V. 1er septembre 2020

Etude relative à la mise en œuvre de la formation judiciaire en matière de cybercriminalité et preuve électronique (Algérie)

rédigée dans le cadre du projet CyberSud

Clause de non-responsabilité

Les opinions exprimées dans ce rapport ne reflètent pas nécessairement les positions officielles du Conseil de l'Europe, de la Commission européenne ou des parties aux traités mentionnés.

Financé par l'Union européenne et le Conseil de l'Europe
UNION EUROPÉENNE
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Mis en œuvre par le Conseil de l'Europe

Table des Matières

LISTE DES ABREVIATIONS FREQUENTES

Algérie : République algérienne démocratique et populaire

CoE : Conseil de l'Europe

Convention de Budapest : Convention sur la cybercriminalité du Conseil de l'Europe

EJCN : European Judicial Cybercrime Network

ESM : Ecole Supérieure de la Magistrature (Algérie)

Formation judiciaire "Cyber" : formation judiciaire en cybercriminalité et preuve électronique

GAFA : Google/Amazon/Facebook/Apple

GLACY / GLACY + : Global Action on Cybercrime / Global Action on Cybercrime Extended

ISM : Institut Supérieur de la Magistrature (Maroc, Tunisie)

Maroc : Royaume du Maroc

Tunisie : République tunisienne

INTRODUCTION

Fort du constat de la menace grandissante de la cybercriminalité et de l'enjeu vital du développement sain de l'économie numérique dans les pays du voisinage Sud, les pays que sont l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie ont été considérés comme des pays prioritaires pour le programme CyberSud.

D'une durée de 54 mois (juin 2017- Décembre 2021) et doté d'un budget de plus de 5 millions d'euros, le programme CyberSud a pour ambition de renforcer la législation et les capacités institutionnelles sur la cybercriminalité et la preuve électronique en prenant en considération les droits de l'homme et l'Etat de droit, à travers 5 résultats principaux : *renforcement des cadres légaux de la législation pénale au regard de la Convention de Budapest ; la spécialisation des services d'enquête et la coopération publique-privée dans une approche durable ;* ***l'harmonisation de la formation judiciaire sur la cybercriminalité et la preuve électronique*** *; l'amélioration des outils et des compétences des autorités de poursuite pour la coopération internationale sur la cybercriminalité et la preuve électronique ; l'identification des priorités stratégiques sur la cybercriminalité et la preuve électronique*.

La présente étude rentre dans le cadre des activités prévues au titre de l'objectif d'harmonisation de la formation judiciaire sur la cybercriminalité et la preuve électronique. **Le champ de l'étude a toutefois été restreint aux pays bénéficiaires que sont l'Algérie, le Maroc et la Tunisie.**

Pour mémoire, le Maroc a bénéficié du projet joint UE/COE relatif à l'Action globale sur la cybercriminalité (**GLACY**) ayant pour objet de permettre aux autorités judiciaires pénales de s'engager dans la coopération internationale en matière de cybercriminalité et de preuve électronique sur le fondement de la Convention de Budapest sur la cybercriminalité. La durée du projet était de 36 mois (novembre 2013 - octobre 2016) avec un budget de 3,35 millions d'euros. Il était en grande partie financé par l'instrument de stabilité de l'Union Européenne soutenu par un co-financement du Conseil de l'Europe. Le projet GLACY a connu une extension sous l'acronyme GLACY+, d'une durée de cinq ans (2017 - 2021) avec un budget dédié.

Enfin, il convient de rappeler l'existence du Cybercrime Programme Office (C-PROC), basé à Bucarest (Roumanie), et qui assiste les pays à renforcer leur cadre légal et leur capacité à lutter contre la cybercriminalité, en complétant les travaux du Comité de la Convention de Budapest (T-CY).

L'étude présentera tout d'abord la volonté forte du Conseil de l'Europe d'initier et pérenniser des stratégies nationales de formation judiciaire en matière de cybercriminalité et preuve électronique (formation judiciaire Cyber) **(PARTIE I**), avant d'analyser les retours d'expérience des pays bénéficiaires (Algérie, Maroc, Tunisie) (**PARTIE II**).

PARTIE 1 Une volonté forte du Conseil de l'Europe d'initier et pérenniser des stratégies nationales de formation judiciaire en matière de cybercriminalité et preuve électronique

Avant d'étudier sa mise en œuvre et présenter une méthode d'évaluation (**II**), l'enjeu de la formation judiciaire Cyber au cœur du programme CyberSud sera présenté (**I**).

I. La formation judiciaire Cyber : un enjeu au cœur du programme CyberSud

Il sera d'abord exposé l'esprit de la stratégie CyberSud en matière de formation judiciaire Cyber (**A**) avant de présenter les éléments du système de formation judiciaire (**B**) ainsi qu'un état des lieux synthétiques des pays bénéficiaires objets de la présente étude (**C**).

A. L'esprit de la stratégie CyberSud en matière de formation judiciaire Cyber

La volonté du Conseil de l'Europe d'établir une stratégie de formation judiciaire en matière de cybercriminalité et de preuve électronique est ancienne (2009). Elle a pris forme d'un "papier concept" de la formation judiciaire en cybercriminalité produit par le Conseil de l'Europe (*Project on Cybercrime)* du 8 octobre 2009[1], élaboré en collaboration avec le réseau Lisbonne des institutions de formation judiciaire, et soutenu par les sociétés Microsoft et McAfee.

Les objectifs étaient alors de pallier les insuffisances constatées en matière de formation judiciaire dans le domaine de la cybercriminalité et de la preuve électronique, et se présentaient comme suit :

- *permettre aux instituts de formation d'assurer une formation initiale et continue en ce domaine et basée sur les standards de qualité internationale ;*
- *inculquer au plus grand nombre possible de juge et de procureur avec une connaissance basique sur la cybercriminalité et la preuve électronique ;*
- *fournir une formation avancée pour un nombre critique de juges et de procureurs ;*
- *soutenir une spécialisation continue et une formation technique des juges et procureurs ;*
- *contribuer à améliorer la connaissance au travers d'un réseau entre les juges et procureurs ;*
- *faciliter l'accès aux différentes initiatives de formation et réseaux.*

En conséquence dès 2009, les mesures suivantes étaient recommandées par le Conseil de l'Europe :

1. *Institutionnaliser la formation initiale*
2. *Institutionnaliser la formation continue*
3. *Développer des cours standardisés et adaptables*
4. *Permettre l'accès à de la documentation de formation/autoformation*
5. *Créer des centres pilotes pour la formation basique et avancée*
6. *Améliorer la connaissance au travers de réseaux*
7. *Tirer partie de la coopération publique/privée*

Ces idées inspireront largement la stratégie du programme CyberSud élaborée lors d'une conférence (30 juillet-3 août 2018) relative à l'adaptation de la formation judiciaire sur la cybercriminalité et la preuve électronique.

