formation judiciaire.
- Au Portugal, la plupart des formateurs du Centre d'études judiciaires sont des juges ou des procureurs. Pour la formation en cours d'emploi (par exemple, séminaires ou formations brèves), des formateurs du secteur privé et d'autres experts peuvent être sollicités.
- En Croatie, des spécialistes des unités de police spécialisées dans la lutte contre la criminalité organisée et économique participent à la conception et à la dispense des formations.
- En Belgique, la majeure partie du budget alloué à la formation des juges et des procureurs est gérée par les universités. Il est cependant possible de faire participer des experts du secteur privé à certains programmes de formation.

Les implications pour la formation des juges et des procureurs en matière de cybercriminalité et de preuve électronique sont les suivantes :

- Les juges et les procureurs – en règle générale – commencent leur formation par des études supérieures de droit. On peut donc supposer que plus les questions relatives à la cybercriminalité et à la preuve électronique seront régies par la législation, plus elles seront abordées dans les manuels et les programmes de droit. Cependant, il pourrait être utile de faire des propositions à cet égard aux responsables de la conception des matériels d'enseignement universitaire.
- Dans les pays où la formation initiale est assurée par des institutions de formation judiciaire, il devrait être possible d'intégrer une formation à la cybercriminalité et à la preuve électronique dans les programmes.
- Lorsque la formation initiale s'effectue sur le lieu de travail, cela risque d'être plus difficile.
- Dans la plupart des pays, la formation en cours d'emploi est assurée par des institutions de formation judiciaire et il devrait donc être possible d'intégrer une formation à la cybercriminalité et à la preuve électronique dans les programmes.
- Si la formation en cours d'emploi peut être dispensée au cas par cas, l'intégration d'une formation en matière de cybercriminalité/preuve électronique dans les programmes officiels ne peut se faire que dans le cadre d'une procédure formelle et nécessite un accord officiel, donc une institutionnalisation de la formation.
- Dans la mesure où la formation en cours d'emploi est généralement facultative, il faudra convaincre les juges et les procureurs de suivre une formation dans un domaine technique tel que la cybercriminalité et la preuve électronique[8].
- L'expertise externe des secteurs public et privé est indispensable et peut être utilisée dans le cadre de l'élaboration des formations, de la formation des formateurs et de la dispense des formations.

[8] Au Portugal, la formation en cours d'emploi est obligatoire (l'ensemble des juges et des procureurs doivent suivre au moins deux stages de formation par an). En Roumanie, elle peut être obligatoire dans certains cas.

4 Les compétences et connaissances nécessaires aux juges et aux procureurs

Il est évident que dorénavant, un nombre croissant d'affaires portées devant les tribunaux, aussi bien pénales que civiles et administratives, seront liées d'une manière ou d'une autre aux technologies de l'information et de la communication et que la plupart des juges et des procureurs pénaux seront un jour confrontés, si ce n'est à la cybercriminalité, du moins à la question de la preuve électronique. Former des juges et des procureurs spécialisés n'est donc pas suffisant.

Une large diffusion des connaissances en matière de cybercriminalité et de preuve électronique s'avère nécessaire : l'ensemble ou le plus grand nombre possible de juges et de procureurs devraient donc suivre au moins une formation élémentaire dans le domaine de la cybercriminalité et de la preuve électronique. Ces connaissances élémentaires devraient être transmises lors de la formation initiale des futurs juges et procureurs et lors de la formation en cours d'emploi des juges et des procureurs en exercice.

Dans le même temps, il s'agit de questions très techniques qui évoluent en permanence, et on ne peut pas demander à l'ensemble des juges et des procureurs de se tenir continuellement au courant des dernières évolutions technologiques. C'est pourquoi il est nécessaire de faire en sorte qu'un nombre suffisant de juges et de procureurs acquièrent des connaissances plus poussées et se spécialisent dans le domaine de la cybercriminalité et de la preuve électronique.

4.1 Connaissances élémentaires

Dans la majorité des systèmes juridiques, il n'est pas possible de prévoir à l'avance quel juge traitera quelle affaire (principe du juge naturel). C'est pourquoi l'ensemble des juges, juges d'instruction et procureurs devraient avoir des connaissances élémentaires en matière de cybercriminalité et de preuve électronique. Ces « connaissances élémentaires » devraient couvrir les domaines suivants :

- les systèmes informatiques et les réseaux : comment ils fonctionnent, notions élémentaires du fonctionnement de l'Internet, rôle des fournisseurs de services, difficultés particulières qui se posent aux juges et aux procureurs
- la cybercriminalité : comment les technologies de l'information et de la communication sont utilisées pour commettre des infractions
- la législation en matière de cybercriminalité : législation interne (y compris la jurisprudence) et normes internationales
- juridictions concernées et compétences territoriales
- la preuve électronique : procédures techniques et aspects juridiques

A l'issue de cette formation élémentaire, les juges et les procureurs devraient être capables :

- de faire le lien entre une conduite délictueuse et les dispositions correspondantes de la législation interne
- d'approuver des techniques d'investigation
- d'ordonner la perquisition et la saisie de systèmes informatiques et la production de preuves électroniques
- d'accélérer la coopération internationale
- d'interroger des témoins et des experts
- de présenter/valider des preuves électroniques.

Voici un exemple de formation élémentaire type pour juges et procureurs :

Exemple : formation en matière de cybercriminalité et de preuve électronique – module type de formation élémentaire.

Objectif de la formation	A l'issue de la formation, les juges et les procureurs doivent avoir une connaissance élémentaire de ce que constituent la cybercriminalité et les preuves électroniques, de la manière de les aborder, du droit matériel et procédural pouvant être appliqué et des technologies pouvant être utilisées, des mesures urgentes et efficaces à prendre et de la coopération internationale à mettre en place.
Session 1	A propos de la cybercriminalité
	➢ Pourquoi se préoccuper de la cybercriminalité ? ➢ Qu'est-ce que la cybercriminalité ? ➢ Les problèmes posés aux juges et aux procureurs ➢ La législation nationale et les normes internationales
Session 2	La technologie
	➢ Le fonctionnement de l'Internet (notions élémentaires) ➢ Glossaire ➢ Protocoles
Session 3	La cybercriminalité en tant qu'infraction pénale dans la législation interne
	➢ Les infractions à l'encontre des données et des systèmes informatiques ➢ La fraude et la falsification informatique ➢ Les infractions se rapportant au contenu (pornographie enfantine, xénophobie, racisme) ➢ Les infractions se rapportant à la propriété intellectuelle ➢ Décisions judiciaires/jurisprudence
Session 4	La preuve électronique
	➢ A propos de la preuve électronique : définitions et caractéristiques ➢ Conditions à respecter en matière de preuve électronique ➢ L'informatique judiciaire
Session 5	Droit procédural/mesures d'investigation
	➢ Juridictions concernées et compétences territoriales ➢ La conservation rapide de données informatiques ➢ Les injonctions/ordres de produire ➢ La perquisition et la saisie de données informatiques ➢ L'interception de données relatives au trafic et au contenu ➢ Les sauvegardes
Session 6	Les relations avec le secteur privé
Session 7	La coopération internationale
	➢ La Convention sur la cybercriminalité en tant que cadre de coopération internationale ➢ Principes généraux ➢ Mesures provisoires et rôle des points de contact 24/7 ➢ Entraide judiciaire et rôle des autorités compétentes
Session 8	Evaluation et conclusion
Logistique et matériels	La formation peut être dispensée en ligne ou dans une salle de formation. Si elle est dispensée en salle : ➢ Une salle de formation équipée d'un ordinateur et d'un projecteur pour les présentations est suffisante (cette formation ne comprenant pas d'exercices pratiques tels que la présentation de logiciels de criminalistique ou de techniques d'investigation, un laboratoire informatique n'est pas nécessaire). ➢ Extraits pertinents du droit matériel et procédural. ➢ Convention de Budapest sur la cybercriminalité et son rapport explicatif

- Un mémento et un glossaire ainsi que d'autres informations générales
- Si la formation est dispensée dans une langue étrangère, un service d'interprétation devrait être prévu et les matériels devraient être traduits.

4.2 Connaissances approfondies

Parfois, des connaissances élémentaires ne sont pas suffisantes pour traiter une affaire de cybercriminalité. Pour faire face à ce genre de situation, il serait nécessaire que de très nombreux juges, juges d'instruction et procureurs acquièrent des connaissances approfondies, qui leur permettront d'instruire, de traiter et de juger des affaires complexes touchant à la cybercriminalité et à la preuve électronique, ou d'assister d'autres procureurs ou juges.

