LA LUTTE CONTRE LA CYBERCRIMINALITÉ

ENTRAIDE JUDICIAIRE
PROJET BEPI

SOMMAIRE

LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Abréviations, acronymes utilisés

BC	Convention de Budapest
BSI	« Basic Suscriber information » = informations basiques sur le souscripteur
CoB	Convention de Budapest
CoE	Conseil de l'Europe
DDoS	Distributed denial of Service/Déni de service
IMEI	Numéro d'identification d'un équipement mobile
IP	« Internet Protocol »
OSINT	« Open Source Intelligence » = Renseignement d'origine source ouverte
STAD	Système automatique de traitement des données

INTRODUCTION

Les technologies de l'information se sont insinuées, d'une manière ou d'une autre, dans tous les aspects des activités humaines, il ne reste quasiment plus aucun secteur qu'elles n'aient marqué de leur empreinte.

Ces développements ont également fait apparaître de nouveaux champs de délinquance qui s'appuient sur ces nouvelles technologies.

De fait, les menaces posées par la cybercriminalité sont diverses.

Ainsi, les **attaques contre les systèmes d'information**, en particulier celles liées à la criminalité organisée, constituent une menace croissante à l'échelle mondiale, et l'**éventualité d'attaques terroristes contre les systèmes d'information** qui font partie de l'infrastructure critique des États suscite de plus en plus d'inquiétude.

Outre les attaques dont ils sont victimes, les systèmes d'information peuvent être utilisés comme instruments d'infractions comme la violence sexuelle exercée en ligne, les atteintes à la dignité et à l'intégrité des personnes, le vol, l'utilisation abusive de données personnelles qui constituent une violation du droit au respect de la vie privée, les escroqueries de toutes sortes, etc.

L'information circule plus facilement que jamais à travers le monde. Sauf exception, les frontières ne font pas obstacle si bien que la **délinquance ne se cantonne plus à un espace géographique donné.** Les nouvelles technologies bousculent donc les principes juridiques existants notamment celui de la territorialité des infractions, dès lors que leurs auteurs peuvent se trouver dans des lieux fort éloignés de ceux où leurs actes produisent leurs effets.

Plusieurs instruments internationaux visant à favoriser la coopération internationale des organes de lutte se proposent de relever le défi ainsi posé, en tenant dûment compte de la nécessité de respecter les droits de l'Homme dans la nouvelle société de l'information.

Après avoir décrit, dans un premier temps, les différentes menaces observées et leurs acteurs, seront présentés les instruments internationaux de lutte contre la cybercriminalité, et enfin les difficultés rencontrées en terme d'investigation et de poursuite de ce type d'infraction.

L'on trouvera en annexe un glossaire des principales expressions techniques utilisées dans la fiche.

MODULE 1. LES PHÉNOMÈNES CRIMINELS

La cybercriminalité est définie comme telle lorsqu'un système automatique de traitement des données (STAD[1]) est l'objet du crime ou est utilisé comme outil pour commettre une infraction.

La cybercriminalité est polymorphe, ses acteurs vont du « brouteur » de cybercafé, à l'organisation criminelle à financement étatique. Ses atteintes vont du vol de compte bancaire au blocage d'une administration d'Etat.

I. LES CYBERMENACES

A - ATTEINTES VISANT LES STAD

Un cybercriminel peut utiliser un système automatique de traitement des données (STAD) pour accéder aux informations personnelles d'un utilisateur, à des informations confidentielles professionnelles, à des informations gouvernementales, pour désactiver un appareil, saturer un site, etc.[2]

Il s'agit d'exploiter les vulnérabilités des systèmes d'information eux-même.

a - Le déni de service

Les organisations les plus exposées comme les hôpitaux, les services administratifs, sont souvent ciblées par l'attaque informatique dite par déni de service (DDoS) qui vise à rendre inaccessible un site web en envoyant, par exemple, une grande quantité de requêtes pour en saturer l'accès. Une attaque DDoS s'appuie sur l'exploitation d'une faille de sécurité et conduit à stopper un service ou à nuire à son fonctionnement.

Afin de provoquer un déni de service par saturation de requêtes, des méthodes sophistiquées sont utilisées telle la création et l'utilisation de « réseaux zombies », qui consiste à établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyberattaques ciblées. Une fois créé, le réseau d'ordinateurs contaminés est activé

1 On se reportera pour les termes techniques au glossaire en annexe I

2 Voir par exemple pour l'analyse de la menace : https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

à l'insu des utilisateurs de ces terminaux dans le but de lancer une cyberattaque à grande échelle qui va provoquer l'interruption des services de réseaux présentant un intérêt public important, causer des coûts financiers majeurs, la perte de données à caractère personnel ou d'informations sensibles.

L'attaque peut avoir un objectif financier et cesser moyennant paiement d'une rançon, ou viser à nuire à un Etat en paralysant ses services ou menaçant des infrastructures vitales.

b - Le rançongiciel

Aussi appelé ransomware, il s'agit d'une attaque informatique qui repose sur un programme malveillant qui empêche l'accès aux ordinateurs ou aux fichiers en les chiffrant. Le but de cette attaque informatique est d'extorquer de l'argent, bien souvent en cryptomonnaie, en échange du rétablissement de l'accès aux données ou au système pris en otage. Comme pour les DDoS, les entreprises, les administrations ainsi que les centres hospitaliers sont régulièrement victimes de ce type d'attaque aux répercussions fortement préjudiciables en terme financier ou d'image.

En général, l'installation du rançongiciel sur la configuration ciblée intervient lors de l'ouverture d'une pièce jointe infectée ; il suffit d'un clic sur un lien malveillant contenu dans un mail de phishing ou en naviguant sur un site web compromis. Le rançongiciel peut aussi être installé à la suite d'une intrusion sur le système via une vulnérabilité non corrigée.

c - La fuite et la violation de données

La fuite et la violation de données personnelles ou confidentielles correspondent à l'accès, au déplacement, au stockage et à la diffusion non autorisés d'informations confidentielles, personnelles ou financières détenues par un tiers, qui peut être un site internet, une entreprise, une collectivité, une administration.

La fuite de données est le résultat d'une exposition involontaire d'une base de données sensibles. Cette exposition peut avoir lieu sur Internet ou résulter de la perte d'un disque dur ou de tout autre appareil contenant ces données.

La violation de données est liée à une cyberattaque menée par un logiciel malveillant.

Quelle que soit la forme prise, il s'agit d'une violation sérieuse de la sécurité et de la vie privée, pouvant causer de graves préjudices aux victimes (personnes et organisations). La fuite et la violation de données personnelles peuvent avoir un impact financier et juridique important et nuire gravement à la réputation de l'organisation en entrainant une perte de confiance des clients, usagers et partenaires.

Les sms corrompus (smishing) sont un fréquent vecteur d'attaque en violation des données, en particulier bancaires.

d - Le piratage informatique

Le piratage informatique fréquemment utilisé par les cybercriminels, consiste pour le pirate (hacker), à s'installer furtivement dans un ordinateur, un serveur, un réseau, un service en ligne, un téléphone mobile ou un objet connecté pour en prendre le contrôle. Une fois dans la place, le pirate collecte de manière illicite les données sensibles de l'organisation.

Orchestrée à partir de vulnérabilités non corrigées du système d'information et des équipements connectés, cette attaque va notamment servir à mener des opérations de fraude bancaire, d'usurpation d'identité, etc.

e - L'usurpation de site

L'attaque informatique par détournement de site web, ou website spoofing, repose sur l'usurpation d'identité. Son mode opératoire est le suivant : un site à forte notoriété est cloné pour créer un site malveillant et y attirer les internautes afin de collecter des informations de connexion, des informations bancaires et autres données confidentielles qu'ils croient livrer à un site authentique.

La redirection des internautes vers ces faux sites se fait à partir de liens trompeurs présents dans des mails de phishing. Certains programmes malveillants peuvent également modifier le fichier d'accueil des terminaux pour rediriger les personnes vers des sites web illicites plutôt que vers des sites officiels. Ainsi, en associant l'adresse par exemple d'une banque à celle d'un faux site, l'utilisateur sera redirigé automatiquement vers une page falsifiée similaire à l'originale, mais truffée de liens frauduleux.

f -Les virus

Il s'agit d'une attaque informatique qui cherche à compromettre la sécurité des systèmes dans lesquels ils sont injectés, d'altérer le bon fonctionnement des ressources numériques, ou de prendre leur contrôle. Ils peuvent aussi servir à voler des données confidentielles et sensibles.

Certains virus s'installent de manière dérobée en exploitant des vulnérabilités système ou logicielles non corrigées. Les virus informatiques n'ont pas besoin d'un fichier hôte pour se propager. Ils se répliquent automatiquement, contaminant d'autres appareils via les réseaux ou les e-mails.

Les virus classiques utilisent un fichier joint piégé ou se cachent dans un logiciel illicite ; ils s'activent dès leur ouverture et amorcent leur réplication. Les virus polymorphes modifient leur structure et ne conservent jamais la même signature, ce qui rend leur détection par des antivirus inopérante et complexifie grandement leur éradication.

Parmi les virus les plus connus, on peut citer :

- Les chevaux de Troie (« Trojans ») sont cachés dans un programme en apparence légitime à partir duquel ils ouvrent une porte dérobée (*backdoor*) qui leur permet de prendre le contrôle de l'appareil infecté, collecter des données…

- Le *keylogger* est un virus espion dont l'objectif est d'enregistrer les frappes clavier de l'utilisateur et de mémoriser les données saisies. Cette technique est souvent utilisée pour voler des identifiants de connexion et des données bancaires.