La Stratégie CyberSud pour aider les pays bénéficiaires à améliorer la formation judiciaire en matière de cybercriminalité et de preuve électronique s'articule ainsi autours d'objectifs et d'activités, afin de parvenir à une standardisation de la formation :

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c3

Objectifs à la fin du projet :

- inclusion de modules de formation en cybercriminalité et preuve électronique dans les programmes de formation des institutions de formation ;
- développement de cours de formation judiciaire nationaux sur la cybercriminalité et les preuves électroniques dans tous les pays prioritaires ;
- participation des magistrats de référence ayant reçu une formation de base et avancée dispensée par des formateurs locaux.

Activités prévues afin d'atteindre ces objectifs :

- préparer une évaluation (étude) sur les systèmes de formation des juges et des capacités dans la région de Voisinage du Sud ;
- organiser un atelier régional pour les représentants des institutions de formation judiciaire afin de parvenir à un accord sur la démarche à suivre ;
- organiser des ateliers de formations aux formateurs (dans cinq pays) ;
- soutenir l'adaptation des supports de formation (cours de base) ;
- soutenir la dispense d'un cours de base par des formateurs formés dans les cinq pays ;
- organiser une conférence régionale sur les progrès réalisés et sur l'intégration de la formation sur la cybercriminalité et la preuve électronique dans les programmes de formation des institutions de formation ;
- soutenir les ateliers nationaux pour le développement des cours de formation judiciaire nationaux sur la cybercriminalité et la preuve électronique ;
- soutenir la mise en place d'activités de formation dans le pays sur la base des cours de formation judiciaire nationaux et la mise en place d'une formation TOT pour les magistrats de référence.

Pour mémoire, le Conseil de l'Europe a développé une formation initiale et avancée (documentation pédagogique) en cybercriminalité et preuve électronique à destination des magistrats couvrant :

- le volet technique,
- la menace cybercriminelle,
- le droit matériel,
- le droit procédural,
- la preuve électronique,
- et la coopération internationale.

En résumé, l'approche de CyberSud est une "stratégie pour les inspirer tous", en ce qu'elle est le ferment des stratégies nationales propres des pays bénéficiaires. Comme indiqué en introduction, le champ de l'étude est restreint à l'Algérie, le Maroc et la Tunisie.

B. Eléments du système de formation judiciaire

Tout système de formation judiciaire repose sur des éléments structurants essentiels que sont l'institut de formation judiciaire, le programme de formation, le matériel de formation, les cours de formation, l'entraînement des formateurs (Training of Trainers) et bien évidemment les formateurs eux-mêmes.

Un institut de formation judiciaire

Le pilier central du système est naturellement l'organisme ou institut de formation judiciaire établi au niveau national. Classiquement le statut de cet institut est un établissement public à caractère administratif placé sous la tutelle du ministère de la Justice, bénéficiant d'un directeur et dont la gouvernance est souvent confiée à un conseil d'administration au sein duquel seront représentées des personnalités du monde judicaire (président et/ou procureur de la Cour de Cassation ou assimilés).

Traditionnellement l'institut de formation judiciaire aura en charge les missions suivantes :

- l'organisation des concours d'accès ;
- la formation initiale des futurs magistrats reçus aux concours ;
- la formation continue des magistrats en fonction.

Pour mémoire, la recommandation (2010) 12 du Comité des ministres du Conseil de l'Europe sur les juges[2] prévoit :

- que « les juges devraient bénéficier d'une formation initiale et continue théorique et pratique, entièrement prise en charge par l'Etat. […] ;
- qu'une autorité indépendante devrait veiller, en respectant pleinement l'autonomie pédagogique, à ce que les programmes de formations initiale et continue répondent aux exigences d'ouverture, de compétence et d'impartialité inhérentes aux fonctions judiciaires. »

Spécifiquement vis-à-vis de la formation à la lutte contre la cybercriminalité, qui est une nouvelle thématique, la quasi-totalité des juges et procureurs en fonction actuellement n'ont pas eu de formation en cybercriminalité. En conséquence, la formation continue des magistrats professionnels est un enjeu aussi impérieux que le développement de la formation initiale.

Programme de formation

Les programmes seront évidemment distincts entre la formation initiale et la formation continue, mais toutefois une mise en cohérence sera nécessaire une fois la formation initiale en place afin d'éviter les doublons de formation.

Un accent particulier sera mis sur la coopération internationale, indispensable en matière de cybercriminalité, et les mécanismes de la Convention de Budapest. Concernant la preuve électronique, son étude devrait adresser à la fois ses aspects techniques les plus marquants, mais aussi les nombreuses problématiques soulevées lors de son recueil dans une enquête pénale, le public visé étant constitué de juristes et non de techniciens. Les aspects de droit matériel et procéduraux devront être abordés, si possible après une première sensibilisation aux enjeux numériques.

Concernant la formation continue, il paraît très utile d'intégrer des déplacements dans les services d'enquête spécialisés en cybercriminalité mais aussi dans des laboratoires de Forensics.

Les formations pourront être classées en module « Basique » et « Avancé » (possible niveau « intermédiaire »). Par exemple, le module « basique » devra permettre d'expliquer le fonctionnement d'un ordinateur, des réseaux informatiques, d'Internet et des réseaux sociaux. Le résultat attendu est que le magistrat ait une connaissance suffisante de la définition d'une adresse IP, d'un disque dur ou d'un compte de réseau social. Ce point est essentiel pour assimiler les actes d'enquêtes indispensables et rédiger des missions d'expertise réalistes (procureur ou juge d'instruction).

Formellement, un arrêté du ministère de la Justice est parfois nécessaire pour modifier les programmes de formation, ce qui peut introduire une certaine lourdeur et requiert donc un dialogue de qualité entre la direction de l'institut de formation et les responsables de l'administration centrale du ministère.