Dans certains pays, des unités ou des services spécialisés ont été créés au sein du ministère public (par exemple, en Roumanie et en Serbie). Dans d'autres pays, les principaux services du ministère public disposent d'un certain nombre de procureurs spécialisés. Aux Pays-Bas, un programme intitulé « intensiveringsprogramma » a été mis en place pour faire notamment en sorte que chacun des onze principaux bureaux du ministère public possède au moins un procureur spécialisé en matière de cybercriminalité. En Italie, dans le cadre de la nouvelle législation sur la cybercriminalité, 29 bureaux du ministère public ont désormais compétence en la matière. Au Portugal, le Service du ministère public du district de Lisbonne possède une section spécialisée dans la criminalité informatique, à laquelle sont renvoyées les enquêtes en matière de cybercriminalité.

Dans certains pays, des procureurs spécialisés peuvent superviser les activités des unités de police spécialisées dans les crimes liées à la haute technologie. Dans la plupart des pays, les services du ministère public sont organisés de manière hiérarchique, de sorte qu'un procureur principal puisse assigner une affaire à un procureur spécialisé. Ainsi, il est possible d'identifier les procureurs qui devraient avoir une connaissance approfondie des questions de cybercriminalité.

S'agissant des juges, dans certains pays, il arrive qu'une affaire de cybercriminalité soit confiée à un juge spécialisé siégeant dans une juridiction traitant de types d'infractions particulières, telles que la criminalité organisée. La Serbie, dont le tribunal de district de Belgrade possède un service spécialisé dans les affaires de cybercriminalité, offre un bon exemple de ce type d'organisation (peut-être le seul en Europe). Cependant, dans la mesure où la plupart des systèmes judiciaires reposent sur le principe du juge naturel, une autre approche est nécessaire. Les Pays-Bas possèdent un système probablement unique en Europe : cinq centres regroupent des juges spécialisés auxquels les autres juges peuvent faire appel en cas de besoin. En Espagne, un projet similaire est actuellement examiné par le Conseil général de la magistrature, prévoyant la mise en place d'un groupe de juges spécialisés dans la cybercriminalité et les preuves électroniques qui assisterait et conseillerait les autres juges. En Belgique, aucune spécialisation n'est exigée par la loi, mais la plupart des juridictions ont la possibilité de demander à l'un ou à plusieurs de leurs membres de se spécialiser. Toutefois, l'assignation de telle ou telle affaire à un juge spécialisé ne relève que de l'organisation interne des tribunaux. Parfois, la loi donne compétence à certaines juridictions (Bruxelles) pour juger certaines affaires. Cependant, dans la majorité des cas, la compétence est déterminée par le lieu de commission de l'infraction et un juge ou un procureur spécialisé n'est pas toujours présent. Dans de nombreux pays, certaines juridictions sont plus souvent saisies d'affaires de cybercriminalité que d'autres, et ont donc besoin de se spécialiser davantage.

Par « connaissances approfondies », il faut entendre que les juges et les procureurs doivent avoir une compréhension concrète et être capables d'appliquer leurs connaissances dans les domaines suivants :

- Systèmes informatiques et réseaux :
  - glossaire de termes relatifs à l'informatique et à la cybercriminalité

- fonctionnement de l'Internet
- protocoles et technologie
- rôle des fournisseurs de services

- Cybercriminalité :
  - évolution de la cybercriminalité
  - typologies : techniques et types particuliers de cybercriminalité (hameçonnage (phishing), réseaux de machines zombies (botnets) et autres logiciels malveillants, pornographie enfantine)
  - exemples concrets et simulations

- Législation en matière de cybercriminalité :
  - législation interne et jurisprudence
  - coopération internationale : accords internationaux et bilatéraux, possibilités de coopération judiciaire et moyens concrets de coopération accélérée

- Enquêtes et preuves électroniques :
  - juridictions concernées et compétences territoriales
  - les dispositions du droit procédural et leur application concrète
  - perquisition, saisie et préservation des preuves électroniques
  - caractéristiques des logiciels de criminalistique
  - identification des suspects
  - suivre l'argent sale
  - sauvegardes et conditions
  - présenter des preuves électroniques devant les tribunaux.

Exemple : formation en matière de cybercriminalité et de preuve électronique – module type de formation avancée[9].

Objectif de la formation	A l'issue de la formation, les juges et les procureurs doivent avoir une connaissance approfondie – et pouvant être appliquée dans la pratique – des domaines suivants : le fonctionnement des systèmes informatiques et des réseaux, qu'est-ce que la cybercriminalité, la législation en matière de cybercriminalité, les juridictions compétentes, les moyens d'investigation, les preuves électroniques et la coopération internationale.
Session 1	Systèmes informatiques et réseaux
	➢ Glossaire de termes relatifs à l'informatique et à la cybercriminalité ➢ Fonctionnement des TIC/de l'infrastructure de l'Internet - Protocoles et technologie - Comment les ordinateurs communiquent entre eux - Recherche d'adresses IP et preuves électroniques – numéros et codes d'identification des ordinateurs - Rôle des fournisseurs de services ➢ Informations sur l'Internet - Recueillir des informations - Utiliser des bases de données Internet (cachées) ➢ Profilage de groupes sociaux - manières de communiquer - manières de préserver leur anonymat ➢ Détection/détermination de la localisation et de l'identité des ordinateurs, des entreprises et des personnes présentes sur l'Internet
Session 2	Cybercriminalité et risques pour la sécurité
	➢ Evolution de la cybercriminalité ➢ Typologies : techniques et types particuliers de cybercriminalité

[9] Fondé sur les réponses au questionnaire et sur l'exemple fourni par les Pays-Bas.

	(hameçonnage (phishing), réseaux de machines zombies (botnets) et autres logiciels malveillants, pornographie enfantine) ➢ Comment les malfaiteurs utilisent les technologies de l'information et de la communication ➢ Les auteurs d'infractions ➢ L'impact de la cybercriminalité ➢ Comment améliorer la sécurité des TIC ➢ Exemples concrets et simulations
Session 3	La législation en matière de cybercriminalité : le droit pénal matériel
	➢ Les infractions à l'encontre des données et des systèmes informatiques ➢ La fraude et la falsification informatique ➢ Les infractions se rapportant au contenu (pornographie enfantine, infractions motivées par la haine) ➢ Les infractions se rapportant à la propriété intellectuelle ➢ Décisions judiciaires/jurisprudence
Session 4	Enquêtes et preuves électroniques
	➢ Les preuves électroniques - Traces/empreintes laissées dans les ordinateurs, sur l'Internet, dans la communication numérique - Perquisition, saisie et préservation des preuves électroniques - Caractéristiques des logiciels de criminalistique - Identifier les suspects - Suivre l'argent sale - Sauvegardes et conditions - Gestion/préparation des affaires - Présenter des preuves électroniques devant les tribunaux ➢ Organisation du système répressif dans le domaine de la cybercriminalité et des preuves électroniques ➢ Etudes de cas
Session 5	La législation en matière de cybercriminalité : le droit procédural
	➢ La conservation rapide de données informatiques ➢ Les injonctions de produire ➢ La perquisition et la saisie de données informatiques ➢ L'interception de données relatives au trafic et au contenu ➢ les sauvegardes ➢ La coopération avec les fournisseurs de services Internet/le secteur privé ➢ Etudes de cas
Session 6	Juridictions concernées et compétences territoriales
	➢ Principes généraux ➢ La compétence en matière de cybercriminalité – défis ➢ Dispositions relatives à la compétence dans la Convention sur la cybercriminalité ➢ Etudes de cas
Session 7	La coopération internationale
	➢ La Convention sur la cybercriminalité en tant que cadre de coopération internationale ➢ Principes généraux ➢ Mesures provisoires, rôle des points de contact 24/7 et coopération policière ➢ Entraide judiciare et rôle des autorités compétentes ➢ Etudes de cas
Session 8	Evaluation et conclusions
Logistique et matériels	La formation peut être dispensée en ligne ou dans une salle de formation. Si elle est dispensée en salle :

- Salle de formation équipée d'un ordinateur et d'un projecteur pour les présentations
- Il serait souhaitable que les participants à la formation aient accès à un ordinateur connecté à l'Internet (mais ce n'est pas une condition indispensable).
- Extraits pertinents du droit matériel et procédural national
- La Convention de Budapest sur la cybercriminalité et son rapport explicatif
- Un mémento et un glossaire ainsi que d'autres informations générales
- Si la formation est dispensée dans une langue étrangère, un service d'interprétation devrait être prévu et les matériels devraient être traduits.