B - ATTEINTES FACILITÉES PAR LES STAD

Il s'agit là pour les cybercriminels d'exploiter les vulnérabilités, non plus des systèmes eux-mêmes mais des individus qui les utilisent.

Ces atteintes peuvent être regroupées en trois catégories :

- Atteintes aux biens : infractions crapuleuses bien connues, mais dont le mode opératoire s'est modernisé avec l'informatique.

- Atteintes aux personnes.

- Atteintes à la souveraineté et à la démocratie : les cyber techniques constituent un champ d'action idéal pour le développement des ingérences étrangères.

a -Les atteintes aux biens

Manifestation	Mode opératoire	Qualification possible
Romance sous une identité artificielle	Utilisation des réseaux sociaux, création de fausses identités, faux mails, utilisation de sites doublons	Escroquerie : utilisation d'une fausse qualité pour provoquer la remise de fonds
Faux sites bancaires		
Faux sites de vente en ligne		
Faux ordres de virement		
Se procurer des informations ou images sensibles par l'usage d'une fausse qualité ou par intrusion dans un STAD	Menaces de diffusion des images intimes ou compromettantes	Extorsion, chantage
	Menace de diffuser des informations sensibles	

b -Les atteintes aux biens

Manifestation	Mode opératoire	Qualification possible
Envoi de nombreux messages de dénigrement	Utilisation des réseaux sociaux, des courriels, de plusieurs comptes	Escroquerie : utilisation d'une fausse qualité pour provoquer la remise de fonds
Utilisation de données fuitées	Piratage de données personnelles dans un site et mise en vente à travers Instagram, Telegraph, Snapchat	Recel d'atteinte à un STAD
Chercher à entrer en contact avec des mineurs en ligne	Utilisation des réseaux Snapchat, Facebook, etc.	Prémisses d'une infraction future
Prostitution en ligne	Monter un site de prostitution en ligne	Proxénétisme
Diffusion d'images pédopornographiques	Diffuser, vendre des images illicites à travers des réseaux sociaux	Pédocriminalité
Révélation de la véritable identité et des informations personnelles d'une personne connue en ligne sous un pseudo	Utilisation des réseaux sociaux, souvent utilisé en cas de vengeance personnelle	Harcèlement

A cette liste non exhaustive peut-être ajouté le trafic de produits illicites, notamment les stupéfiants, en ligne.

c -Les atteintes à la souveraineté de l'Etat

<table>
<tr><th>Manifestation</th><th>Mode opératoire</th><th>Qualification possible</th></tr>
<tr><td>Compromission d'un employé</td><td>Piratage de boite mail, d'informations intimes dont la publication serait critique</td><td>Atteinte au STAD, extorsion, chantage</td></tr>
<tr><td>Attaques contre des sites institutionnels</td><td rowspan="2">Attaques par déni de service, logiciels malveillants</td><td rowspan="2">Atteinte au STAD</td></tr>
<tr><td>Dégradation, destruction de réseaux</td></tr>
<tr><td>Stratégie de désinformation en ligne</td><td>Création d'un réseau de zombies et de faux comptes multipliant de fausses informations prenant l'apparence de vraies</td><td rowspan="2">Fonction des droits nationaux ; par ex. infraction de diffusion de fausses informations...</td></tr>
<tr><td>Influence sur le débat public</td><td>Multiplication des soutiens ou les critiques des candidats</td></tr>
</table>

II. LES ACTEURS DE LA CYBERCRIMINALITÉ

Être un cybercriminel ne requiert pas nécessairement un haut niveau de connaissance technique mais suppose l'utilisation de STAD pour parvenir à ses fins. En fonction de leur niveau de compétence, les cybercriminels pourront trouver les instruments nécessaires à leur activité sur des réseaux clandestins, le plus souvent sur ce qui est dénommé le *dark web*.

Sont ainsi accessibles, les outils et données suivants :

- Journaux d'infostealers[3] non analysés et bases de données compromises (données divulguées ou volées), qui peuvent contenir des données personnelles, des identifiants d'utilisateur pour divers services, des contrefaçons de navigateur et d'autres informations sensibles.
- Données de cartes bancaires non analysées ou vérifiées (généralement obtenues par skimming numérique).
- Vente en masse de détails de cartes vérifiées.
- Offres d'accès initial, allant des identifiants pour des services et comptes à distance (par exemple RDP, VPN, pare-feu, dispositifs réseau et environnements cloud) jusqu'à des accès via des portes dérobées à des systèmes et réseaux d'entreprise.
- Identifiants de connexion pour divers services web, y compris les comptes email, les réseaux sociaux, les sites de commerce en ligne et les sites de contenu pour adultes.
- Abonnements à des kits de *phishing*, des infostealers, des kits d'exploitation de vulnérabilités, des droppers (programmes qui installent des malwares), des services de spoofing (usurpation d'identité) et des modèles de langage malveillants (LLMs).
- Des solutions d'évasion de détection, telles que les VPN, l'hébergement à l'épreuve des poursuites (BPH[4]), les proxies résidentiels, les services de blanchiment d'argent, les manuels de sécurité opérationnelle (OpSec), etc.

Dresser une typologie des acteurs est une gageure car les mêmes criminels peuvent intervenir sur plusieurs « marchés ». Peuvent être distingués cependant des catégories d'acteurs en fonction de leurs niveaux de compétence technique.

Les cybercriminels spécialisés dans le vol de données et la vente d'accès initial[5] utilisent une large gamme de méthodes. Ils ciblent les victimes et les systèmes en masse et cherchent à exploiter les failles techniques et humaines ; cette approche opportuniste se reflète dans la diversité des outils et des techniques qu'ils emploient, choisis en fonction de leur pertinence et de leur disponibilité.

3 Un « infostealer » est un logiciels voleurs d'informations ; un journal d'infostealer est le relevé de toutes les informations volées pour un jour donné. Il contient des informations très diverses et doit être exploité pour en tirer les données utiles à la commission d'une autre infraction.

4 BPH : Bulletproof hosting ; service d'hébergement web conçu pour protéger les activités illégales contre les interventions extérieures

5 « Initial access brokers » (IABs)

Ils utilisent des infostealers (logiciels voleurs d'informations), dont l'achat est proposé sur des plateformes criminelles occultes, pour collecter des informations auprès de leurs victimes. Ils les diffusent via des botnets qui orchestrent des campagnes de *phishing*, de spams, de publicité, utilisées pour distribuer des logiciels malveillants.

Les données volées, telles que les journaux d'infostealers et les bases de données piratées sont, soit exploitées directement soit revendues et exploitées par d'autres criminels spécialisés dans l'extraction et l'analyse de ce type d'informations.

Les données volées qui permettent par exemple l'accès à des cibles stratégiques (grandes entreprises internationales, chaînes logistiques informatiques, infrastructures critiques), sont négociées par les voleurs avec des groupes cybercriminels qui peuvent être spécialisés dans les *ransomwares*, ou *dropper* ; la rémunération de l'offreur se fait parfois en pourcentage des gains du groupe acheteur[6].

Certains groupes criminels se spécialisent dans le vol de données financières et l'accès aux systèmes de paiement. Ils sont les principaux clients des fournisseurs de services illégaux comme les kits de phishing et les skimmers numériques qui permettent de créer de fausses pages web dont les liens sont diffusés via des campagnes de phishing ou insérés dans des sites mal sécurisés.

Les informations volées (identifiants bancaires, données personnelles) ainsi collectées sont ensuite revendues sur des plateformes en ligne spécialisées dans ce type de commerce.

Les auteurs d'escroquerie, les fraudeurs au sentiment, n'ont pas besoin d'un très haut niveau de compétence pour commettre leurs forfaits. Ils ne cherchent en général pas à vendre les données personnelles de leurs victimes sur un marché quelconque, ils les utilisent directement pour essayer de les faire chanter ou de les extorquer. Les spécialistes de la pédopornographie cherchent à vendre les images illicites collectées à des amateurs, en général sur des marchés clandestins qui peuvent se trouver sur le dark web, mais également dans des messageries cryptées.

Certains de ces criminels peuvent ne pas travailler seuls mais partagent les données personnelles de leurs cibles avec des groupes organisés repérés sur des applications chiffrées; cette coopération permettant d'augmenter la pression sur les victimes, confrontées à plusieurs chantages simultanés.

Les groupes étatiques constituent un autre type d'acteur. Composé soit de services proches de certains Etats, travaillant parfois avec des groupes criminels indépendants, ils participent à des campagnes de désinformation ou de déstabilisation par l'utilisation de botnets ou de faux comptes.

QUESTIONS

- Avez-vous eu connaissance d'atteintes de cet ordre à titre personnel ou professionnel ?
- Connaissez-vous les services en charge de la lutte contre cette forme de criminalité dans votre pays ?
- Avez-vous eu connaissance de campagnes de prévention ?
- Savez-vous comment essayer de s'en prémunir ?

6 Source Europol ; https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

MODULE 2. LE DROIT DE LA CYBERCRIMINALITÉ

Il s'agira dans ce module de dresser un tableau rapide des dispositions internationales et nationales de lutte contre cette forme moderne de criminalité, les dispositif propres à la cybersécurité n'étant pas abordés.