Matériel de formation

Le matériel est souvent une combinaison de plusieurs formats (traitement de texte classique, *slides* de présentation, voire des vidéos). Un des avantages de la formation en cybercriminalité est l'abondance de

[2] https://rm.coe.int/16807096c2

source ouverte sur Internet avec du contenu de qualité pour illustrer les cours de formation. Il est possible également de tester de nouveaux formats pédagogiques comme le « serious game », des recherches en temps réel (sur Internet ou en mode sécurisé « bac à sable »). D'autre part, la préparation de cas pratique adaptés à la législation locale est essentielle pour des cours avancés.

Enfin, il sera toujours utile de distribuer en support de cours les textes de la Convention de Budapest (avec protocole et rapport explicatif) en plus de toute référence normative utile au thème du cours.

Cours de formation

Un des points importants est l'adéquation du volume horaire à l'ambition du cours abordé. En effet à titre d'exemple, il est impossible d'expliquer le fonctionnement et l'écosystème des cryptoactifs, ses possibilités de blanchiment associées et les bonnes pratiques de saisies dans le cadre d'une enquête pénale… en 30mn. Les formations initiales devraient au strict minimum prévoir 20h de cours et conférences. Les formations continues quant à elles pourraient être calibrées sur une semaine complète (5 jours). En tant que possible, des groupes moyens (entre 15 et 25 personnes) pourraient être constitués afin de permettre une meilleure participation.

Entraînement des formateurs

Il est d'une grande importance de constituer et conserver un vivier de formateurs. Les magistrats locaux qui bénéficient de formations en cybercriminalité et preuve électronique devraient être véritablement fléchés et fidélisés à des postes de formateurs/intervenants extérieurs réguliers afin de permettre un « retour sur investissement » en termes de formation cyber. Ces magistrats pourront bien sûr avoir un déroulement de carrière au sein des unités spécialisées en charge des affaires complexes (crime organisé, délinquance financière, anti-terrorisme, cybercriminalité).

Formateurs eux-mêmes

Les formateurs seront au premier titre des magistrats bien sûr (en détachement à l'institut de formation mais aussi en intervention extérieure ponctuelle), mais il ne faudrait pas hésiter à associer davantage d'autres experts, issus du monde de l'expertise Forensics, des services spécialisés d'enquête, ou encore de chercheurs en cybersécurité.

C. Etats des lieux synthétiques des Pays bénéficiaires concernés par la présente étude antérieurement au programme CyberSud

Il semble utile de dresser succinctement un état des lieux, antérieur au programme CyberSud, concernant les pays bénéficiaires étudiés. Les aspects sont variés, couvrant par exemple l'adhésion ou non à la Convention de lutte contre la cybercriminalité du Conseil de l'Europe (dite de Budapest), le statut de l'école de formation judiciaire, le formalisme nécessaire à la modification des programmes, l'existant en terme de formation initiale et continue (contenu pédagogique, volume horaire...).

1. Algérie

A titre préliminaire, il convient de relever que l'Algérie n'a pas encore adhéré à la Convention de Budapest, ni même était invitée officiellement par le Conseil de l'Europe à l'adhésion. Toutefois, il est à noter que la Convention de 2011 a inspiré le législateur algérien dans certaines dispositions du code pénal, et qu'une certaine compatibilité est déjà présente entre les deux échelons normatifs, ce qui ne peut que faciliter une future adhésion qui nous semble souhaitable.

Selon le document du 9 mars 2018, établi dans le cadre du projet CyberSud, intitulé "*Rapport de situation initiale*" sur les capacités de la justice pénale en matière de cybercriminalité et du traitement de la preuve

électronique en Algérie, la formation judiciaire est qualifiée de « *véritable fer de lance de la lutte contre la cybercriminalité, [...] apparue comme le domaine présentant les plus grandes possibilités de développement eu égard à l'existant et aux besoins exprimés* » (p32).

Selon des sources ouvertes3, l'école de formation judiciaire en Algérie est l'Ecole Supérieure de la Magistrature (ESM). Cette école qui était l'institut national de la magistrature depuis 1990, a été érigée en école supérieure par une loi organique du 6 septembre 2004, ayant le statut d'un établissement public à caractère administratif, jouissant de la personnalité morale et de l'autonomie financière.

Placée sous tutelle du Ministère de la Justice, elle est chargée de la formation de base des élèves-magistrats et de la formation continue des magistrats en exercice (décret exécutif du 20 août 2005, portant organisation de l'ESM et fixant les modalités de son fonctionnement, les conditions d'accès, le régime des études et les droits et obligations des élèves magistrats).

Ainsi, et toujours selon le rapport précité, « *les* ***représentants de la formation initiale*** *sont* ***conscients des nécessités*** *de l'apprentissage au plus tôt de la problématique liée au numérique mais* ***regrettent qu'une stratégie nationale soit inexistante*** ».

Il était suggéré dans le cadre du renforcement des capacités cyber des magistrats algériens de former à minima deux personnes par région (Wilaya) lesquelles pourraient ensuite relayer ladite formation en interne. Les autorités algériennes souhaitaient pour leur part disposer d'au moins 48 magistrats-référents pour couvrir l'ensemble des 48 Wilayas (division administrative territoriale).

De manière générale, il était envisagé les objectifs suivants :
- adapter et développer un module de formation élémentaire en matière de cybercriminalité et de preuve électronique à intégrer dans le cadre des modules obligatoires de droit matériel et de droit procédural en collaboration avec l'ESM ;
- créer des modules facultatifs avancés axés sur la cybercriminalité, la preuve électronique, sur les spécificités des infractions commises en Algérie ;
- organiser une formation de formateur pour la formation élémentaire et accompagner la dispense de la formation ;
- soutenir l'intégration de ces nouveaux modules dans le programme de formation initiale des magistrats ;
- créer un glossaire en langue arabe des termes techniques à destination de tous les magistrats.

De même afin de développer la formation continue, les actions suivantes étaient à privilégier :
- soutien à la dispense de la formation élémentaire en matière de cybercriminalité à destination des magistrats référents par des magistrats formateurs algériens ;
- adapter les modules facultatifs de la formation avancée au besoin des magistrats en exercice ;
- former les magistrats référant au guide sur le respect des exigences de la protection des données et des libertés fondamentales dans le cadre des enquêtes cybercrime ou impliquant la preuve électronique et faciliter la dissémination du guide.