Les juges et les procureurs n'auront généralement pas besoin d'acquérir le type de compétences et de connaissances nécessaires aux enquêteurs en criminalité technologique ou en criminalistique. Il pourrait cependant être utile de rappeler les efforts déployés pour parvenir à l'élaboration d'un programme de formation systématique des représentants des forces de l'ordre.

Sur la base d'un financement de la Commission européenne (Programme Falcone 2002), un projet mené par la police de la République d'Irlande avec la participation d'experts de dix Etats membres de l'Union européenne a conduit à l'élaboration d'un programme de formation élémentaire standardisé en matière de cybercriminalité (Niveau 1) destiné aux représentants des forces de l'ordre. Depuis 2004, un cours de deux semaines est disponible et a été suivi dans de nombreux pays européens et non européens. Le cours a été agréé par University College Dublin (UCD) en 2006.

Dans le cadre d'autres projets menés par la police irlandaise en partenariat avec UCD, des modules supplémentaires de niveau intermédiaire et avancé ont été élaborés, dans l'objectif global de mettre en place un programme de Master agréé en informatique judiciaire et en enquête sur la cybercriminalité destiné à l'ensemble des représentants des forces de l'ordre. Les modules de niveau intermédiaire actuels portent sur les domaines suivants :

- Enquêtes sur l'Internet
- Enquêtes sur les réseaux
- Expertise technico-légale des systèmes de fichiers NT
- Expertise technico-légale des systèmes LINUX
- Expertise technico-légale des téléphones mobiles
- Réseaux locaux sans fil et VOIP
- Le langage script – niveau avancé
- Expertise technico-légale de données réelles
- Expertise technico-légale de Microsoft Vista

Ces modules sont actualisés en permanence et des modules supplémentaires sont en cours d'élaboration[10].

En juillet 2007, Europol a mis en place le Cybercrime Investigation Training Harmonisation Group (Groupe d'harmonisation des formations en matière d'enquête sur la cybercriminalité) afin de coordonner les initiatives de formation touchant à la criminalité technologique au sein de l'Union européenne. L'objectif visé est d'établir un programme de formation agréé pour les enquêteurs des services répressifs européens et de le diffuser au-delà de l'Europe à d'autres services policiers et judiciaires intéressés. Parmi les partenaires du projet figurent la Commission européenne, l'OLAF, Eurojust, le CEPOL, Interpol, le Conseil de l'Europe, les Nations Unies, le Centre d'enquête sur la cybercriminalité de UCD, l'Université de Troyes, Canterbury Christchurch University, l'Université de Bologne et l'industrie des TIC.

[10] On peut également citer les programmes de criminalité technologique mis en place par la UK National Policing Improvement Agency (agence chargée de l'amélioration des services de police du Royaume-Uni).

4.3 Connaissances spécialisées

Certains juges et procureurs peuvent acquérir des connaissances spécialisées en suivant des études de troisième cycle universitaire, par l'autoformation, en faisant appel à leur réseau de relations et par l'expérience professionnelle. Ces connaissances ne seront pas enseignées dans le cadre des programmes de formation ordinaires. Les juges et les procureurs possédant de telles connaissances spécialisées constituent de ce fait une ressource précieuse pour leurs collègues et pour les formateurs.

5 La formation actuelle en matière de cybercriminalité et de preuve électronique

5.1 La formation initiale

Par « formation initiale », il faut entendre la formation que suivent les candidats – après avoir achevé leurs études supérieures de droit – en vue de devenir juges et/ou procureurs. Dans de nombreux systèmes, la formation initiale est assurée par des institutions de formation judiciaire pendant une période d'un à trois ans. Dans d'autres systèmes, la formation initiale consiste en une formation pratique sur le tas plus ou moins formalisée et sans programme spécifique.

Dans la plupart des pays, la cybercriminalité et la preuve électronique ne sont pas ou très peu abordées dans la formation initiale. Par exemple :

- En France, la formation en droit procédural dispensée à l'Ecole nationale de la magistrature (ENM) comprend un cours de trois heures donné par un expert informaticien sur la recherche de preuves électroniques et sur les technologies. La cybercriminalité n'est pas étudiée.
- En Géorgie, la cybercriminalité n'est pas abordée dans le cadre de la formation initiale des procureurs, mais dans celle des juges et du personnel des services judiciaires, sous la forme d'une conférence d'une demi-journée.
- En Allemagne, l'étude de ces questions n'est pas obligatoire dans le cadre de la formation pratique sur le lieu de travail.
- En Croatie, en Pologne et en Roumanie, ces questions ne sont pas prises en compte dans le cadre de la formation initiale.

En revanche, dans certains pays, la cybercriminalité et la preuve électronique font partie intégrante de la formation initiale ordinaire. Par exemple :

- Aux Pays-Bas, la formation initiale comprend une journée d'initiation à la cybercriminalité, assurée par l'institut de formation pour les procureurs et les juges (SSR) à Utrecht ou à Zutphen, lors de laquelle un mémento et d'autres informations générales sont distribués. La formation consiste en des séminaires interactifs et des études de cas. Outre cette formation élémentaire d'une journée, une formation approfondie de quatre jours et une formation supérieure de deux jours sont proposées.

- L'Ecole judiciaire espagnole dispense une formation initiale en matière de cybercriminalité et de preuve électronique aux juges récemment nommés, abordant aussi bien les questions de procédure que les questions de fond. Elle s'inscrit dans le cadre de la formation obligatoire en matière de droit procédural et d'instruction. La cybercriminalité et la preuve électronique sont abordées lors de séminaires organisés sur quatre après-midi et couvrant les thèmes suivants : droit interne, instruments de coopération internationale, présentation de logiciels de criminalistique et de techniques d'investigation, saisie de preuves électroniques et études de cas. De plus, une fois par an, l'école organise un séminaire spécial sur la preuve électronique, ainsi qu'un séminaire sur le droit matériel (infractions commises par des moyens électroniques). Ces séminaires sont présentés par des juristes et des spécialistes des technologies de l'information. Les juges ont en outre accès à une bibliothèque virtuelle sur la criminalité électronique. Cette formation initiale vise à apporter aux intéressés des connaissances de base en matière de cybercriminalité et de preuve électronique.

- Dans « L'ex-République yougoslave de Macédoine », l'Ecole de formation des juges et des procureurs prévoit une formation initiale en matière de cybercriminalité et de preuve électronique dans le cadre de la formation sur le droit pénal, les technologies de l'information et les recherches. Dix heures sont ainsi consacrées à la cybercriminalité et à la preuve électronique.

- Au Portugal, la cybercriminalité n'est pas abordée en tant que sujet spécifique et indépendant. Cependant, dans le cadre de la formation en matière d'enquête pénale, un séminaire est consacré à la cybercriminalité et à la preuve numérique (une heure et demie). Dans le cadre de la formation en matière de droit pénal et de droit pénal procédural, 9 heures sont consacrées à la criminalité informatique et aux procédures d'obtention de preuves numériques et 9 heures sont consacrées aux TIC.

Les formations sont dispensées par des formateurs permanents, des juges, des procureurs ou des juristes ayant de l'expérience en la matière, des fonctionnaires de police spécialisés, des experts en informatique ou des spécialistes du secteur privé.

Les informations disponibles nous amènent aux conclusions suivantes :

- Notre objectif étant de faire en sorte que l'ensemble des juges et des procureurs acquièrent des connaissances élémentaires en matière de cybercriminalité et de preuve électronique, l'offre de formation est beaucoup trop limitée.
- A de rares exceptions près, la formation initiale ne couvre que le niveau de base et aucune formation approfondie n'est prévue.
- En règle générale, aucun matériel de formation standardisé permettant la reproduction des formations n'est disponible.

5.2 La formation en cours d'emploi

La formation en cours d'emploi, c'est-à-dire la formation continue des juges et des procureurs en exercice, est assurée soit par des institutions publiques de formation judiciaire, soit par diverses autres organisations. Par exemple :

- En France, l'Ecole nationale de la magistrature organise un séminaire de niveau avancé de cinq jours et propose des stages de deux jours au sein de l'Office Central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Le coût de ces stages (quelque 5 000 € par stages) est couvert par l'école. Les formateurs sont des juges, des procureurs, des fonctionnaires de police, des experts en informatique ou des experts du secteur privé.