I. LES INSTRUMENTS INTERNATIONAUX DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Confronté à la dimension transfrontalière de la cybercriminalité les Etats, au niveau régional, ou à celui des Nations Unies ont élaboré des conventions organisant une réponse commune. Ces conventions ont été transposées dans les droits nationaux pour ce qui concerne les Etats parties ou ont inspiré les droits positifs des Etats non parties.

A -LES PRINCIPAUX INSTRUMENTS

Il s'agit de conventions signées dans un cadre régional et, récemment, universel :

▶ Convention du Conseil de l'Europe sur la cybercriminalité signée à Budapest le 27 novembre 2001 (STE185[7]).

Il s'agit d'une convention ouverte qui a notamment été signée par les Etats Unis, le Bénin, le Sénégal ou la Côte d'Ivoire. Elle vise à :

- Harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité.
- Fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique.
- Mettre en place un régime rapide et efficace de coopération internationale, notamment par la création d'un réseau 24/7 d'entraide rapide entre les Parties, constitué de correspondants capables de répondre en permanence aux demandes des autres Etats parties.

▶ Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et la divulgation de preuves numériques (STCE n°224[8]).

Il vient compléter la convention précédente. Il vise à renforcer la capacité des autorités de justice

7 STCE 185 - Rapport explicatif de la Convention sur la cybercriminalité

8 Liste complète - Bureau des Traités : https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=224

pénale (Justice, Police) à recueillir des preuves électroniques d'une infraction au moyen d'outils de coopération entre autorités compétentes plus rapides et efficaces.

▶ Convention de l'Union Africaine sur la cybersécurité et la protection des données personnelles signée à Malabo le 27 juin 2014.

En droit pénal substantiel, elle modernise les instruments de répression de la cybercriminalité, par l'élaboration d'une politique d'adoption d'incriminations nouvelles spécifiques et par l'adaptation de certaines incriminations, des sanctions et du régime de responsabilité pénale en vigueur dans les États Membres à l'environnement des technologies de l'information et de la communication. En droit pénal procédural, elle fixe le cadre de l'aménagement de la procédure classique relativement aux technologies de l'information et de la communication.

▶ Convention des Nations Unies contre la cybercriminalité, ouverte à la signature à Hanoï le 25 octobre 2025.

Elle a pour objectif le renforcement de la coopération internationale pour la lutte contre certaines infractions commises au moyen de systèmes d'information et de communication et établit un régime de communication de preuves sous forme électronique des infractions instaurées par la Convention.

POUR MÉMOIRE :

▶ La Convention arabe sur la lutte contre les infractions liées aux technologies de l'information signée le 21/12/2010

Son objectif principal est de consolider et améliorer la coopération entre les Etats arabe en matière de lutte contre la cybercriminalité. La Mauritanie en est signataire.

▶ Directive C/DIR/1(08)11 du 19 aout 2011 de la CEDEAO sur la lutte contre la cybercriminalité dans l'espace CEDEAO

Elle vise à harmoniser les cadres de répression pénale en vue de lutter efficacement contre la cybercrimnalité. Elle est antérieure à la Convention de Malabo qui en développera les éléments.

B - CRÉER LES CONDITIONS D'UN DROIT PARTAGÉ

Classiquement, ces conventions contiennent des dispositions d'harmonisation du droit pénal de fond permettant d'éviter les refus de coopération pour absence de double incrimination, ainsi que d'adaptation du droit procédural à la spécificité des données numériques, de telle sorte que les Etats parties se dotent de moyens d'action procéduraux identiques. Elles prévoient également des dispositions favorisant l'entraide pénale.

La structure de ces instruments est constante puisqu'ils visent à harmoniser le droit de fond, le droit processuel et faciliter l'entraide.

a - Harmonisation du droit pénal de fond

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ

Les mesures à prendre au niveau national en matière de droit pénal sont prévues au Titre I de la Convention :

Titre I : « Infractions contre la confidentialité, l'intégrité et la disponibilité des données » qui incluent :

- Accès intentionnel sans droit à tout ou partie d'un système informatique ;
- L'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique.
- Le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
- L'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.
- La production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies ci-dessus; d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre de ces infractions.

Titre II : « Les infractions informatiques » incluent :

- Falsification : altération, effacement ou suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles.
- Fraude : toute introduction, altération, effacement ou suppression de données informatiques, toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre III : Infractions se rapportant au contenu (pornographie enfantine) ;

Titre IV : Infractions liées aux atteintes à la propriété intellectuelle.

CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SÉCURITÉ

Article 29 : Les infractions spécifiques aux Technologies de l'Information et de la Communication :

Les État Parties s'engagent à prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale :

a. Atteintes aux systèmes informatiques

a) Accéder ou tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé.

b) Accéder ou tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé avec l'intention de commettre une nouvelle infraction ou faciliter une telle infraction.

c) Se maintenir ou tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique.

d) Entraver, fausser ou tenter d'entraver ou de fausser le fonctionnement d'un système informatique.

e) Introduire ou tenter d'introduire frauduleusement des données dans un système informatique.

f) Endommager ou tenter d'endommager, effacer ou tenter d'effacer, détériorer ou tenter de détériorer, altérer ou tenter d'altérer, modifier ou tenter de modifier frauduleusement des données informatiques.

b. Atteintes aux données informatisées

a) Intercepter ou tenter d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

b) Introduire, altérer, effacer ou supprimer intentionnellement et sans droit des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles.

c) En connaissance de cause, faire usage des données obtenues de manière frauduleuse.

d) Obtenir frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique.

e) Même par négligence, procéder ou faire procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre.

f) Participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente convention.

c. Les infractions se rapportant au contenu

a) à d) pédopornographie

e) Créer, télécharger, diffuser ou mettre à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

f) Menace de commettre une infraction pénale envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

g) Proférer une insulte envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique,

ou l'appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

h) Nier délibérément, d'approuver ou de justifier des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

CONVENTION DES NATIONS UNIES CONTRE LA CYBERCRIMINALITÉ

Chaque État partie adopte les mesures législatives et autres nécessaires pour conférer le caractère d'infraction pénale conformément à son droit interne, lorsque l'acte a été commis intentionnellement et sans droit à :

Article 7. L'accès illégal : accéder à tout ou partie d'un système d'information et de communication sans droit.

Article 8. L'interception illégale : intercepter des données électroniques lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système d'information et de communication.

Article 9. L'atteinte à l'intégrité de données électroniques : endommager, effacer, détériorer, altérer ou supprimer des données électroniques.

Article 10. L'atteinte à l'intégrité d'un système d'information et de communication : entraver gravement le fonctionnement d'un système d'information et de communication par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données électroniques.

Article 11. Utilisation abusive de dispositifs

a) L'obtention, la production, la vente, la fourniture pour utilisation, l'importation, la distribution ou à d'autres formes de mise à disposition :

i) D'un dispositif, y compris un programme, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 7 à 10 de la présente Convention ou ;

ii) D'un mot de passe, de justificatifs d'accès, d'une signature électronique ou de données similaires permettant d'accéder à tout ou partie d'un système d'information et de communication ; afin que ce dispositif, y compris ce programme, ou ce mot de passe, ces justificatifs d'accès, cette signature électronique ou ces données similaires servent à commettre l'une des infractions établies conformément aux articles 7 à 10 de la présente Convention et ;

b) À la détention d'un élément visé aux alinéas a) i) ou ii) du paragraphe 1 du présent article.

Article 12 : Falsification en rapport avec les systèmes d'information et de communication : effacement ou suppression de données électroniques engendrant des données non authentiques.

Article 13 : Vol ou fraude en rapport avec les systèmes d'information et de communication

a) Toute introduction, toute altération, tout effacement ou toute suppression de données électroniques ;

b) Toute atteinte au fonctionnement d'un système d'information et de communication ;

c) Tout acte de tromperie concernant des circonstances factuelles, commis à l'aide d'un système d'information et de communication, qui incite une personne à faire ou à omettre de faire quelque chose qu'elle n'aurait autrement pas fait ou omis de faire ;

dans l'intention frauduleuse ou malhonnête de réaliser sans droit un gain financier ou autre à son

profit ou à celui d'autrui.

Article 14 : Infractions relatives à des contenus en ligne présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants :

a) Produire, offrir, vendre, distribuer, transmettre, diffuser, exhiber, publier ou mettre autrement à disposition des contenus présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants au moyen d'un système d'information et de communication ;

b) Solliciter ou fournir des contenus présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants ou accéder à de tels contenus au moyen d'un système d'information et de communication ;

c) Détenir ou contrôler des contenus présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants stockés dans un système d'information et de communication ou sur un autre support de stockage;

d) Financer des infractions établies conformément aux alinéas a) à c) du présent paragraphe, ce que les États parties peuvent ériger en infraction distincte.

Aux fins du présent article, par « contenu présentant des abus sexuels sur enfant ou l'exploitation sexuelle d'enfants », on entend tout contenu visuel, et on peut entendre tout contenu écrit ou sonore, qui dépeint, décrit ou représente une personne de moins de 18 ans :

a) Se livrant à un acte sexuel réel ou simulé ;

b) En présence d'une personne qui se livre à un acte sexuel ;

c) Dont les organes sexuels sont exhibés à des fins principalement sexuelles ; ou

d) Qui est soumise à des actes de torture ou à des peines ou traitements cruels, inhumains ou dégradants, lorsque ce contenu est à caractère sexuel.

Article 15 : Sollicitation ou manipulation psychologique aux fins de commettre une infraction sexuelle à l'encontre d'un enfant.