Une formation de magistrats spécialistes était soutenue, afin de créer un véritable vivier :
- créer un concept de séminaire annuel en matière de cybercriminalité et de preuve électronique avec des interventions du secteur privé à destination des magistrats référents et des agents des forces de l'ordre ayant un niveau enquêteur cybercriminalité afin de discuter des nouvelles tendances et solutions pour les praticiens ;

[3] De manière surprenante, le rédacteur de la présente étude n'a pas trouvé le site officiel de l'ESM, potentiellement car il serait exclusivement en langue arabe.

- développer des formations sur des thématiques spécifiques pour les magistrats issus des 4 pôles spécialisés notamment l'entraide judiciaire en matière de cybercriminalité et de preuve électronique ;
- faciliter la mise en réseaux des magistrats référents de la région.

II. La mise en œuvre de la stratégie CyberSud de formation Cyber et la nécessaire évaluation de ces pays bénéficiaires

Les travaux du programme CyberSud dans les pays bénéficiaires seront exposés (**A**) avant d'aborder la création du Réseau Judiciaire CyberSud (**B**) et la méthodologie de l'évaluation de la présente étude (**C**).

A. Les travaux menés par le programme CyberSud pour l'élaboration d'une formation Cyber localement autonome

1. Algérie

Une première réunion est intervenue en **septembre 2018**, relative à la formation judiciaire de niveau basique, dans une logique "former les formateurs", avec un public de 24 magistrats algériens. Globalement positif, le retour de cette réunion pointait toutefois un manque de cas pratique pertinents. D'autre part, l'Algérie n'étant pas membre de la Convention de Budapest comme déjà évoqué, un temps important de réunion a été consacré à faire des comparaisons utiles entre les dispositions de la Convention de Budapest et celle de la procédure pénale locale.

Une seconde réunion l'a complété en **décembre 2018**, relative à la formation judiciaire de niveau avancé, toujours au bénéfice de 24 magistrats. Une participation active des magistrats a été soulignée, démontrant le sérieux de leur investissement professionnel. Le but de la réunion était de convaincre les autorités algériennes du besoin de créer une formation locale avant de la diffuser aux autres régions administratives (waliyas). Il était également recommandé d'adapter les documents de formation au droit local, ainsi que d'organiser des visites des unités spécialisés (police) afin de mieux appréhender les problématiques de preuve électronique.

Lors de l'atelier régional CyberSud des **23-25 janvier 2019** sur la formation judiciaire Cyber, les constats concernant l'Algérie ont été les suivants :
- la formation initiale actuelle est seulement un cours de sensibilisation sur la cybercriminalité et la preuve électronique. Depuis 2019, le programme de l'ESM a changé et prévoit désormais 4 années de formation pour les nouveaux magistrats. De nouveaux cours ont été introduits dont un **module entier dédié à la cybercriminalité et la preuve électronique** ;
- Il n'y a pas de stratégie nationale de formation en soi, mais la réflexion est en cours. Les points suivants sont considérés comme essentiels pour l'élaboration de cette stratégie : l'identification des besoins, l'établissement d'objectifs, un horizon, un mécanisme d'évaluation, un monitoring de la pérennité, une mobilisation transversale, et le développement de cours d'apprentissage en ligne sur la cybercriminalité et la preuve électronique ;
- En Algérie, le ministère de la justice donne les contours des objectifs des formations et ensuite l'ESM doit les mettre en œuvre. Sur les 6000 magistrats algériens, 40 ont été formés, notamment dans des universités occidentales sur la cybercriminalité et la preuve électronique. La prochaine étape est de former des magistrats référents pour chaque région, grâce au projet CyberSud.

Ainsi, la **première réunion du groupe de travail (GT) s'est tenue à l'ESM les 16 au 20 juin 2019**, notamment sur l'élaboration d'un manuel de formation judiciaire en cybercriminalité et preuve électronique. Il est à mettre au crédit de l'Algérie d'avoir déjà développé les contours détaillés de la formation initiale devant être dispensée aux futurs magistrats. Le directeur de la formation initiale a précisé que l'Algérie mène désormais une politique de spécialisation des magistrats et attache beaucoup

d'importance à développer ses propres ressources documentaires et capacités en termes de formations. Toutefois, il a été précisé que **l'intégration des cours en cybercriminalité se faisant en 3ème année, il semble que les futurs magistrats n'en bénéficieraient qu'à partir de l'année 2022**. Dans l'intervalle, l'ESM prévoit de déployer des formations continues pour les magistrats en fonction (niveau basique et avancé), en **privilégiant les magistrats référents** (avant les autres magistrats) ce qui fait sens. Le Conseil de l'Europe souhaitait apporter son soutien à la délivrance de formations locales aux magistrats référents. Les détails suivants peuvent être ajoutés :

- cours en formation initiale : les contours détaillés du cours sont donc élaborés, et programmés dans la 3ème année de cursus. La **partie théorique prévue est de 22,5 heures accompagnées d'une partie de travaux dirigés de 30 heures**. Le contenu de cette formation initiale sert de base de travail pour l'élaboration de la formation continue ;
- formation continue : **5 jours pour les formations basiques et avancées**, afin de se caler sur la durée standard des formations continues dispensées en Algérie pour les magistrats. Concernant la formation continue avancée, des travaux ont été menés sur des cas pratiques qu'il a été nécessaire d'adapter à la procédure locale avec un découpage en 2 phases (petits groupes de travail simulant des enquêteurs et un procureur ou juge d'instruction ; présentation des résultats de l'enquête par chaque groupe).

L'analyse des annexes au rapport de cette réunion de juin 2019 est instructive et démontre le sérieux de la démarche algérienne.

Par ailleurs, certaines recommandations semblent particulièrement pertinentes : avant d'entamer chaque phase, le formateur commence par une introduction afin d'en expliquer l'objectif ; remise d'attestations de participation souhaitable (avec la mention : « *formation en collaboration avec le conseil de l'Europe dans le cadre du programme CyberSud* ») ; assurer la variété des magistrats participants (parquet, instruction, siège).