- En Géorgie, la formation en cours d'emploi des juges est exclusivement assurée par l'Ecole supérieure de justice. Elle organise une formation élémentaire de deux jours sur la cybercriminalité, qui est financée par l'Etat. Les formateurs sont des membres de la faculté et des juges de la Cour suprême et des cours d'appel. Les procureurs sont formés par le service de formation du ministère de la Justice, mais aucune formation sur la cybercriminalité et la preuve électronique n'a à ce jour été organisée.

- En Allemagne, la formation en cours d'emploi des juges et des procureurs est assurée par l'Académie allemande de la magistrature, qui organise quelque 150 séminaires par an. En 2009, deux de ces séminaires, chacun d'une durée de quatre jours, ont porté sur la cybercriminalité. Les formateurs sont généralement des procureurs et des juges ayant de l'expérience dans le domaine de la cybercriminalité, mais peuvent également être issus de la police, des douanes, des autorités fiscales ou d'autres secteurs. Le coût des formations est partagé entre les autorités fédérales et étatiques. Il s'agit de formations de niveau élémentaire et avancé.

- Aux Pays-Bas, bien que la formation en cours d'emploi soit facultative, tous les juges sont tenus de consacrer chaque année un nombre d'heures déterminé à la formation. Chaque juge peut décider du domaine qu'il souhaite étudier. L'Institut de formation des juges et des procureurs (SSR) ainsi que plusieurs autres institutions et organismes de formation de

troisième cycle proposent des formations en cours d'emploi sur la cybercriminalité et la preuve électronique de niveau élémentaire et avancé. Le SSR propose chaque année trois formations de niveau élémentaire, trois formations approfondies et une formation de niveau supérieur. Les formateurs sont des magistrats du ministère public spécialisés dans la cybercriminalité et des experts du secteur privé. Toutefois, le SSR propose également un large éventail d'autres formations portant sur des domaines à la fois juridiques et pratiques (environ 400 formations au total). La cybercriminalité est donc en concurrence avec tous les autres thèmes proposés.

- En Pologne, l'Ecole nationale des juges et des procureurs propose des formations de niveau élémentaire et de niveau avancé sous la forme de conférences d'une durée de quatre à cinq jours. En 2009, deux conférences ont été organisées sur « La méthodologie des infractions commises à l'aide de systèmes informatiques » et « Les preuves électroniques dans les procédures judiciaires ».

- En Roumanie, l'Institut national de la magistrature propose des formations en cours d'emploi, mais seulement de niveau élémentaire. Par exemple, entre 2006 et 2009, deux séminaires de deux jours destinés chacun à environ 25 juges ou procureurs ont été organisés chaque année. La plupart de ces séminaires ont été financés par l'Institut national de la magistrature, d'autres ont été subventionnés par le programme PHARE de la Commission européenne et d'autres (en 2006) par eBay. Les formateurs sont des magistrats roumains, des spécialistes des technologies de l'information et des experts étrangers financés par des organisations telles que le Conseil de l'Europe. La cybercriminalité est par ailleurs une matière obligatoire dans les formations décentralisées dispensées au sein des bureaux du ministère public attachés aux cours d'appel. Ces formations sont également coordonnées par l'Institut national de la magistrature.

- En Espagne, l'Ecole judiciaire, placée sous la direction du Conseil général de la magistrature, assure la formation en cours d'emploi des juges en matière de cybercriminalité et de preuve électronique. Pour les procureurs, une telle formation est assurée par le Centre d'études juridiques, sous la direction du ministère de la Justice. Dans les deux cas, la formation est organisée en coopération avec CYBEX, une entreprise privée spécialisée dans ce domaine. L'Ecole judiciaire dispose d'un budget de quelque 42 000 € pour la formation en matière de cybercriminalité. Il est également possible d'obtenir des financements et des aides du secteur privé. La formation en cours d'emploi est de niveau élémentaire, dure entre trois et quatre jours et consiste en des cours magistraux et des analyses de cas pratiques. Les matériels sont publiés et mis normalement à la disposition de chaque juge. En 2008 et en 2009, deux séminaires de ce type ont été organisés chaque année. Bien que certains sujets soient traités relativement en profondeur, il n'existe pas de formation systématique de niveau avancé.

- Au Portugal, la formation en cours d'emploi en matière de cybercriminalité est assurée par le Centre d'études judiciaires, qui organise quelque 30 séminaires par an. Deux séminaires sont régulièrement consacrés à la cybercriminalité (aspects élémentaires). D'autres séminaires touchant à des domaines afférents, tels que les droits d'auteur en ligne ou les technologies et les tribunaux sont parfois organisés. Les formateurs sont des juges, des procureurs, des juristes, des fonctionnaires de police et des experts du secteur public et privé. Les séminaires sont appréciés et attirent un grand nombre de participants (essentiellement des procureurs, mais aussi des juristes et des juges pénaux).

- En Belgique, le programme de formation en cours d'emploi est encore en cours d'élaboration du fait de la création récente de l'Institut de formation judiciaire. L'objectif poursuivi est manifestement d'organiser la formation en tenant compte des conclusions et des recommandations de plusieurs groupes de réflexion et notamment des observations du Conseil de l'Europe. La participation de magistrats belges à des formations à l'étranger peut être financée par l'Institut, sur demande des magistrats (par exemple, un juge et un

procureur ont suivi le séminaire de formation ECCE (Certificat européen sur la cybercriminalité et la preuve électronique) organisé à Paris en février 2009).

- En Croatie, il n'existe actuellement pas de formation en cours d'emploi portant sur la cybercriminalité et/ou la preuve électronique. Ces questions n'ont à ce jour été abordées que dans le cadre du programme CARDS auquel la Croatie a participé.

- Dans « L'ex-République yougoslave de Macédoine », aucune formation en cours d'emploi n'est organisée.

- Les formations proposées par l'Académie de droit européen (ERA). ERA, officiellement créée à l'initiative du Parlement européen en 1992, vise à offrir une connaissance et une analyse approfondies du droit européen et communautaire en organisant des séminaires axés sur la pratique et des formations destinées aux praticiens du droit. L'académie est également un espace d'échanges d'expériences et d'opinions sur les politiques et le droit européens. L'ERA organise régulièrement des manifestations publiques sur le thème de la cybercriminalité, qui attirent des participants venus de toute l'Union européenne. En 2009 et 2010, en coopération avec le programme TAIEX, l'ERA organisera une série de séminaires en Roumanie, en Bulgarie, dans les pays candidats et dans les pays candidats potentiels, lors desquels les principaux instruments européens et internationaux de lutte contre la cybercriminalité seront présentés.
  Tous les séminaires sont envisagés comme des occasions de débattre et de faire le point sur la manière dont la législation européenne en matière de cybercriminalité est appliquée dans les différents Etats membres et dans les pays candidats et de réfléchir à la possibilité d'une campagne européenne contre l'utilisation illégale de l'Internet. Les instruments et les textes juridiques les plus récents, tels que la Convention du Conseil de l'Europe sur la cybercriminalité (2001), la décision-cadre 2005/222/JAI du Conseil relative aux attaques visant les systèmes d'information et la décision cadre 2004/68/JHA du Conseil sur la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, sont également examinés. La question de la coopération en cours avec des fournisseurs de services et des entreprises liées à l'Internet tels que Google, Microsoft et Yahoo fait aussi l'objet de discussions.
  Chaque séminaire utilise un éventail de méthodes de formation : cours introductifs, cours plus approfondis, études de cas, autres types d'apprentissage interactif. Une attention particulière est accordée aux discussions en petits groupes de travail. La présentation des cours magistraux et l'animation des groupes de travail sont assurées par des experts européens et nationaux.

- Dans un certain nombre de pays, des séminaires de formation sont organisés en partenariat avec le secteur privé. Par exemple :

  En Allemagne, eBay a participé à la nouvelle formation « Nouveaux média et droit pénal » organisée par l'Académie allemande de la magistrature à l'intention des juges et des procureurs, en envoyant un intervenant pour présenter le site marchand eBay, les activités délictueuses qu'il suscite, les contre-mesures prises et comment eBay collabore avec les services répressifs. eBay a aussi participé à plusieurs séminaires occasionnels organisés par le ministère de la Justice de Berlin, auxquels cent procureurs environ ont assisté à chaque fois.