Article 16 : Diffusion non consentie d'images intimes :

1. Au fait de vendre, de distribuer, de transmettre, de publier ou de mettre autrement à disposition une image intime d'une personne au moyen d'un système d'information et de communication, sans le consentement de la personne représentée sur l'image.

2. Aux fins du paragraphe 1 du présent article, on entend par « image intime » un enregistrement visuel.

Article 17 : Blanchiment du produit du crime

i) Conversion ou transfert de biens dont celui ou celle qui s'y livre sait qu'ils sont le produit du crime, dans le but de dissimuler ou de déguiser l'origine illicite desdits biens ou d'aider toute personne qui est impliquée dans la commission de l'infraction principale à échapper aux conséquences juridiques de ses actes ;

ii) Dissimulation ou déguisement de la nature véritable, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété de biens ou de droits y relatifs, dont celui ou celle qui s'y livre sait qu'ils sont le produit du crime ;

iii) À l'acquisition, à la détention ou à l'utilisation de biens dont celui ou celle qui les acquiert, les détient ou les utilise sait, au moment de leur réception, qu'ils sont le produit du crime ;

iv) À la participation à l'une des infractions établies conformément au présent article ou à toute association, entente, tentative ou complicité par fourniture d'une assistance, d'une aide ou de conseils en vue de sa commission.

b - Harmonisation du droit procédural

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ

La Section 2 de la Convention est entièrement dédiée au « droit procédural ».

L'article 14 porte le principe général selon lequel : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques. »

L'article 16 concerne la conservation rapide des données stockées : chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ;

- Permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification. »
- Obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne. »

L'article 17 regarde la conservation et divulgation partielle rapides de données relatives au trafic

« Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a) Ppour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et :

b) Pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise. »

L'article 18 propose que les Etats instaurent une mesure d'injonction permettant à ses autorités compétentes d'ordonner :

« A une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

A un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services. »

L'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu.

L'article 19 est relatif à la perquisition et saisie de données informatiques stockées.

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a) À un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et

b) À un support du stockage informatique permettant de stocker des données informatiques sur son territoire. »

Ces mesures sont précisées au § 3 et incluent :

« a) Saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;

b) Réaliser et conserver une copie de ces données informatiques;

c) Préserver l'intégrité des données informatiques stockées pertinentes;

d) Rendre inaccessibles ou enlever ces données informatiques du système informatique consulté. »

Les règles relatives à la collecte en temps réel de données de trafic sont évoquées à **l'article 20**.

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a) À collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique. »

Celles relative à la collecte des données de contenu le sont à **l'article 21** :

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b) À obliger un fournisseur de services, dans le cadre de ses capacités techniques :

i) À collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique. »

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secret le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. »

CONVENTION DE L'UNION AFRICAINE SUR LA CYBERSECURITÉ ET LA PROTECTION DES DONNÉES PERSONNELLES SIGNÉE À MALABO LE 27 JUIN 2014.

Le § 3 de l'Article 31 de la Convention porte les mesures nécessaires que les État Parties s'engagent à prendre pour favoriser la saisie et la conservation des données sollicitées par d'autres Etats parties :

> a) Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire d'un État Partie, sont utiles à la manifestation de la vérité, la juridiction saisie puisse opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.
>
> b) Lorsque l'autorité judiciaire en charge de l'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, soient copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés, selon des modalités prévues dans les législations des États Parties.
>
> c) [.]
>
> d) Si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, l'autorité judiciaire en charge de l'instruction puisse faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou une toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret.
>
> e) Si les nécessités de l'information l'exigent l'autorité judiciaire en charge de l'instruction puisse utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant sur son territoire ou ceux des États Parties, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

CONVENTION DES NATIONS UNIES CONTRE LA CYBERCRIMINALITÉ

Le chapitre IV de la Convention énonce les mesures qui doivent être adoptées par les Etats parties pour « instaurer les pouvoirs et procédures prévus aux fins d'enquête et de poursuite pénale » afférentes aux infractions relatives à la cybercriminalité. Il s'agit de mesures permettant[9] :

Article 25 : Préservation accélérée de données électroniques stockées

« 1) Permettre à ses autorités compétentes d'ordonner ou d'obtenir de façon similaire la préservation rapide de certaines données électroniques, y compris des données de trafic, des données de contenu et des informations relatives aux personnes abonnées qui ont été stockées au moyen d'un système d'information et de communication, notamment lorsqu'il existe des raisons

9 Le texte des articles cités n'est pas repris in extenso mais soit résumé soit partiellement cité d'où la discontinuité de numérotation des §

de penser que ces données électroniques sont particulièrement susceptibles d'être perdues ou modifiées.

2) Lorsqu'un État partie donne effet au paragraphe précédent au moyen d'une injonction ordonnant à une personne de préserver certaines données électroniques stockées qui se trouvent en sa possession ou sous son contrôle, il adopte les mesures nécessaires pour obliger cette personne à préserver lesdites données électroniques et à en protéger l'intégrité pendant une durée au maximum de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation.»

Article 26 : Préservation et divulgation partielle accélérées de données de trafic

Afin d'assurer la préservation des données de trafic en application de l'article 25 de la présente Convention, chaque État partie adopte les mesures législatives et autres nécessaires :

> « a) Pour veiller à la préservation rapide de ces données de trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de la communication ; et
>
> b) Pour veiller à la divulgation rapide à son autorité compétente, ou à une personne désignée par cette autorité, d'une quantité de données de trafic suffisante pour que l'État partie puisse identifier les fournisseurs de services et la voie par laquelle la communication ou les informations indiquées ont été transmises. »

Article 27 : Injonction de produire

Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à ordonner :

> « a) À une personne présente sur son territoire de communiquer des données électroniques spécifiées qui sont en sa possession ou sous son contrôle et qui sont stockées dans un système d'information et de communication ou sur un support de stockage de données électroniques ; et
>
> b) À un fournisseur de services offrant des prestations sur son territoire de communiquer les données relatives aux personnes abonnées qui sont en sa possession ou sous son contrôle concernant ces prestations. »

Article 28 : Perquisition et saisie de données électroniques stockées

Chaque État partie adopte les mesures législatives et autres nécessaires pour :

« 1) Habiliter ses autorités compétentes à perquisitionner :

> a) Un système d'information et de communication ou une partie de celui-ci ainsi que les données électroniques qui y sont stockées ; et
>
> b) Un support de stockage de données électroniques dans lequel pourraient être stockées les données électroniques recherchées, ou à y accéder de façon similaire sur son territoire.

2) Que ses autorités locales soient en mesure de procéder rapidement à la perquisition pour obtenir l'accès à cet autre système d'information et de communication.

3) Habiliter ses autorités compétentes à saisir ou à obtenir de façon similaire, sur son territoire, des données électroniques auxquelles il a été accédé conformément aux paragraphes 1 ou 2 du présent article. Ces mesures incluent les prérogatives suivantes :

> a) Saisir ou obtenir de façon similaire un système d'information et de communication, ou une partie de celui-ci, ou un support de stockage de données électroniques ;

b) Réaliser et conserver une copie de ces données électroniques au format électronique ;

c) Préserver l'intégrité des données électroniques stockées concernées ;

d) Rendre ces données électroniques inaccessibles ou les retirer du système d'information et de communication auquel il a été accédé. »

Article 29 : Collecte en temps réel de données de trafic

Chaque État partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer, par l'application de moyens techniques sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer, par l'application de moyens techniques sur son territoire ; ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer ; en temps réel, les données de trafic associées à des communications spécifiées transmises sur son territoire au moyen d'un système d'information et de communication.

Article 30 : Interception de données de contenu

Chaque État partie adopte les mesures législatives et autres nécessaires, en ce qui concerne diverses infractions pénales graves à définir en droit interne, pour habiliter ses autorités compétentes à :

a) Collecter ou enregistrer, par l'application de moyens techniques sur son territoire ; et

b) Obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i) À collecter ou à enregistrer, par l'application de moyens techniques sur son territoire ; ou

ii) À prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer ; en temps réel, les données de contenu de communications spécifiées transmises sur son territoire au moyen d'un système d'information et de communication.

Article 31 : Gel, saisie et confiscation du produit du crime

1) Chaque État partie adopte, dans toute la mesure possible dans le cadre de son système juridique interne, les mesures nécessaires pour permettre la confiscation :

a) Du produit du crime provenant d'infractions établies conformément à la présente Convention ou de biens dont la valeur correspond à celle de ce produit ;

b) Des biens, matériels ou autres instruments utilisés ou destinés à être utilisés pour les infractions établies conformément à la présente Convention.

2) Chaque État partie adopte les mesures nécessaires pour permettre l'identification, la localisation, le gel ou la saisie de tout ce qui est mentionné au paragraphe 1 du présent article aux fins de confiscation ultérieure.