La seconde réunion du GT sur l'élaboration d'un manuel de formation judiciaire en cybercriminalité et preuve électronique s'est déroulée les **17-18 février 2020.** Il est **dommage que le ministère de la justice algérien n'ait pas suivi la recommandation du Conseil de l'Europe de désigner les mêmes participants que la 1ère réunion du GT**, ce qui a fait perdre un temps précieux sur place.

Plusieurs modules ont été préparés sur des aspects de droit matériel, de procédure pénale, de preuve électronique, de coopération internationale, de coopération avec le secteur privé et sur les bonnes pratiques en matière de lutte contre la cybercriminalité et de récupération de preuve électronique.

Concernant la formation basique, il est précisé que certains des 10 modules doivent être redéfinis et recomposés, afin d'ajuster les thématiques abordées et mettre en concordance le temps nécessaire à la diffusion du contenu pédagogique. A titre d'exemple, le premier module de présentation générale prévoyait initialement une durée de 2h alors que le support comptait 112 *slides*. A l'inverse, le module sur les infractions en cybercriminalité prévoyait une durée de 3h et comptait 25 *slides* insuffisamment élaborées. Le module 9 (relatif à la recherche de preuve, aux réquisitions, investigation et jugements des affaires de cybercriminalité) semblait inachevé de manière flagrante (seulement 10 *slides*, avec une faible durée d'1h15).

Concernant la formation avancée, les éléments de cette formation ont été discutés, avec un aspect pratique à développer, une vraie connaissance et expérience des modèles (*templates*) à destination des fournisseurs de service numérique, une compréhension du fonctionnement du réseau 24/7 et de la rédaction d'une DEPI (MLAT), un esprit critique sur les possibilités et limites de l'analyse Forensics, et enfin une appropriation des enjeux de légalité de la preuve. Afin d'optimiser le temps de formation, il était recommandé de distribuer des documents à lire en amont sur des aspects techniques ou juridique comme support de cours.

Il existe une perspective encourageante malgré de nécessaires travaux de finalisation. La **troisième réunion du groupe de travail se tiendra dans la période à venir** et sera consacrée à la révision finale du manuel du cours avancé sur la cybercriminalité et les preuves électroniques pour la formation initiale et continue.

De cette manière, et **normalement d'ici la fin de l'année 2020, un cours complet, de base et avancé, de formation initiale et continue sur la cybercriminalité et les preuves électroniques sera disponible pour les magistrats algériens.**

B. Création du Réseau judiciaire CyberSud

Actée lors de l'atelier régional CyberSud de janvier 2019, la création du Réseau Judiciaire CyberSud s'est concrétisée par une première réunion organisée les **3-4 décembre 2019** à Lisbonne, avec le soutien du Bureau du Procureur Général du Portugal. Les pays bénéficiaires avaient missionné 2 (Maroc) ou 3 (Algérie et Tunisie) participants.
Bénéficiant de l'expérience du ministère public portugais en matière de coordination d'autres réseaux judiciaires internationaux (notamment Cibercrime), cet événement a rassemblé les pays prioritaires de CyberSud (**l'Algérie**, la Jordanie, le Liban, le **Maroc** et la **Tunisie**) dans le but d'établir le Réseau qui constituera un forum continu, permettant des échanges d'informations et de connaissances sur la cybercriminalité et les preuves électroniques.
La réunion s'est conclue avec l'accord des pays du CyberSud pour poursuivre cette initiative, en établissant la mission et les objectifs du Réseau pour la période future (3 années).
Plus précisément, **chaque pays devrait nommer 2 représentants permanents à ce réseau. Il convient de noter que l'ambition initiale était de nommer 3 représentants permanents par pays, avec 3 spécialités** (spécialiste de la lutte contre la cybercriminalité, membre du GT de l'élaboration du manuel Cyber, spécialiste de la coopération internationale).
Le projet CyberSud continuera à soutenir le Réseau judiciaire CyberSud et ses activités spécifiques en 2020. La prochaine réunion devait se tenir en juin 2020 en Tunisie. A la connaissance de l'expert rédacteur, cette réunion n'a pu être organisée, sans doute en raison de la crise sanitaire mondiale actuelle. **Il semblerait utile qu'une telle réunion puisse se tenir au dernier trimestre 2020, même en format virtuel, afin de ne pas casser une dynamique vertueuse.**

C. Exposé de la méthode d'évaluation de la présente étude

Afin de mettre en place une évaluation objective, conçue pour servir de base à d'autres évaluations ultérieures, l'auteur de la présente étude a défini 7 critères d'évaluation.

Les 7 critères retenus

Qualité du portage institutionnel
Implication et assiduité des magistrats locaux
Pérennité et fidélisation des magistrats locaux formés (CyberSud, GLACY +…)
Qualité du travail fourni en GT
Adéquation du volume horaire dans les formations locales
Implication dans le Réseau Judiciaire CyberSud
Calendrier de mise en œuvre des formations

De plus, une série de questions complémentaires a été posée aux responsables des pays bénéficiaires, via le Conseil de l'Europe (délai de réponse restreint au 6 août 2020) :

1. ***Pouvez-vous expliciter le niveau d'engagement politique et institutionnel dans votre pays relatif à l'établissement et la mise à jour de la stratégie de formation judiciaire en matière de cybercriminalité et de preuve électronique ?***
2. ***Quelles mesures concrètes ont été prises pour assurer la pérennité des travaux relatifs à l'élaboration des documents de formation judiciaire eux-mêmes, et à quel degré d'autonomie estimez-vous être parvenu dans leur élaboration au terme des actions menées jusqu'à présent dans le programme CyberSud (et potentiellement GLACY +) ?***
3. ***Avez-vous conduit des avancées significatives ces derniers mois dans l'élaboration des documents de formation judiciaire et dont les responsables du programme CyberSud du Conseil de l'Europe n'auraient pas encore été avisées ?***
4. ***Quelles mesures concrètes ont été prises pour capitaliser les investissements intellectuels des magistrats nationaux ayant reçu les formations du Conseil de l'Europe dans la perspective du concept "former les formateurs", notamment dans leurs parcours de carrière professionnelle (fidélisation, valorisation)***
5. ***Quels sont votre vision et vos attentes concernant le récent Réseau Judiciaire CyberSud ? Réciproquement, quels sont les moyens (humains et financiers) que vous êtes prêts à consentir pour faire vivre de Réseau ?***