  En Roumanie, eBay a animé de nombreuses formations destinées aux juges, aux procureurs et aux représentants des forces de l'ordre. En particulier, eBay a collaboré avec les services secrets des Etats-Unis à l'ambassade américaine en vue de former 25 procureurs issus de différents bureaux de la Direction des enquêtes sur le crime organisé et le terrorisme, ainsi que 15 juges et 20 fonctionnaires de police à Silbiu. Par ailleurs, eBay a participé à la formation complémentaire de juges à Targu Jiu et de 60 juges de différentes juridictions relevant de la cour d'appel de Craiova.

Comme indiqué précédemment, dans presque tous les cas, tout changement ou ajout à un programme institutionnel de formation judiciaire doit être approuvé et validé par des instances officielles[11].

Si, de toute évidence, de nombreuses initiatives sont prises pour répondre à la nécessité de mieux former les juges et les procureurs à la cybercriminalité, il existe un manque de cohérence flagrant entre les approches décrites ci-dessus.

Bien qu'il faille tenir compte des particularités des droits nationaux et de la grande diversité des systèmes éducatifs, la cybercriminalité est, par nature, un problème international et exige un minimum de coordination et de cohérence entre les pays. Ce n'est qu'en acquérant une compréhension identique de ce que constitue la cybercriminalité que l'on parviendra à une meilleure cohérence entre les décisions judiciaires et que l'on empêchera la création de zones où les malfaiteurs sont en sécurité, tout en fournissant aux institutions de formation des contenus de qualité à des coûts réduits.

Les informations disponibles nous amènent aux conclusions suivantes :

- La plupart des formations en cours d'emploi proposées sont de niveau élémentaire.
- Les formations sont très peu nombreuses et n'atteignent qu'une faible minorité de juges et de procureurs.
- Dans la plupart des cas, les formations élémentaires ne semblent pas être standardisées. Elles ne sont donc pas reproductibles et n'assurent pas aux juges et aux procureurs une progression systématique entre le niveau élémentaire et le niveau avancé. Les Pays-Bas semblent être une exception.
- Les matériels de formation semblent dispersés et élaborés au cas par cas.
- Si l'on considère qu'au bout du compte, l'ensemble des juges et des procureurs doivent avoir au moins des connaissances élémentaires en matière de cybercriminalité et de preuve électronique, la formation proposée est largement insuffisante, sachant que selon toute probabilité, la génération actuelle de juges et des procureurs en activité n'ont reçu aucune formation initiale ni abordé ces questions pendant leurs études universitaires.
- A de rares exceptions près, il n'existe pas de formation pour juges et procureurs de niveau avancé.
- Compte tenu du caractère international de la cybercriminalité, un minimum de coordination et de cohérence entre les pays serait nécessaire.

[11] Dans ce contexte, le projet de Certificat européen sur la cybercriminalité et la preuve électronique mis en œuvre par CYBEX et financé par la Commission européenne (JPEN) est intéressant. Il prévoit une formation élémentaire standardisée de quatre jours destinée aux juges, aux procureurs et aux juristes. Entre le début 2009 et la fin 2010, la formation sera testée dans quatorze pays pilotes d'Europe et d'Amérique latine. Les participants recevront un certificat attestant de l'acquisition de connaissances théoriques, pratiques, juridiques et techniques de niveau élémentaire en matière de preuve électronique et de cybercriminalité.
Le Conseil de l'Europe – dans le cadre du Projet sur la cybercriminalité – a également commencé à élaborer un manuel de formation pour les juges et les procureurs, qui sera utilisé dans le cadre d'une formation élémentaire de deux jours axée sur la législation en matière de cybercriminalité.

6 L'approche proposée

6.1 Objectif

Comme indiqué dans la partie précédente, en règle générale, les formations initiales et en cours d'emploi existantes n'apportent pas aux juges et aux procureurs les connaissances nécessaires pour aborder la question de la cybercriminalité et de la preuve électronique.

C'est pourquoi, le concept de formation des juges et des procureurs a pour objectif :

- de faire en sorte que les institutions de formation judiciaire soient en mesure de dispenser une formation – initiale et en cours d'emploi – en matière de cybercriminalité fondée sur les normes internationales ;
- de faire en sorte que le plus grand nombre possible d'auditeurs de justice ainsi que de juges et de procureurs en exercice acquièrent des connaissances élémentaires en matière de cybercriminalité et de preuve électronique ;
- de faire en sorte que des formations de niveau avancé soient proposées à un nombre conséquent de juges et de procureurs ;
- d'encourager la spécialisation et la formation technique permanente des juges et des procureurs ;
- de contribuer à l'enrichissement des connaissances des juges et des procureurs par le travail en réseau ;
- de faciliter l'accès à différents réseaux et initiatives de formation.

Les mesures suivantes devraient contribuer à atteindre ces objectifs :

6.2 L'institutionnalisation de la formation initiale

- Dans les pays où la formation initiale consiste en une formation pratique sur le lieu de travail (un type d'apprentissage ou une série de stages) sans programme officiel, il est recommandé qu'une partie au moins de cette formation (par exemple, un stage ou une activité identique) soit consacrée à la cybercriminalité et à la preuve électronique.

- Dans les pays où la formation initiale est assurée par des institutions de formation judiciaire :
  - les programmes devraient comporter au moins un module de niveau élémentaire concernant la cybercriminalité et la preuve électronique ;
  - ces questions devraient en outre être abordées dans le cadre des modules obligatoires de droit matériel et de droit procédural ;
  - des modules facultatifs de niveau avancé axés sur la cybercriminalité et la preuve électronique devraient être proposés.

Les modules de formation spécifiques devraient être standardisés de manière à être reproductibles et à assurer une progression des candidats entre le niveau élémentaire et le niveau avancé. Par « reproductibles », il faut entendre qu'ils doivent pouvoir être reproduits au moins dans le même pays pour différentes personnes, afin que les participants à différentes formations aient un niveau de connaissances identique. Cela suppose également que les méthodes de formation soient standardisées. Afin d'assurer des formations de qualité constante, une évaluation devrait être effectuée à l'issue de chaque formation.

6.3 L'institutionnalisation de la formation en cours d'emploi

- Les institutions de formation en cours d'emploi devraient proposer au moins un module de niveau élémentaire sur la cybercriminalité et la preuve électronique, afin que les juges et les procureurs en exercice puissent accéder aux connaissances de base qu'ils n'ont pas pu acquérir lors de leur formation initiale.

- Elles devraient également proposer des formations de niveau avancé.

- Dans ce cas également : les modules de formation spécifiques devraient être standardisés de manière à être reproductibles et à assurer une progression des candidats entre le niveau élémentaire et le niveau avancé. Par conséquent, dans la mesure du possible, une harmonisation des modules de formation en cours d'emploi avec les modules de formation initiale serait nécessaire. Les méthodes de formation devraient également être standardisées, ainsi que les contrôles de qualité effectués à l'issue des formations.

- Afin de former des juges et des procureurs spécialisés, la mise en place de stages au sein des unités spécialisées dans les crimes liés à la haute technologie ou de formations de troisième cycle devrait être encouragée[12].

6.4 Des formations/modules standardisés et reproductibles

- Des formations ou des modules standard pouvant être reproduits à grande échelle à un coût avantageux et permettant d'assurer aux juges et aux procureurs en exercice une progression entre le niveau de base et le niveau avancé devraient être élaborés.

- Les formations élémentaires existantes[13] pouvant être intégrées aux programmes de formation initiale ou en cours d'emploi devraient être évaluées. Une formation standard pourrait par la suite être recommandée aux institutions de formation initiale et en cours d'emploi.

- Une évaluation similaire pourrait être effectuée pour les formations de niveau avancé et une formation de niveau avancé standard pourrait ensuite être recommandée.

- Enfin, des formateurs locaux devraient être formés afin d'être en mesure de dispenser ces formations en langue locale et de limiter ainsi le recours à des formateurs internationaux[14].

6.5 L'accès aux matériels de formation ou d'autoformation

- Des matériels de formation mettant en évidence les normes internationales communes et les bonnes pratiques en ce domaine devraient être élaborés et mis à la disposition des institutions de formation à un coût avantageux, afin de pouvoir être utilisés localement. A l'évidence, si une formation fortement standardisée axée sur les technologies et la criminalistique est possible pour les services de police, cela s'avère plus difficile pour les juges et les procureurs qui doivent avant tout être formés à l'application de la législation interne. Il est néanmoins possible de mettre au point des matériels de formation standardisés laissant suffisamment de place pour l'étude des législations et des systèmes nationaux.

- Dans certains pays, des matériels de formation en ligne sont mis à la disposition des juges et des procureurs[15]. Cette pratique devrait être adoptée par d'autres pays.