3) Chaque État partie adopte, conformément à son droit interne, les mesures législatives et autres nécessaires pour réglementer l'administration par les autorités compétentes des biens gelés, saisis ou confisqués visés aux paragraphes 1 et 2 du présent article.

c -Renforcer la coopération

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ ET SON PROTOCOLE ADDITIONNEL N°2

Le Protocole additionnel n°2 dont 2 chapitres sur 3 sont entièrement dédiés à la coopération internationale, contient des dispositions très novatrices, qui seront reprises par la Convention des Nations Unies. Il est le fruit de l'expérience acquise au long des années d'application de la Convention de Budapest. Son préambule mérite d'être cité :

« CONSCIENTS que les preuves recueillies sous forme électronique de toute infraction pénale sont de plus en plus stockées sur des systèmes informatiques situés dans des juridictions étrangères, multiples ou inconnues, et convaincus que des mesures supplémentaires sont nécessaires pour obtenir légalement ces preuves afin de permettre une réponse effective par la justice pénale et de défendre l'État de droit;

RECONNAISSANT la nécessité d'une coopération accrue et plus efficace entre les États et le secteur privé et que, dans ce contexte, une plus grande clarté ou sécurité juridique est nécessaire pour les fournisseurs de services et autres entités concernant les circonstances dans lesquelles ils peuvent répondre à des demandes directes de divulgation de données électroniques émanant des autorités de justice pénale d'autres Parties;

ENTENDANT donc renforcer encore la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques grâce à des outils supplémentaires relevant d'une entraide plus efficiente et d'autres formes de coopération entre autorités compétentes; de la coopération en situation urgente; et de la coopération directe entre autorités compétentes et fournisseurs de services et autres entités qui possèdent ou contrôlent les informations pertinentes… ».

Il convient de se référer à son texte pour en apprécier la portée [10].

CONVENTION DE L'UNION AFRICAINE SUR LA CYBERSECURITÉ ET LA PROTECTION DES DONNÉES PERSONNELLES SIGNÉE A MALABO LE 27 JUIN 2014.

L'Article 28 est dédié à la Coopération internationale, ses dispositions sont les suivantes :

« 1) Harmonisation

Les États Parties s'engagent à garantir que les mesures législatives et/ou réglementaires adoptées pour lutter contre la cybercriminalité renforcent la possibilité d'harmonisation régionale de ces mesures et respectent le principe de la double incrimination.

2) Entraide judiciaire

Les États Parties qui n'ont pas de conventions d'assistance mutuelle en matière de cybercriminalité s'engagent à encourager la signature des conventions d'entraide judiciaire en conformité avec le principe de la double incrimination tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre les organisations des États membres sur une base bilatérale et multilatérale. »

10 https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=224

CONVENTION DES NATIONS UNIES CONTRE LA CYBERCRIMINALITÉ

Les dispositions relatives à la Coopération internationale sont prévues au Chapitre V de la Convention

L'Article 35 fixe les principes généraux relatifs à la coopération internationale

1) Les États parties coopèrent entre eux conformément aux dispositions de la présente Convention, ainsi que des autres instruments internationaux applicables concernant la coopération internationale en matière pénale, et à leur droit interne, aux fins suivantes :

> a) Enquêtes, poursuites et procédures judiciaires concernant les infractions pénales établies conformément à la présente Convention, y compris le gel, la saisie, la confiscation et la restitution du produit de ces infractions ;
>
> b) Collecte, obtention, préservation et communication de preuves sous forme électronique des infractions pénales établies conformément à la présente Convention ;
>
> c) Collecte, obtention, préservation et communication de preuves sous forme électronique de toute infraction grave, dont celles établies conformément à d'autres conventions et protocoles des Nations Unies applicables en vigueur au moment de l'adoption de la présente Convention.

2) En matière de coopération internationale, chaque fois que la double incrimination est considérée comme une condition, celle-ci est réputée remplie, que la législation de l'État partie requis qualifie ou désigne ou non l'infraction de la même manière que l'État partie requérant, si l'acte constituant l'infraction pour laquelle l'assistance est demandée est une infraction pénale en vertu de la législation des deux États parties.

L'Article 36 est relatif à la protection des données personnelles.

L'Article 37 fixe les règles de l'extradition dont on retiendra pour l'essentiel :

1) Le présent article s'applique aux infractions pénales établies conformément à la présente Convention lorsque la personne faisant l'objet de la demande d'extradition se trouve sur le territoire de l'État partie requis, à condition que l'infraction pour laquelle l'extradition est demandée soit punissable par le droit interne de l'État partie requérant et de l'État partie requis.

2) Nonobstant le paragraphe 1 du présent article, un État partie dont la législation le permet peut accorder l'extradition d'une personne pour l'une quelconque des infractions pénales établies conformément à la présente Convention qui ne sont pas punissables en vertu de son droit interne.

3) Chacune des infractions auxquelles s'applique le présent article est de plein droit incluse dans tout traité d'extradition en vigueur entre les États parties en tant qu'infraction pouvant donner lieu à extradition. Les États parties s'engagent à inclure ces infractions en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition qu'ils concluront entre eux.

L'Article 38 concerne le transfèrement des personnes condamnées

L'Article 39 traite du transfert des procédures pénales

« 1. Si un État partie qui subordonne le transfert des procédures pénales à l'existence d'un traité reçoit une demande de transfert d'un État partie avec lequel il n'a pas conclu pareil traité, il peut considérer la présente Convention comme la base légale du transfert des procédures pénales pour les infractions auxquelles le présent article s'applique. »

L'Article 40 fixe les principes généraux et les procédures d'entraide judiciaire

1) Les États parties s'accordent mutuellement l'entraide judiciaire la plus large possible lors des

enquêtes, poursuites et procédures judiciaires concernant les infractions établies conformément à la présente Convention, et aux fins de la collecte de preuves sous forme électronique des infractions établies conformément à la présente Convention, ainsi que d'infractions graves.

2) L'entraide judiciaire qui est accordée en application du présent article peut être demandée aux fins suivantes :

a) Recueillir des témoignages ou des dépositions ;

b) Signifier des actes judiciaires ;

c) Effectuer des perquisitions et des saisies, ainsi que geler des avoirs ;

d) Perquisitionner des données électroniques stockées au moyen d'un système d'information et de communication, ou y accéder de façon similaire, les saisir ou les obtenir de façon similaire, et les divulguer conformément à l'article 44 de la présente Convention ;

e) Collecter en temps réel des données de trafic conformément à l'article 45 de la présente Convention ;

f) Intercepter des données de contenu conformément à l'article 46 de la présente Convention ;

g) Examiner des objets et visiter des lieux ;

h) Fournir des informations, des preuves et des estimations d'experts ;

i) Fournir des originaux ou des copies certifiées conformes de documents et dossiers pertinents, y compris des documents administratifs, bancaires, financiers ou commerciaux et des documents de société ;

j) Identifier ou localiser le produit du crime, des biens, des instruments ou d'autres choses afin de recueillir des preuves ;

k) Faciliter la comparution volontaire de personnes dans l'État partie requérant ;

l) Recouvrer le produit du crime ;

m) Fournir tout autre type d'aide compatible avec le droit interne de l'État partie requis.

3) Les États parties peuvent invoquer l'absence de double incrimination pour refuser de fournir une aide en application du présent article. [.] L'aide peut être refusée lorsque la demande porte sur des questions mineures ou des questions pour lesquelles la coopération ou l'aide demandée peut être obtenue sur le fondement d'autres dispositions de la présente Convention.

4) Toute personne détenue ou purgeant une peine sur le territoire d'un État partie et dont la présence est requise dans un autre État partie à des fins d'identification ou de témoignage ou pour qu'elle apporte de toute autre manière son concours à l'obtention de preuves dans le cadre d'enquêtes, de poursuites ou de procédures judiciaires relatives à des infractions établies conformément à la présente Convention, peut faire l'objet d'un transfèrement. »

II. LES DROITS NATIONAUX

Les Etats partenaires du Projet ont adopté des dispositifs légaux de lutte contre la cybercriminalité. Seront cités les principaux textes applicables tels qu'ils résultent des contributions des participants à l'atelier.

A - BÉNIN

Le dispositif de lutte contre la cybercriminalité résulte de :

- Loi n°2017-20 du 20 avril 2018 portant code du numérique, telle que modifiée par la loi n° 2020-35 du 06 janvier 2021
- Loi n° 2018-16 du 28 décembre 2018 portant code pénal en République du Bénin.

Le Centre National d'Investigations Numériques (CNIN) est en charge de cette lutte. Il travaille en synergie avec la Cellule Nationale de Traitement des Infractions Financières (CENTIF).

Le Bénin est signataire des conventions de Budapest et Malabo.

B - CÔTE D'IVOIRE

Le texte de base est la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité est le principal instrument juridique en la matière.

Depuis le 30 octobre 2024, la Côte d'Ivoire s'est dotée d'une Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), autorité nationale chargée de protéger les infrastructures critiques, les systèmes d'information publics et privés, et de coordonner la réponse aux crises liées au cyberespace.

La Cote d'Ivoire a signé les Conventions de Budapest et Malabo.

C - GUINÉE

La lutte contre la cybercriminalité est régie en Guinée par :

- Loi N°/2016/037/AN relative à la Cyber-sécurité et la protection des données à caractère personnel
- Loi N°/2021/0024/AN portant lutte contre le blanchiment de capitaux et le financement du terrorisme en République de Guinée.

Aux termes de la Loi 2016/037, l'ANSSI est chargée de la prévention (veille), de l'alerte, des investigations, de la recherche, de la détection, de la riposte.

La Guinée est signataire de la Convention de Malabo.