Les réponses de l'Algérie ont été les suivantes :

1. *Dans le cadre de la politique de formation, nous veillons à accompagner les mutations juridiques et judiciaires aux niveaux national et international, notamment à travers les différents programmes de formation. A cet effet, une importance capitale a été accordée à la lutte contre la cybercriminalité et les preuves électroniques dans les programmes de formation continue et spécialisée destinés aux magistrats, dont un nombre considérable a participé à des formations spécialisées au niveau des universités étrangères, en plus des actions de formation en Algérie et à l'étranger réalisées dans le cadre de la coopération avec les Etats et les organisations internationales. Il est à noter que dans le cadre du programme européen de lutte contre le cybercrime (CyberSud), plusieurs actions de formation ont été inscrites au profit de notre secteur, dont une session de base et une session de formation approfondie ont été réalisées au profit d'un groupe de magistrats (21 magistrats de différentes juridictions), en plus de la participation de 10 magistrats et 06 cadres aux actions réalisées à l'étranger dans ce cadre.*
2. *A cet effet, un groupe de magistrats a été constitué pour élaborer les programmes de la formation continue pour les magistrats en exercice et de la formation de base au profit de élèves-magistrats. Deux réunions ont été tenues avec les experts du programme européen de lutte contre le cybercrime (CyberSud). Cette activité se poursuit encore actuellement.*
3. *La coordination est en cours au sein du groupe de travail chargé d'élaborer le document de la formation judiciaire et l'opération est en cours. Dès la finalisation du travail entrepris, les experts du programme seront avisés.*
4. *Dans le cadre de la stratégie de formation, nous œuvrons à exploiter le produit de la formation à travers l'animation des sessions de formation par les magistrats, ayant déjà bénéficié de la formation, au profit de leurs pairs et autres personnels du secteur de la justice, y compris l'officiers de la police judiciaire. Ces magistrats seront également appelés à transmettre leurs expériences et connaissances dans le cadre de la consultation. Par ailleurs, l'évaluation des magistrats au cours de la formation continue, les travaux réalisés et les titres obtenus, sont pris en compte lors de la promotion des magistrats.*
5. *En ce qui concerne le volet formation, le réseau pourrait être d'une grande utilité, notamment en matière d'échange de bonnes pratiques, de bons procédés et des évolutions en matière de lutte contre la cybercriminalité. Par ailleurs, ce réseau pourrait entretenir les échanges dans le domaine entre les professionnels. Nous attendons d'en savoir plus sur l'organisation et les modalités de fonctionnement projetées pour ledit réseau, pour faire des propositions à nos autorités, concernant l'adhésion au réseau et la contribution à son entretien.*

PARTIE 2 Des retours d'expérience inégaux mais encourageants de ces investissements au bénéfice de l'Algérie, du Maroc et de la Tunisie

Il sera procédé à l'évaluation des pays bénéficiaires (**I**) avant d'esquisser les points d'attention et pistes d'amélioration possibles (**II**). Les principales recommandations (communes et ciblées par pays bénéficiaire) feront l'objet d'un résumé en fin d'étude.

I. Evaluation des pays bénéficiaires dans leur appropriation de la stratégie CyberSud

L'évaluation repose donc sur l'appréciation des 7 critères précédemment évoquées, dotée d'une représentation visuelle en diagramme. Il sera précisé si les réponses complémentaires des représentants des pays bénéficiaires ont modifié l'appréciation initiale.

A. Algérie

Qualité du portage institutionnel. *La direction de l'ISM s'est pleinement engagée à soutenir le programme de formation judiciaire mis en place par le projet CyberSud, mais d'autres mesures doivent être prises pour impliquer davantage le ministère de la justice dans la mise en œuvre du programme.*

Implication et assiduité des magistrats locaux. *Les magistrats algériens ont démontré un grand sérieux dans la démarche, et ils ont participé activement aux cours de formation dispensés dans le cadre du projet en expliquant la législation nationale et en présentant des exemples nationaux.*

Pérennité et fidélisation des magistrats locaux formés. *Si les participants au GT n'ont pas toujours été les mêmes ce qui a été dommageable pour les travaux de rédaction, les travaux ont progressé grâce à l'engagement des magistrats concernés et il y a de bonnes perspectives de terminer l'adaptation du matériel de formation avant la fin de 2020. Concernant les magistrats devant bénéficier de la formation continue, le choix de privilégier les magistrats référents est cohérent.*

Qualité du travail fourni en GT. *La qualité du travail est assurée par l'engagement et l'expérience des magistrats impliqués dans le GT. Le produit final suivra les normes internationales et les meilleures pratiques adaptées au contexte national et à la législation qui permettront aux magistrats d'Algérie d'avoir accès à des cours de formation sur la cybercriminalité et la preuve électronique.*

Adéquation du volume horaire dans les formations locales. *Le format du cours de formation est conforme aux meilleures pratiques du niveau international et aux besoins actuels du pays, la partie théorique ayant prévue 22,5 heures accompagnées d'une partie de travaux dirigés de 30 heures, pour la formation initiale. Concernant la durée de la formation continue, une durée de 5 jours est adaptée.*

Implication dans le Réseau Judiciaire CyberSud. *Le Réseau Judiciaire CyberSud est à ces débuts, mais l'Algérie a montré de l'intérêt en envoyant 3 participants à la première réunion. Le projet CyberSud assurera le suivi de cette initiative et une deuxième réunion sera organisée afin de mettre en place le réseau et d'obtenir l'engagement des pays à se l'approprier dans le but de renforcer la coopération internationale dans la région.*

Calendrier de mise en œuvre des formations. *L'Algérie a fait le choix d'inclure les cours de formation Cyber seulement en 3ème année de formation initiale, ce qui a pour conséquence de ne faire bénéficier les futurs magistrats d'une formation Cyber qu'à compter de 2022, ce qui pourrait devoir être réévalué étant donné le besoin croissant de connaissances sur les enquêtes en matière de cybercriminalité et de preuve électronique pour les magistrats.*

Les efforts de l'Algérie en la matière ont donc été cohérent et fructueux, même si les effets en formation initiale ne seront pas perceptibles à court terme.

II. Points d'attention et pistes d'amélioration

Il doit être souligné l'importance d'une gouvernance adaptée (**A**) avant de suggérer des points d'attention et des pistes d'amélioration (**B**).