---

[11] A titre d'exemple, la formation élémentaire de deux semaines mise au point par la police irlandaise et University College Dublin pourrait également présenter un intérêt pour les juges et les procureurs.

[13] Par exemple, la formation ECCE élaborée et actuellement expérimentée par CYBEX.

[14] Un programme de « formation des formateurs » a été élaboré par UCD et Interpol et pourrait être mis à disposition. Il porte sur les techniques de formation, l'élaboration des formations, etc. Il n'est PAS réservé aux services de police et peut être utilisé par tous.

[15] C'est le cas des Pays-Bas et de la e-bibliothèque CYBEX. Dans le cadre du projet 2CENTRE, UCD prévoit de développer un service de ressources en ligne qui proposera certains matériels de formation relatifs aux programmes AGIS/ISEC.

- Des formations en ligne devraient être élaborées et mises à disposition[16].

- L'accès aux formations (nationales et internationales) devrait être facilité autant que possible par une simplification des procédures d'agrément.

6.6 Les centres pilotes de formation élémentaire et avancée

- Plusieurs centres pilotes spécialisés dans la formation élémentaire et avancée des juges et des procureurs dans le domaine de la cybercriminalité et de la preuve électronique devraient être créés. Ces centres pourraient :
  - tester et améliorer les formations et les matériels standardisés
  - diffuser de bonnes pratiques
  - mener des recherches sur la formation
  - tenir un registre des formateurs
  - former des formateurs
  - proposer des formations à d'autres pays utilisant des systèmes et des langues similaires.

- Il serait souhaitable que les centres pilotes coordonnent leurs travaux, avec l'aide du Conseil de l'Europe.

- Les juges et les procureurs qui souhaitent devenir spécialistes devraient envisager de participer aux formations proposées par les centres d'excellence et destinées aux forces de l'ordre et au secteur privé[17].

6.7 L'enrichissement des connaissances par le travail en réseau

Si la formation initiale et la formation en cours d'emploi permettront aux juges et aux procureurs d'acquérir des connaissances en matière de cybercriminalité, la coopération entre pairs et le travail en réseau entre juges et procureurs, mais aussi avec diverses parties prenantes, seront aussi extrêmement importants.

Par conséquent :

- Les juges et les procureurs devraient utiliser les réseaux de juges[18] et de procureurs existants (tels que le GPEN)[19].

---

[16] Par exemple, UCD propose actuellement deux programmes de Master de sciences, dont une partie des cours est entièrement dispensée en ligne. Le Centre d'études judiciaires du Portugal prévoit de mettre en place une formation en ligne sur « Les tribunaux et les technologies de l'information et de la communication », comprenant des modules sur la cybercriminalité et la preuve électronique. La formation sera en portugais et la possibilité de l'étendre à d'autres pays de langue portugaise (Brésil, Cap-Vert, Angola, Mozambique, Guinée-Bissau, São Tomé ou Timor) est envisagée.

[17] L'initiative 2Centre (Cybercrime Centres of Excellence Network for Training Research and Education – Réseau de centres d'excellence pour la formation et la recherche sur la formation en matière de cybercriminalité) a été lancée en mars 2009 (pendant la Conférence Octopus du Conseil de l'Europe). Le projet 2Centre « examine les méthodes actuelles de formation des forces de l'ordre et du secteur privé dans le domaine de l'informatique judiciaire et des enquêtes sur la cybercriminalité. Il passe en revue les activités menées par les membres des forces de l'ordre et le personnel des entreprises concernées afin d'acquérir des connaissances et des compétences dans un domaine où coexistent actuellement divers niveaux de formation professionnelle, de formation interne, de formation polyvalente et de formation sur le tas ». University College Dublin est le premier centre d'excellence, l'Université de Troyes deviendra le second en 2010.

[18] Aucun réseau international de juges axé sur la cybercriminalité et la preuve électronique ne semble actuellement encore exister. A titre d'exemple d'initiative nationale, on peut citer celle mise en place aux Pays-Bas, où une ressource intranet de type wiki a été créée.

- La possibilité de créer un réseau international de juges spécialisés dans la cybercriminalité ou la criminalité électronique (semblable au GPEN pour les procureurs) devrait être examinée par le Conseil de l'Europe.
- Le Conseil de l'Europe et le Réseau européen de formation judiciaire devraient soutenir le travail en réseau entre les institutions européennes proposant des formations en matière de cybercriminalité et de preuve électronique.
- Afin de faciliter l'accès des juges et des procureurs aux différents réseaux touchant à la cybercriminalité, le Conseil de l'Europe devrait recenser ces derniers ainsi que les initiatives s'y rapportant – sur son site www.coe.int/cybercrime – et créer un portail présentant des liens, de brèves informations et les coordonnées des personnes à contacter pour chaque réseau. Un tel portail pourrait également faciliter la coordination entre les réseaux ainsi que l'accès aux initiatives et aux matériels de formation existants.

6.8 La coopération public-privé

Afin de faciliter les enquêtes sur la cybercriminalité et de recueillir des preuves électroniques, une coopération structurée et réglementée entre les forces de l'ordre et le secteur privé (industrie des TIC, notamment les fournisseurs de services Internet) est absolument indispensable[20]. Il est également essentiel que le secteur privé contribue par son expertise et par d'autres formes de soutien aux initiatives de formation des forces de l'ordre.

Le soutien du secteur privé à la formation des juges et des procureurs serait également bénéfique, dans la mesure où le secteur privé possède une expertise intéressante dans le domaine qui nous intéresse. Dans le même temps, les juges et les procureurs doivent rester indépendants et impartiaux.

Par conséquent :

- Les institutions de formation judiciaire pourraient utiliser l'expertise du secteur privé dans le cadre de la conception des programmes de formation, de l'élaboration des matériels de formation et de la dispense des formations elles-mêmes.

- Cependant, le soutien du secteur privé aux institutions de formation ne doit pas être envisagé comme un moyen potentiel de s'assurer la faveur des tribunaux ou de faire des affaires : il s'agit de permettre aux juges et aux procureurs d'accéder aux informations appropriées et de prendre des décisions en connaissance de cause.

- Le secteur privé pourrait soutenir en toute transparence des organisations internationales ou nationales, des universités, des initiatives de formation et d'autres tierces parties qui pourront à leur tour offrir un appui à des structures de formation indépendantes.

- Si les juges et les procureurs doivent acquérir une vue d'ensemble de l'Internet et de la cybercriminalité, il est également important de leur fournir des informations relatives à

[19] Le GPEN (Global Prosecutor's E-Crime Network – Réseau international de procureurs spécialisés dans le crime électronique) a été créé en 2008 sous l'égide de l'Association internationale des procureurs et des poursuivants (AIPP). Il a pour but de faciliter les échanges d'informations et la coopération entre les procureurs dans les affaires touchant à la criminalité électronique ou à la cybercriminalité en s'appuyant sur la Convention sur la cybercriminalité, d'élaborer et de proposer des programmes de formation et de fournir des ressources en ligne aux procureurs. Le GPEN est un réseau de procureurs spécialisés dans la criminalité électronique et chaque membre organisationnel de l'AIPP a été invité à nommer au moins un procureur en qualité d'agent de liaison national du GPEN. Le réseau est géré par le Conseil de développement du GPEN, qui est composé de membres de l'AIPP.

[20] Voir par exemple les Lignes directrices pour la coopération entre organes de répression et fournisseurs de services Internet, adoptées par la Conférence Octopus du Conseil de l'Europe en avril 2008.

certaines plates-formes informatiques spécifiques. Le secteur privé pourrait fournir des matériels pour certains modules (plutôt que pour l'ensemble d'une formation) expliquant le fonctionnement des plates-formes majeures.

7 Soutenir la mise en œuvre du concept

La mise en œuvre du concept incombe en premier lieu aux institutions de formation judiciaire, mais devrait également être encouragée par les institutions et les partenaires des secteurs public et privé, notamment les organisations internationales. Au vu de l'importance des technologies de l'information et de la communication pour la société, le financement de telles formations représente un investissement rentable et tous les efforts doivent être entrepris afin de doter les institutions de formation de ressources suffisantes.

Le Conseil de l'Europe et le Réseau européen de formation judiciaire (REFJ), ainsi que d'autres organismes, devraient promouvoir la mise en œuvre du concept dans toute l'Europe et au-delà.

Par ailleurs, le REFJ et le Conseil de l'Europe pourraient organiser à brève échéance une conférence commune sur le concept.

Il conviendrait enfin que le Conseil de l'Europe et le REFJ évaluent régulièrement les progrès réalisés.