D - MAURITANIE

La Mauritanie a adopté un dispositif complexe constitué de plusieurs textes législatifs qui couvrent différents aspects de la lutte[11] :

- Loi n° 07/2016 relative à la cybercriminalité, qui prévoit des procédures spécifiques,
- Loi n° 014/2021 relative aux services et moyens de paiement électronique
- Loi n° 025/2013 relative aux communications électroniques

11 On se reportera à l'annexe II pour une présentation détaillée de ces textes

- Loi n° 022/2018 relative aux échanges électroniques
- Loi n° 020/2017 relative à la protection des données à caractère personnel
- Loi n° 023/2018 relative à la criminalisation de la discrimination
- Loi n° 015/2020 relative à la lutte contre la manipulation de l'information
- Loi n° 021/2021 relative à la protection des symboles nationaux et à la criminalisation des atteintes à l'autorité de l'État et à la dignité du citoyen.

La Mauritanie est pas ailleurs signataire de :

- La Convention de Malabo
- La Convention arabe sur la lutte contre les infractions liées aux technologies de l'information.

E - SÉNÉGAL

Le dispositif sénégalais de lutte contre la cybercriminalité est le suivant :

- Loi 2008-11 du 25 janvier 2008 sur les infractions commises à travers les technologies de l'information et de la communication
- Loi 2008-12 sur la protection des données personnelles
- Loi 2008-08 du 25 janvier 2008 sur les transactions électroniques
- Loi 2008-10 du 25 janvier 2008 sur la société de l'information
- Loi 2016-29 du 08 novembre 2016 sur les infractions liées aux technologies de l'information et de la communication
- Loi 2021-34 relative à la procédure applicable à la criminalité organisée et des interceptions de correspondances téléphoniques ou émises par voie électronique

Le Sénégal est par ailleurs signataire des conventions de Budapest et de Malabo.

F - TCHAD

Le dispositif tchadien de lutte contre la cybercriminalité repose sur le cadre juridique établi par plusieurs ordonnances et une autorité nationale : l'Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE) qui, sous la tutelle du ministère de la sécurité, est en charge de la cybersécurité et des transactions électroniques.

Le cadre juridique est constitué par :

- La loi 2014-006 sur la lutte contre la cybercriminalité qui définit les infractions et les procédures y afférents.
- Ordonnance n°009 du 31 août 2022 qui adapte le dispositif aux nouvelles menaces notamment en imposant aux entités publiques et privés des obligations d'audit de sécurité ?

QUESTIONS

Par rapport aux conventions dont votre pays est signataire,

- Ont été ou non transposées en droit national ?
- Sont-elles accessibles aux magistrats ?
- Dans l'affirmative, quelles sont les dispositions qui , selon vous, seraient manquantes dans les textes de transpositions par rapport aux conventions signées
- Quelles dispositions seriez-vous ou avez-vous été le plus en mesure d'appliquer ?

MODULE 3. LES « CYBER INVESTIGATIONS »

I. LES INVESTIGATIONS TECHNIQUES[12]

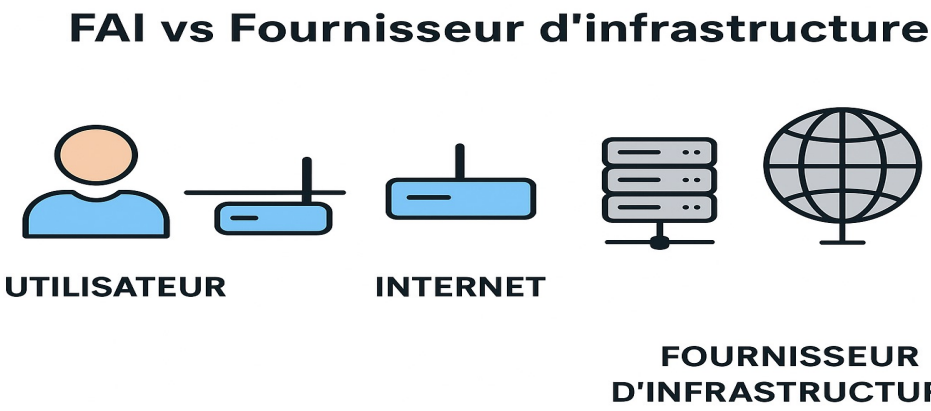
Une rapide description de l'architecture de l'internet et de ses opérateurs précèdera un exposé des actions qui peuvent être entreprises pour démasquer les criminels cachés au fond de la toile...

Cette image est purement illustrative et ne préjuge pas des affirmations qui y sont portées.

A - L'ARCHITECTURE DE L'INTERNET

L'Internet » est un univers constitué d'une multitude d'intervenants.

12 Pourront être consultés utilement les guides suivants qui ont , entre autres, servi à l'élaboration de présente fiche technique : https://www.osce.org/files/f/documents/a/534684/8.pdf ; https://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation



Ce schéma simplifié fonctionne sur une structure en couches (application, transport, réseau, liaison de données, physique) qui permet de gérer sa complexité. Chaque couche remplit une fonction spécifique, et les couches communiquent entre elles en respectant des règles appelées protocoles. Cette organisation est complémentaire aux architectures réseau qui définissent l'interaction entre les appareils (comme le modèle client-serveur ou poste à poste).

Les couches d'architecture réseau de l'internet sont généralement décrites par deux modèles : le modèle OSI[13] qui est un modèle conceptuel à sept couches, et le modèle TCP/IP[14] modèle opérationnel à quatre couches, qui détaillent les fonctions nécessaires à la communication des données sur un réseau.

Le modèle TCP/IP est le plus couramment utilisé, ses couches sont les suivantes :

1. Couche application : elle est au sommet de la pile et gère les applications que l'utilisateur final utilise (ex: web, email, etc.). Protocoles utilisés : http, Ftp, SMTP, DNS (nom de domaine)

2. Couche transport : assure la fiabilité de la connexion entre les applications, par exemple via le protocole TCP qui contrôle le flux des données et garantit une arrivée en bonne ordre, ou UDP, pour une transmission plus rapide, mais moins fiable, sans connexion.

3. Couche réseau : responsable de l'acheminement des paquets sur l'ensemble du réseau mondial, en utilisant des adresses IP pour identifier chaque appareil.

4. Couche physique : s'occupe de la transmission brute des bits (données de bas) sur le support physique (câbles, ondes radio, etc.).

B - LA CYBER-INVESTIGATION

Ne seront évoqués dans les développements suivants que les investigations menées dans le cyber-espace et auprès de ses opérateurs. Celles consistant à saisir le matériel d'une personne physique et à l'exploiter après copie, sont d'une nature très différente.

13 Open System Interconnection : cadre conceptuel qui divise la communication réseau en sept couches, chacune ayant des fonctions spécifiques.
14 Transmission Control Protocol/Internet Protocol

a - Observations générales

La première question que se pose toute autorité en charge de la constatation des cyber-infractions est de savoir si les éléments matériels portés à sa connaissance sont ou non constitutifs d'une infraction. Il appartiendra ensuite à l'enquêteur, en lien avec l'autorité judiciaire, d'essayer d'en identifier l'auteur.

Cette identification peut être relativement aisée lorsqu'il s'agit de faits d'extorsion ou d'escroquerie commis par un individu solitaire, beaucoup plus complexe sinon parfois impossible, lorsqu'il s'agit d'atteintes aux STAD perpétrées par un groupe criminel organisé.

La démarche d'enquête va dans tous les cas consister à identifier les matériels à partir desquels l'atteinte a été commise (ordinateurs, serveurs, réseaux, appareils mobiles), les types de données qui ont été volées ou contaminées (emails, fichiers, logs système) et les personnes impliquées.

En matière d'atteinte au STAD, l'infraction est impossible à constater tant que ses effets demeurent cachés ; une intrusion peut avoir été réalisée, mais tant que son auteur n'a pas décidé du moment de l'attaque, celle-ci reste occulte. Le blocage du STAD, du site web, une demande de rançon, l'utilisation de données volées révèlent l'atteinte dont il reste encore à trouver le *modus operandi*, ce qui relève tout autant du domaine de compétence des services de cyber sécurité que de celui des services d'enquête pénale.

En matière d'atteinte facilitée par les STAD, la ou les victimes visées sont identifiées et la nature de l'infraction connue dès lors que révélée : extorsion, chantage, escroquerie, etc. Reste à en trouver l'auteur qui peut avoir accéder au réseau internet à partir de n'importe quelle localisation.

Dans tous les cas, faire le lien entre une infraction constatée et son auteur, suppose de la part des services d'investigation d'identifier ce dernier ce qui va consister à recueillir les données relatives au trafic de son compte et au contenu des données transportées.

Classiquement, la préoccupation des services d'enquête est de recueillir, conserver, transmettre la preuve de l'infraction. Pour dévoiler les auteurs d'une infraction commise dans l'univers physique et conduire à son arrestation, ces services disposent de la perquisition, la saisie, des produits ou des instruments du crime, de moyens de surveillance tels les écoutes téléphoniques, la géolocalisation, etc.

Ces méthodes d'investigation classiques peuvent se déployer dans le cyber-espace virtuel qui se singularise par son caractère a-territorial, dématérialisé et la nature volatile des données. Ces caractéristiques ont rendu nécessaires les adaptations procédurales contenues dans les conventions internationales et reprises par les lois nationales, qui transposent les notions procédurales classiques au cyber-espace[15].

La collecte et la gestion de la preuve numérique se heurtent à certaines difficultés :

- Les données nécessaires à l'enquête pénale peuvent être stockées dans des juridictions multiples, changeantes ou inconnues (« le nuage ») ;
- Ces données sont fragiles et fugaces : elles peuvent être effacées ou modifiées rapidement, d'où la nécessité d'interventions rapides et la mise en pratique de procédures de stockage et conservation des données ;
- L'anonymat des utilisateurs d'internet : utilisation d'avatars, partage d'IP dans les cybercafés, utilisation de Proxy ou VPN, rend difficile l'imputation pénale ;
- La preuve doit être admissible par la juridiction.