A. L'importance d'une gouvernance adaptée

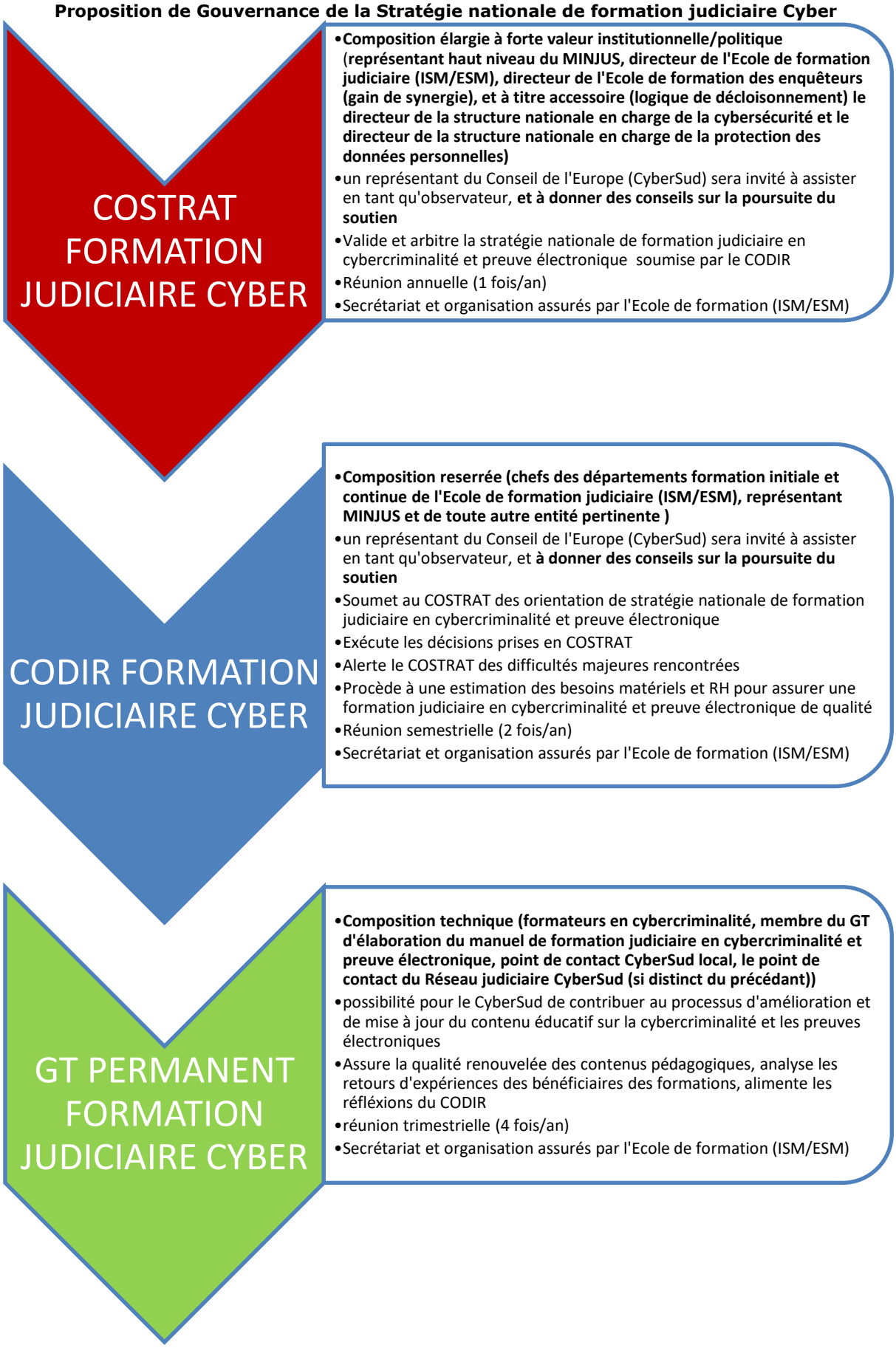
En tant que suggestion pour améliorer le portage institutionnel, il est vivement recommandé de mettre en place un schéma de gouvernance ambitieux (*cf schéma détaillé infra*), avec à sa tête un Comité Stratégique (COSTRAT) garant d'une légitimité politique forte, assisté d'un Comité de Direction (CODIR) en charge de la stratégie et s'appuyant sur un Groupe de Travail (GT) permanent ad hoc, à vocation technique.

Le secrétariat et l'organisation de cette comitologie seraient confiés à l'Ecole de formation judiciaire du pays bénéficiaire (ESM ; ISM). Une comitologie à 3 échelons permet d'assurer une fluidité et un suivi très régulier des progrès réalisés mais aussi d'identifier le plus en amont possible les difficultés susceptibles d'affecter la feuille de route stratégique établie par le CODIR et validée par le COSTRAT.

Le schéma proposé intègre également le support du projet CyberSud afin d'instaurer une relation institutionnelle de qualité, qui s'ajoute naturellement aux contacts étroits entre experts missionnés par le Conseil de l'Europe et leur contrepartie au niveau local.

La stratégie nationale de formation judiciaire Cyber aurait également vocation à assurer un soutien à long terme du récent Réseau Judiciaire CyberSud.

Proposition de Gouvernance de la Stratégie nationale de formation judiciaire Cyber



B. Autres pistes d'amélioration

Diverses suggestions sont faites pour améliorer certain des critères retenus pour l'évaluation, qui mériterait une mise à jour annuelle.

Suggestion pour la pérennité et la fidélisation des magistrats locaux formés

Il conviendrait de généraliser les **réseaux nationaux de magistrats référents** cyber au niveau des parquets (ou juge d'instruction), de mettre en place des **formations "certifiées" voire diplômantes** (avec des partenariats associant des universités de droit et/ou d'informatique[4]), de mettre en place de **véritables parcours de carrière des magistrats spécialisés en cybercriminalité** (avec l'aide de la direction des ressources humaines du ministère de la justice).