Sur le plan pratique, la mise en œuvre du concept devrait également être soutenue par des donateurs. Les organisations et les donateurs intéressés pourraient participer au développement de projets visant à soutenir les institutions de formation et les autres parties prenantes disposées à adopter les mesures proposées par le présent concept et à en assumer les responsabilités.

Afin de réduire les risques de conflits d'intérêt ou d'atteinte à l'impartialité des juges et des procureurs, les donateurs pourraient apporter leurs contributions financières par l'intermédiaire d'une tierce partie neutre – et non directement- telle que des organisations internationales qui coopéreraient par la suite avec les institutions de formation.

8 Annexe

8.1 Le Réseau de Lisbonne : liens vers les institutions de formation judiciaire

Quarante-quatre des quarante-sept Etats membres du Conseil de l'Europe sont représentés au sein du Réseau de Lisbonne. Les membres du Réseau de Lisbonne sont les institutions nationales chargées de la formation initiale et continue des juges et des procureurs. Il peut s'agir, selon les cas, d'écoles de la magistrature, de centres de formation judiciaire ou de services de formation des magistrats au sein des ministères de la Justice.

Pour consulter les informations disponibles pour chacun des Etats membres du réseau (y compris, dans certains cas, concernant les programmes de formation associés) voir :

- Albanie
- Allemagne
- Andorre
- Arménie
- Autriche
- Azerbaïdjan
- Belgique
- Bosnie-Herzégovine
- Bulgarie
- Chypre
- Croatie
- Danemark
- Espagne
- Estonie
- Fédération de Russie
- Finlande
- France
- Géorgie
- Grèce
- Hongrie
- Irlande
- Islande
- Italie
- "L'Ex-République yougoslave de Macédoine"
- Lettonie
- Lituanie
- Luxembourg
- Malte
- Moldova
- Monténégro
- Norvège
- Pays-Bas
- Pologne
- Portugal
- Roumanie
- République tchèque
- Royaume-Uni
  - Angleterre et Pays de Galle
  - Ecosse
- Slovaquie
- Slovénie
- Serbie
- Suède
- Suisse
- Turquie
- Ukraine

Observateur

- MINUK

8.2 Exemples de formations de niveau élémentaire : structure et sujets abordés

8.2.1 Exemple de formation dispensée aux Pays-Bas

Formation de niveau élémentaire – 1 jour

Programme :

1 Aspect généraux :
- Qu'est-ce que la cybercriminalité ?
- Manifestations de la cybercriminalité
- Cadre juridique régissant la répression des infractions et les poursuites pénales

2 La répression des infractions :
- L'application du droit numérique en tant que pratique quotidienne
- Méthodes de répression des infractions

3 La répression des infractions (2e partie) :
- L'Internet et la répression des infractions dans le cadre de la loi sur les privilèges spéciaux en matière de répression des infractions.

Conclusions + évaluation

8.2.2 Exemple de formation dispensée en Allemagne (Académie allemande de la magistrature)

Formation de niveau élémentaire « Différentes manifestations et stratégie de lutte contre la cybercriminalité » – 4 jours

Programme :

Jour 1 :
- Le Code pénal allemand
- L'utilisation du Code pénal allemand dans le contexte de la criminalité informatique et de la cybercriminalité
- Problèmes rencontrés dans la pratique quotidienne des services du ministère public et des tribunaux

L'intervenant est un juge du Tribunal de Munich spécialisé dans la criminalité financière et économique et ayant travaillé il y a quelques années en qualité de procureur dans des affaires touchant à la cybercriminalité, à l'espionnage de données, à la falsification de dates etc.

- Problèmes rencontrés dans la pratique quotidienne des services du ministère public et des tribunaux aux Pays-Bas
- Développement de la cybercriminalité et lutte contre ce phénomène en Europe
- Problèmes rencontrés avec les fournisseurs aux Pays-Bas et dans d'autres pays européens
- La Convention sur la cybercriminalité du Conseil de l'Europe
- L'importance et l'intérêt présenté par la Convention sur la cybercriminalité pour l'Europe et le reste du monde (Chine, Etats-Unis, Russie)

L'intervenant est le Professeur Henrik Kaspersen, Pays-Bas.

Jour 2 :
- Le sabotage des systèmes informatiques
- Le piratage sur l'Internet
- Les pièges relatifs aux commandes sur l'Internet
- L'espionnage de données
- La fraude informatique par carte de crédit
- Les attaques contre les données bancaires
- Le hameçonnage et les nouveaux types d'infractions sur l'Internet
- Les réseaux de machines zombies (botnets)
- La fraude sur eBay ou sur d'autres sites marchands

L'intervenant est un fonctionnaire de police du siège de la police allemande (BKA, Wiesbaden).

- Les recherches préventives sur l'Internet pour lutter contre le crime organisé, le terrorisme, les infractions graves, le blanchiment d'argent, etc.
- Les recherches sur l'Internet concernant des personnes atteintes de folie meurtrière (écoles, etc.)
- Les recherches sur l'Internet concernant la pornographie enfantine
- La coopération internationale en matière de recherches sur l'Internet
- La recherche en ligne (problèmes constitutionnels)

L'intervenant est le chef d'un service spécial du siège de la police bavaroise (LKA, Munich).

Jour 3 :

- Sauvegarde et évaluation de données en Allemagne ou dans d'autres pays
- Recherche de données sur l'Internet et traçabilité des données sur le Net.
- Les possibilités offertes par l'informatique judiciaire et les limites de l'analyse de données
- Les systèmes d'anonymisation de données sur le Net
- L'utilisation de cryptogrammes par les malfaiteurs

L'intervenant est un spécialiste du siège de la police de Munich.

- Les nouveaux problèmes juridiques posés par la sauvegarde et l'évaluation des données Internet
- La compétence pour l'ensemble des mesures juridiques de recherche
- La compétence en matière de recueil de preuves pour les enquêtes et les tribunaux
- Evolutions récentes en matière de répression des infractions

L'intervenant est un juge du tribunal pénal supérieur bavarois de Bamberg.

Jour 4 :

- Le réseau d'affaires russe
- Intercage
- La protection contre le sabotage d'ordinateurs ou de données
- Le « piratage » positif
- L'influence et la falsification des machines à voter
- L'influence politique dans les nouvelles lois
- La population dans une maison de verre

L'intervenant est membre du célèbre Chaos computer club (CCC) de Hambourg, dont les membres ont pour but de pénétrer dans les ordinateurs du Gouvernement, de la Maison Blanche, de la CIA. Le club a par exemple montré comment on pouvait manipuler le système de distribution d'eau d'une ville.

8.2.3 Exemples de formations du Conseil de l'Europe

1. Atelier de formation sur la cybercriminalité pour les procureurs, Belo Horizonte, Brésil, 26 août 2008 (organisé par le ministère public de l'Etat du Minas Gerais en coopération avec le Conseil de l'Europe)

Formation de niveau élémentaire – 1 jour
Programme :

1 Séance d'ouverture
- Observations liminaires
- Les réformes législatives actuelles

2 La cybercriminalité : le phénomène
- Tour d'horizon des menaces actuelles

- Menaces spécifiques et affaires examinés au Brésil

3 Le droit matériel : quelles infractions ?
- Les normes internationales
  - Typologie, concepts juridiques
  - La Convention sur la cybercriminalité
- Les dispositions du droit brésilien
  - Dispositions actuelles
  - Réformes juridiques en cours

4 Les enquêtes et la coopération internationale
- Le rôle des procureurs dans les enquêtes sur la cybercriminalité
- Le droit procédural national
- Les mesures procédurales et la coopération internationale prévues par la Convention sur la cybercriminalité

5 Les partenariats public-privé
- Exemples de partenariats public-privé au Brésil
- La répression des infractions – coopération des fournisseurs de services Internet aux enquêtes sur la cybercriminalité : recommandations
- Discussion : la coopération entre les forces de l'ordre et les fournisseurs de services Internet : l'expérience du Brésil

2. La cybercriminalité : formation pour les juges, Le Caire, Egypte, 9 et 10 juin 2008 (organisée par Microsoft avec la participation du Conseil de l'Europe).
Cette formation a été dispensée deux fois à différents groupes de juges siégeant dans des tribunaux de commerce (également chargés des questions de criminalité électronique).