15 Voir supra II.A.ii

Le tableau ci-après résume les deux catégories basiques de preuve électronique dont l'obtention est généralement recherchée :

Preuves électroniques stockées	
Informations sur le souscripteur	Nom du souscripteur, durée d'utilisation du service, adresse (IP)
Données de trafic	« Metadata » : données relatives aux connections, adresse IP, journal d'accès, services fournis
Données de contenu	Texte des messages blog, vidéo, images…
Preuves électroniques de flux (interception de communications)	
Données de trafic	Qui est contacté et depuis quelle adresse
Données de contenu	Interception du contenu des messages, blogs, vidéos, images, sons, conservés sous format digital

Sont considérées comme données de base d'un utilisateur ;

- Le compte ou le nom d'utilisateur (abonné).
- Le nom et l'adresse postale de l'utilisateur.
- Le ou les numéros de téléphone de l'utilisateur.
- L'adresse électronique de l'utilisateur.
- La date et l'heure de la première inscription, le type d'inscription, une copie du contrat, les moyens de vérification de l'identité au moment de l'inscription, ainsi que les copies des documents fournis par l'utilisateur.
- Toute autre information pertinente relative à l'identité de l'utilisateur ou du titulaire de l'abonnement.
- Le type de service, y compris l'identifiant (numéro de téléphone, adresse IP, numéro de carte SIM, adresse MAC) et l'appareil ou les appareils associés.
- Les informations de profil (nom d'utilisateur).
- Les données relatives à la validation de l'utilisation du service, telles qu'une adresse électronique secondaire fournie par l'utilisateur ou le titulaire de l'abonnement.
- Les informations relatives à la carte de débit ou de crédit (fournies par l'utilisateur à des fins de facturation), y compris d'autres moyens de paiement.
- L'adresse de protocole Internet (IP) utilisée par l'utilisateur pour enregistrer le compte ou pour initier le service.
- Toutes les adresses IP utilisées par l'utilisateur pour se connecter au compte.
- Les heures, dates et durées des sessions.
- Toute autre information relative à l'identité de l'utilisateur, y compris, sans s'y limiter, les informations de facturation (y compris le type et le numéro de carte de crédit, le numéro d'identification d'étudiant ou toute autre information d'identification).

Les données suivantes sont regardées comme de trafic :

- **Pour les fournisseurs de services Internet :**
  - Destination de la connexion ou source de la connexion :
  - Date et heure de la connexion et de la déconnexion.
  - Méthode de connexion au système (par exemple : telnet, ftp, http)
  - Volume de transfert de données (par exemple : en octets).
  - Informations de routage (adresse IP source, adresse(s) IP de destination, numéro(s) de port, navigateur, informations d'en-tête de courriel, identifiant de message).
  - Enregistrements / journaux de connexions IP à des fins d'identification.
  - Informations relatives à toute image ou tout autre document téléchargé sur le compte, y compris les dates et heures de téléchargement ainsi que la taille des fichiers, mais sans inclure le contenu de ces fichiers ;
  - Nom et autres détails d'identification des personnes ayant accédé à une image, un fichier ou une page web spécifique pendant une période donnée ou à une date déterminée.
  - Volume de données.
- **Pour les fournisseurs de services d'hébergement web :**
  - Fichiers journaux (logfiles) ;
  - Tickets (d'assistance, d'incident, etc.) ;
  - Historique des achats ;
  - Historique de rechargement de solde prépayé.

Compte tenu de la plasticité du cyber-espace, le recueil de ces preuves se heurte à des problèmes d'identification, de localisation du cybercriminel.

Les adresses IP ainsi que les numéros d'accès et les informations connexes constituent un point de départ essentiel pour les enquêtes pénales dans lesquelles l'identité d'un suspect n'est pas connue. Ces données sont généralement consignées dans un relevé d'événements, également appelé « journal de serveur », qui indique le début et la fin d'une session d'accès d'un utilisateur à un service. Il s'agit souvent d'une adresse IP individuelle ou d'un autre identifiant qui distingue l'interface réseau utilisée lors de la session d'accès.

Des informations connexes portant sur le début et la fin d'une session d'accès d'un utilisateur à un service, telles que les ports de provenance et l'horodatage, sont souvent nécessaires, étant donné que les adresses IP peuvent être partagées entre plusieurs utilisateurs.

Ces éléments peuvent être demandés au fournisseur de services qui produit les données relatives aux abonnés liées à cet identifiant.

Dans certains cas, il peut s'avérer particulièrement difficile de déterminer si un fournisseur de services agit en qualité de responsable du traitement ou en qualité de sous- traitant, notamment lorsque plusieurs fournisseurs de services sont impliqués dans le traitement des données où lorsque des fournisseurs de services traitent des données pour le compte d'une personne physique.

Les données relatives au trafic peuvent être recherchées et leur divulgation rapide s'avérer nécessaire pour remonter à la source d'une communication et servir de point de départ à la col-

lecte de preuves supplémentaires ou à l'identification d'un suspect. De même, comme de nombreuses formes de criminalité en ligne sont facilitées par des domaines créés ou exploités à des fins criminelles, il est nécessaire d'identifier la personne qui a enregistré un domaine de ce type. De telles informations sont détenues par des entités fournissant des services d'enregistrement de noms de domaine, c'est-à-dire, en général, des registraires et des registres.

Les services basés sur un réseau peuvent être fournis à partir de n'importe quel endroit et ne nécessitent pas d'infrastructure physique, de locaux ou de personnel dans le pays où le service en question est proposé. Par conséquent, les preuves électroniques pertinentes sont souvent stockées en dehors de l'État menant l'enquête ou par un fournisseur de services établi en dehors de cet État, ce qui rend plus difficile l'obtention de preuves électroniques dans les procédures pénales.

Par ailleurs, il arrive souvent que les données ne soient plus stockées ou traitées sur le dispositif d'un utilisateur, mais rendues disponibles sur une infrastructure en nuage permettant d'y accéder à partir de n'importe quel endroit. Pour opérer ces services, les fournisseurs de services n'ont pas besoin d'être établis ou d'avoir des serveurs sur un territoire spécifique.

Les fournisseurs de services d'infrastructure internet liés à l'attribution de noms et de numéros, tels que les registres et les bureaux d'enregistrement de noms de domaine et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, ou les registres internet régionaux pour les adresses de protocole de l'internet (IP), présentent un intérêt particulier lorsqu'il s'agit d'identifier des acteurs cachés derrière des sites internet malveillants ou compromis. Ils détiennent des données qui pourraient permettre l'identification d'une personne ou d'une entité cachée derrière un site internet utilisé dans une activité criminelle.

Il résulte de ce qui précède que la plupart des affaires ne pourront être élucidées sans la mise en œuvre de la Coopération internationale et le recours à des opérateurs privés situées à l'étranger, les plus importants d'entre eux se trouvant aux Etats Unis.

b - Obtenir la preuve numérique d'un opérateur

La preuve numérique d'une infraction est constituée de données d'identification de l'auteur, de trafic, de contenu. Dans le cadre de son investigation, et la matière n'échappe pas à la règle générale, l'enquêteur devra collecter, intercepter, saisir, conserver, et enfin produire les preuves numériques obtenues.

Afin de les obtenir, l'enquêteur, sous l'autorité du magistrat, peut recourir à des enquêtes en source ouverte avant de faire appel aux mécanismes de la coopération internationale.

i -La recherche de preuves numériques sans recours à la coopération judiciaire internationale

Selon les dispositions légales applicables à chaque pays, les enquêteurs peuvent constituer un avatar qui viendra participer au réseau social auquel appartient un cybercriminel. Sous réserve de la prohibition de la provocation, l'avatar peut recueillir des informations utiles à l'enquête.

L'OSINT peut également être utilisé par les services d'enquête qui peuvent effectuer des :

- Recherches par image et par image inversée, qui permet d'identifier l'origine d'une image, trouver des versions similaires ou découvrir où elle a été utilisée en ligne (https://tineye.com/)

- Recherches par IMEI est une méthode puissante pour obtenir des informations spécifiques sur un appareil mobile. L'IMEI est un numéro unique attribué à chaque téléphone mobile et à certains autres appareils connectés (https://www.imei.info/fr/)

- Recherches par relais GSM est une technique utilisée pour identifier la localisation d'un appareil mobile en utilisant les tours de téléphonie mobile auxquelles il se connecte.

- La recherche par e-mail est une technique qui permet d'identifier des informations sur une personne ou une entreprise à partir de leur adresse e-mail. Cette méthode peut révéler des profils sociaux, des affiliations professionnelles, des historiques de connexions, et d'autres informations pertinentes.

- Localisation par Google Map.

Les résultats permettent souvent de remonter jusqu'à l'auteur d'une infraction d'atteinte aux personnes, en particulier celles se trouvant sur le territoire national et ainsi de procéder à son arrestation et sa poursuite.

Mais l'identification des auteurs peut s'avérer plus complexe lorsqu'ils se cachent derrière des protections sophistiquées favorisant son anonymisation : sites web, proxies, VPN ; tel est souvent le cas des criminels s'attaquant aux STAD. Le recours à la Coopération internationale est alors indispensable, mais pas toujours suffisant.

ii - La recherche de preuves numériques en ayant recours à la coopération internationale

Lorsque l'OSINT n'a pas suffisamment permis de collecter les preuves utiles ou qu'elles conduisent à relever des éléments d'extranéité, l'enquêteur devra utiliser les procédures d'entraide.