Suggestion pour améliorer la qualité du travail fourni en GT

Il serait opportun de **profiter des travaux menés par ailleurs au niveau international** comme inspiration pour compléter les versions actuelles des documentations pédagogiques. On peut relever ainsi la récente réunion des formateurs nationaux judiciaires sur la cybercriminalité et la preuve électronique (organisée par IPROCEEDS) les 10-12 juillet 2019. De même, il est évoqué une future mise à jour des cours de formation judiciaire en brainstorming avec les représentants de GLACY+, IPROCEEDS2 et CyberEast. Les pays bénéficiaires CyberSud devraient pouvoir avoir des synergies avec les travaux menés par ces entités.

Dans le même ordre d'idée, la **documentation OCTOPUS** qui est en source ouverte, devrait voir de nouveaux cours mis à jour **mi 2021**, avec **plusieurs niveaux de formation[5]** : module d'introduction ; modèle avancé ; preuves électroniques et coopération internationale. Il existe également des guides sur la preuve électronique, Forensics informatique, des Procédures Opérationnelles Standardisées et des modèles (templates) pour l'entraide pénale internationale relative aux données basiques de souscription, ainsi que pour le gel de données (les art 29-31 de la Convention de Budapest).

Enfin, il semble adapté de développer **certaines activités de formation sous un aspect de « serious gaming** », afin de garantir une participation réelle des magistrats formés. Les thèmes de la cryptomonnaie et de la lutte contre les Darknets sont particulièrement adaptés avec des simulations assistées par ordinateur (par exemple en mode « bac à sable »). Un contact pourrait être pris avec EUROPOL afin d'obtenir une possibilité d'utiliser leur outil de serious gaming nommé « Cryptopol »[6].

Suggestion pour la pérennité du Réseau Judiciaire CyberSud

Il est recommandé que le nouveau Réseau Judiciaire CyberSud ait à cœur de tisser des liens avec d'autres réseaux, comme le Forum Cibercrime[7] ou l'EJCN (European Judicial Cybercrime Network)[8] afin de trouver des synergies pour son organisation et son programme d'action.
Il paraît également fondamental d'obtenir un engagement de haut niveau politique et institutionnel afin de faire vivre ce réseau et de le doter de moyens suffisants, notamment en termes de secrétariat permanent du réseau.

---

[4] Une référence en la matière est le DU (Diplôme universitaire) Cybercriminalité de l'Université de Montpellier en France : https://cybercrime.edu.umontpellier.fr/

[5] https://www.coe.int/en/web/octopus/training

[6] https://www.europol.europa.eu/newsroom/news/game-for-europol-and-centric

[7] http://cibercrime.ministeriopublico.pt/en/pagina/launching-cybercrime-and-digital-evidence-forum-portuguese-speaking-public-prosecution

[8] https://rm.coe.int/pedro-verdelho-european-judicial-cybercrime-network/1680921850 ; https://www.coe.int/documents/9252320/50407188/3156_112_European+Cybercrime+Judicial+Network.pdf/a4ee1197-5ba6-db4a-5107-80e0f0764097

CONCLUSION

L'implémentation de la stratégie CyberSud de formation judiciaire Cyber **dans les pays bénéficiaires est réalisée à des degrés divers, mais** entre globalement dans sa dernière ligne droite. Toutefois, force est de constater une certaine fragilité de cette implémentation **générée à la fois par un important turn over des magistrats locaux mais aussi un portage politique et institutionnel variable. Afin de consolider ses fondations et garantir des progrès dans la durée, il est** vivement recommandé d'adopter une comitologie adaptée**, dont un modèle est suggéré dans la présente étude.** Cet aspect nous semble prioritaire**.**

La crise sanitaire mondiale a certainement eu un impact négatif sur l'avancement des travaux relatifs à l'élaboration des documents de formation judiciaire**, mais il est souhaitable désormais de** boucler une version opérationnelle pour le dernier trimestre 2020**.**

Enfin, l'implémentation réelle **dans les formations initiales et continues devrait être mise en place dans un** délai raisonnable et si possible courant 2021**. Les magistrats en fonction bénéficiaires de la formation continue devraient constituer un vivier de magistrats référents en cybercriminalité au niveau des juridictions pénales.**

RESUME DES RECOMMANDATIONS COMMUNES

- ***Mettre en place une comitologie adaptée assurant un haut portage politique et institutionnel, la validation d'une stratégie nationale de formation judiciaire Cyber et un contenu pédagogique de qualité et actualisé*** *;*
- ***S'engager dans la durée afin de faire vivre le Réseau Judiciaire CyberSud*** *;*
- ***Développer/adapter des « serious game » dans des domaines divers de la cybercriminalité (Ex : cryptoactifs et la lutte contre les Darknets****);*
- ***Capitaliser sur les prochaines mises à jour des documents pédagogiques Octopus / IPROCEEDS2 / GLACY+ / CYBEREAST*** *;*
- **Instituer des réseaux nationaux de magistrats référents cyber au niveau des juridictions pénales** ;
- **Mettre en place des formations "certifiées" voire diplômantes en matière de cybercriminalité et de preuve électronique, et faciliter de véritables parcours de carrière des magistrats spécialisés en cybercriminalité.**

RESUME DES RECOMMANDATIONS CIBLEES

- ***[ALGERIE] Réfléchir à la possibilité d'initier une sensibilisation à la cybercriminalité et à la preuve électronique plus tôt dans la formation initiale (et pas seulement au bout de la 3ème année).***

ANNEXES

Liste des documents fournis dans le cadre de l'étude :

- Rapport de situation initiale de l'Algérie sur les capacités de la justice pénale en matière de cybercriminalité et du traitement de la preuve électronique (v 9 mars 2018) ;
- Rapport d'activité sur la formation judiciaire basique en Algérie (23-27 septembre 2018) ;
- Rapport d'activité sur la formation judiciaire avancée en Algérie (3-7 décembre 2018) ;
- Rapport d'activité sur l'intégration de la formation judiciaire Cyber en Algérie (16-20 juin 2019) ;
- Rapport d'activité sur l'intégration de la formation judiciaire Cyber en Algérie -2ème réunion (17-18 février 2020)
- Rapport sur le séminaire « adaptation de la formation judiciaire en cybercriminalité et preuve électronique » (Strasbourg, 30 juillet-3 août 2018) ;
- Rapport sur l'atelier régional « stratégie de formation judiciaire » (23-25 janvier 2019, Liban) ;
- Rapport de la 1ère réunion du Réseau Judiciaire CyberSud (3-4 décembre 2020) ;