Formation de niveau élémentaire – 1 jour

Programme :

1 Séance d'ouverture

2 La cybercriminalité : le phénomène
- Tour d'horizon des menaces actuelles
- Menaces spécifiques
  - Usage frauduleux d'identités et d'informations en ligne : exemples
  - La fraude à la carte de crédit et autres types de fraude

3 Le droit matériel : quelles infractions ?
- Les normes internationales (expert du Conseil de l'Europe)
  - Typologie, concepts juridiques
  - La Convention sur la cybercriminalité
  - Réprimer le vol d'identité
- Les dispositions du droit national
  - Dispositions actuelles
  - Réformes juridiques en cours

2e Partie : la preuve dans les procédures en matière de cybercriminalité

4 Enquêtes et poursuites pénales
- Les mesures procédurales prévues par la Convention sur la cybercriminalité
- Le rôle de la police, des procureurs, des juges, des services spécialisés
- Le droit procédural national

5 La coopération internationale

- La Convention sur la cybercriminalité
- Les dispositions du droit national et les accords bilatéraux

- Les points de contact 24/7
- Le rôle des juges

6 Obtenir, préserver et utiliser des preuves électroniques

- La preuve sur l'ordinateur du prévenu : présence de fichiers numériques utilisés à des fins de cybercriminalité
- La preuve identifiant la localisation d'un réseau : les adresses IP
- La preuve obtenue de fournisseurs de services Internet

7 Les procédures judiciaires et la jurisprudence : exemples

8.3 Exemples de formations de niveau avancé : structure et sujets abordés

8.3.1 Exemple de formation dispensée aux Pays-Bas

Formation approfondie – 4 jours
Programme :

Jour 1 et 2

L'infrastructure de l'Internet

- Comprendre comment fonctionne l'Internet
- Comment les ordinateurs communiquent entre eux ?
- Qu'est-ce que l'adresse IP et le code d'identification de l'ordinateur ?

Les informations sur l'Internet

- Comment recueillir des informations sur l'Internet
- Rechercher dans des bases de données Internet (cachées)

Le profilage de réseaux sociaux

- La communication
- L'anonymat
- La détermination de la localisation et de l'identité des ordinateurs, des entreprises et des personnes présentes sur l'Internet

Les traces numériques

- Qu'est-ce qu'une « trace » ?
- Quelles traces sont laissées sur un ordinateur ?
- Quelles traces sont laissées sur l'Internet ?
- Quelles traces sont laissées par la communication numérique ?

La sécurité

- Les risques de l'Internet
- L'importance d'une bonne sécurité numérique
- Les méthodes sûres de stockage d'informations
- La sécurité en matière de courrier électronique

Pendant ces deux jours, chaque participant a accès à un ordinateur connecté à l'Internet et peut expérimenter par des exercices concrets les sujets abordés. Le nom d'une personne est par exemple donné à chaque participant, à qui il est demandé de rechercher dans des sources Internet en accès libre le plus d'informations possibles à son sujet. Il est également demandé aux participants d'identifier l'origine d'un courrier électronique (à partir de son en-tête) ou de rechercher des traces de communication numérique.

Jour 3 et 4

Le cadre juridique

- Quelles sont les compétences de la police et des procureurs dans les enquêtes en matière de cybercriminalité
- Etude de cas présentée par l'équipe Criminalité technologique

L'Organisation chargée des enquêtes et des poursuites en matière de cybercriminalité aux Pays-Bas

L'interception (ce point ne figurera pas dans la nouvelle formation et sera intégré au programme élémentaire).

Les ripostes numériques

- Quelles ripostes connaissons-nous ?

- La jurisprudence concernant ces ripostes
- A quelles ripostes devons-nous nous attendre à l'avenir et comment réagir ?
- Etudes de cas

Des matériels de formation, un mémento couvrant tous les thèmes abordés pendant la formation et pouvant être utilisé comme ouvrage de référence, une version imprimée des présentations des formateurs et l'ouvrage *Handboek Digitale Criminaliteit* de Arjan Dasselaar sont distribués à chaque participant.

8.3.2 Proposition des Pays-Bas concernant une formation de niveau supérieur

Elaborer une nouvelle formation sur la cybercriminalité

Le "Intensiveringsprogramma Cybercrime", le Procureur national chargé de la cybercriminalité et le Centre de formation judiciaire néerlandais (SSR) mettent actuellement au point une nouvelle formation en matière de cybercriminalité qui comprendra aussi bien des cours généraux (l'interception) que des cours spécialisés sur des sujets plus spécifiques (les réseaux de machines zombies ou « botnets »).

Le programme n'est pas encore achevé, mais le premier jour sera consacré aux principes essentiels de l'interception (écoutes téléphoniques et écoutes sur l'Internet) et le deuxième jour consistera en un cours élémentaire sur la cybercriminalité. Ces deux cours devront être obligatoirement suivis par *tous* les procureurs des Pays-Bas dans le cadre de leur formation permanente. La deuxième partie de la formation sera réservée aux spécialistes de la cybercriminalité (les conditions d'admission seront très strictes) et consistera en un cours approfondi (2 à 4 jours) et en un cours supérieur de deux jours (annuel). Ces cours seront dispensés en coopération avec des partenaires extérieurs, tels que Fox-IT, Digital Intelligence training et Hoffman Bedrijfsrecherche.

La raison qui a poussé à mettre au point ce programme n'est pas le contenu insatisfaisant des formations existantes, mais la volonté de mieux structurer et ajuster leurs différents éléments afin d'éviter tout chevauchement. La restructuration de la formation a également été fortement motivée par la nomination, dans le cadre du « Intensiveringsprogramma », de procureurs spécialisés en matière de cybercriminalité au sein des onze principaux bureaux du ministère public néerlandais. Il est également essentiel qu'il y ait une progression dans la nouvelle formation ; chaque participant sera donc tenu de suivre d'abord les deux cours élémentaires avant d'être admis à la formation approfondie et aux cours supérieurs.

L'une des nouveautés envisagées de la formation sera la réalisation d'illustrations infographiques décrivant le fonctionnement et les risques de l'Internet. Ces illustrations sont actuellement dans la phase finale de leur mise au point et pourront également être utilisées lors des présentations pilotes. Les exemples suivants montrent comment se présenteront les illustrations infographiques.

Suivi

Afin de faire en sorte que les procureurs confrontés à la cybercriminalité dans leur pratique quotidienne puissent maintenir leurs connaissances à jour dans le monde en évolution rapide de la criminalité électronique, deux initiatives complémentaires sont actuellement développées.

La première est la création d'un Centre de connaissances et d'expertise au sein du Bureau national du ministère public de Rotterdam. Ce centre apportera des réponses à des questions d'ordre technique et judiciaire, suivra l'évolution de la jurisprudence et diffusera cette dernière ainsi que toutes autres informations pertinentes à l'ensemble des professionnels de la cybercriminalité, tant de la police que du ministère public (le centre est une initiative commune aux deux organisations).

Deuxièmement et dans le prolongement de ce projet, un « espace de coopération numérique », comparable à une application SharePoint est en cours de création. Dans cet espace virtuel, les cyberprofessionnels pourront débattre de questions liées à leur travail et trouver toutes sortes d'informations présentant un intérêt pour leur activité. Un inventaire des contenus et des possibilités (techniques) envisageables de cet espace numérique sera réalisé en octobre de cette année. Voici un exemple de ce à quoi pourrait ressembler la page d'accueil de cet espace :

Créer un sentiment d'urgence : la formation des responsables

Compte tenu des capacités relativement limitées des forces de police néerlandaises, des choix doivent être faits quant à l'opportunité d'enquêter sur telle ou telle infraction (note : le système juridique néerlandais autorise le ministère public à ne pas poursuivre et enquêter sur certaines infractions ; c'est le principe de l'« opportuniteitsbeginsel »). En général, ces décisions sont prises au niveau des responsables.

Or, de l'avis de la police et du ministère public, les responsables n'ont souvent pas conscience de l'impact de la cybercriminalité et de l'importance qu'il y a à lutter contre ce phénomène et, de ce fait, des affaires importantes peuvent ne pas être traitées parce que d'autres infractions (conventionnelles) sont jugées prioritaires. C'est pourquoi une formation destinée aux responsables des services de police et du ministère public est actuellement développée. D'après le calendrier des travaux, une formation pilote sera mise en place à la fin de cette année. Cette formation s'attachera essentiellement à faire prendre conscience aux responsables qu'il est urgent de lutter contre la cybercriminalité en les mettant face à la réalité de ce phénomène dans la société actuelle. Elle n'abordera donc pas ce thème sur le plan du contenu (comme le fait la formation approfondie), mais sous un angle stratégique et administratif.