Il se trouve que nombre de fournisseurs de service et fournisseurs de données sont soumis à la loi des Etats Unis d'Amérique.

Considérant la masse de requêtes, a été élaborée grâce à l'effort collectif de la *communauté des forces de l'ordre*[16], une liste des Fournisseurs d'Accès à Internet (FAI) qui est une base de données regroupant les fournisseurs de services Internet et autres prestataires de contenu en ligne. Pour chaque fournisseur de services Internet répertorié, sont indiquées les coordonnées d'un point de contact ainsi que les instructions nécessaires pour qu'ils répondent aux requêtes qui leur sont adressées par des autorités légitimes, soit directement, soit par l'intermédiaire du point de contact conventionnel.

Le FAI contenant les procédures normalisées se trouve à l'adresse suivante :

https://www.search.org/resources/isp-list/

L'UNODC a pour sa part diffusé des « conseils utiles » pour les enquêteurs et les procureurs dans leurs demandes de données/preuves électroniques/ numériques auprès des juridictions étrangères[17].

LA DEMANDE DE DIVULGATION D'URGENCE (EMERGENCY DISCLOSURE REQUEST)

Il s'agit d'une requête spéciale qui peut être formulée par une autorité légitime dans les situations où la divulgation de données détenues par un fournisseur de services (SP) peut permettre de prévenir une menace **imminente** de mort ou de blessure sérieuse.

Les données ainsi obtenues seront par exemple utilisées pour éviter un attentat terroriste grâce à l'identification de l'endroit d'où un utilisateur d'une application de messagerie envoie ses communications.

16 Selon la mention portée sur le site

17 Voir : www.unodc.org/documents/organized-crime/tools_and_publications/FRENCH_Tip_electronic_evidence_final.pdf

Cette procédure de divulgation d'urgence ne doit pas être confondue avec une demande urgente de preuves électroniques par le biais d'une demande d'assistance judiciaire, qui emprunte d'autres voies de transmission.

Selon la loi américaine, une situation d'urgence est constituée lorsqu'existe danger imminent de mort ou de blessure physique grave pour toute personne (18 Code des États-Unis § 2702 – Divulgation volontaire des communications ou des dossiers des clients, paragraphes (b)(8) et (c)(4)).

Il est important de noter que l'imminence est un critère essentiel pour déterminer s'il s'agit réellement d'une situation d'urgence. Certains cas nécessitent qu'une demande soit exécutée de manière urgente pour différentes raisons : accélérer les enquêtes, éviter de nouveaux crimes, identifier ces auteurs, raccourcir les délais de procédure. Aucune de ces situations ne sera considérée comme une urgence suffisante dès lors qu'il n'existe pas un danger imminent de mort ou de blessure physique grave pour une personne.

Dans la plupart des cas, les fournisseurs de service acceptent d'exécuter les demandes urgentes en cas de danger imminent portant sur les informations basiques du souscripteur et les données de trafic, dès lors que la personne qui soumet la demande peut établir qu'elle est effectivement un fonctionnaire public et qu'elle respecte les règles fixées par le fournisseur de service.

Ces règles sont publiques et accessibles par internet. Il appartient aux forces de sécurité intérieure de s'y référer pour formuler ce type de demande, mais elles valent aussi pour celles formulées par les autorités judiciaires s'agissant de demande d'entraide.

On pourra par exemple consulter les guides suivants :

- Apple : https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf
- Amazon : https://ler.amazon.com/us
- Microsoft : https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data

Il est cependant beaucoup plus difficile d'obtenir des données de contenu, qui ne seront délivrées qu'en fonction de la politique interne du fournisseur, sauf à utiliser l'entraide judiciaire qui pourra certes être transmise, mais elle ne doit pas être confondue avec l'envoi d'une demande de divulgation d'urgence à un fournisseur de service par un agent habilité.

Une demande de divulgation d'urgence doit contenir les éléments suivants :

- La nature de l'urgence (par exemple : menace de suicide, menace d'attentat.)
- L'imminence du décès ou des blessures corporelles graves ; fournir des éléments indiquant qu'il existe une échéance précise avant laquelle il est nécessaire d'obtenir les informations demandées.
- Expliquer/décrire en quoi les informations demandées aideront à prévenir le décès ou les blessures corporelles graves.
- Expliquer pourquoi une demande directe d'identification et/ou de données de trafic est insuffisante pour obtenir les informations recherchées.
- Tous les autres détails ou contextes disponibles concernant les circonstances particulières.
- Identité de la personne en danger de décès ou de blessures corporelles graves.
- Identification des informations spécifiques que l'on croit être en possession du SP, et explication de la manière dont ces informations se rapportent à l'urgence alléguée.

Le site des opérateurs mentionne également les modes d'adressage de la demande.

LA PRÉSERVATION DES PREUVES ÉLECTRONIQUES

Une infraction doit être prouvée et sa preuve en matière de cybercriminalité est électronique. La préservation des preuves électroniques d'une infraction est donc essentielle et doit être faite au plus tôt afin d'éviter leur suppression ou modification.

Matériellement, la préservation correspondra à une « capture instantanée » (snapshot) du compte utilisateur dont la conservation est demandée, au moment où le prestataire de services reçoit et traite la requête.

Dans un premier temps le service d'enquête devra localiser l'endroit où le prestataire de services détient et contrôle les preuves électroniques car la demande doit être adressée à l'endroit où ce dernier exerce le contrôle sur les données. Dans la pratique, il conviendra là encore de se référer aux directives à l'intention des autorités chargées de l'application de la loi publiées par le fournisseur de service (lorsqu'elles sont disponibles) afin de confirmer l'adresse ou le service compétent pour l'envoi de la demande de préservation.

Il conviendra également de vérifier si les preuves électroniques sont encore conservées par le fournisseur de services soit en consultant ses directives soit par l'intermédiaire des canaux de coopération policière. Le fournisseur ne préservera que les données effectivement présentes dans le compte au moment de la demande de préservation, et n'effectuera pas de vérification pour confirmer si le compte contient des données.

En outre, en raison de la nature du service fourni à leurs utilisateurs, certains SP ne conservent qu'un volume limité de données pendant une courte période. Ainsi, par exemple, la durée de conservation des données de contenu est de trente jours chez Snapchat et WhatsApp ne conserve pas les messages lus. Certains fournisseurs ne conservent les messages détruits que quarante-huit heures.

Devra également être prise en considération par le demandeur la nature de l'infraction poursuivie puisque peut lui être opposé le principe de double incrimination ou une règle de *minimis*[18].

La transmission de la demande de préservation au fournisseur de service, lorsque celui accepte de les traiter directement sans passer par la procédure d'entraide judiciaire, pourra être faite par le réseau 24/7 de la Convention de Budapest ou le i24/7 réseau d'Interpol. La majorité des fournisseurs de service Nord-américain accepte ce mode de transmission.

Cette demande doit comporter au moins les éléments suivants :

- La nature des infractions poursuivies,
- La désignation du compte/site qui doit être préservé,
- La demande de ne pas révéler la procédure à l'abonné ou au titulaire du site,
- Identification du service d'enquête ou du procureur requérant,
- Un engagement de produire une demande d'entraide.

Les fournisseurs de service conservent les données préservées en général pendant une durée de quatre-vingt-dix jours renouvelables sur demande écrite. Passé ce délai, les preuves sont détruites.

En toute hypothèse, une demande d'entraide judiciaire classique doit être envoyée en parallèle.

18 Pas d'action si les peines encourues sont inférieures à un certain montant.

CONCLUSION

Les investigations en matière de cybercriminalité sont complexes et demandent souvent la coopération des fournisseurs de services ou même d'infrastructures.

Elles demandent une technicité qui n'est qu'à la portée de certains services dont la spécialisation est une condition sine qua non de leur réussite.

QUESTIONS

- Connaissez-vous les services en charge de la lutte contre la cyber criminalité opérant dans votre pays ?
- Avez-vous déjà eu des contacts avec eux ?
- Savez-vous s'ils ont un numéro d'urgence ?
- Savez-vous s'il existe une juridiction spécialisée contre ce type de crime ?
- Dans l'affirmative, connaissez-vous les règles de dessaisissement ?

MODULE 4. LA POURSUITE DES CYBER-INFRACTIONS

Au cours de la phase d'investigation, les autorités judiciaires sont appelées à intervenir régulièrement au soutien des investigateurs. Il en effet été indiqué que les demandes formées par les services d'enquête dans le cadre des procédures d'urgence, de préservation et de conservation des preuves électroniques doivent en général être complétées par des demandes d'entraide judiciaire dont quelques règles seront rappelées dans un premier temps.

Une fois les éléments constitutifs de l'infraction réunis, et celle-ci imputée, pourra commencer la phase contentieuse dans laquelle l'autorité de poursuite devra être attentive aux spécificités de la cybercriminalité.

I. LA PHASE PRÉ-CONTENTIEUSE : UTILISATION DE L'ENTRAIDE JUDICIAIRE

Par phase pré-contentieuse, on entendra celle qui précède le renvoi de la personne impliquée. Elle se marque par une indispensable collaboration entre l'autorité judiciaire et les services d'enquête et par l'utilisation par les premières de l'entraide judiciaire, conformément aux conventions applicables et aux guides publiés par les Etats requis.

Outre les cas dans lesquels, comme il a été mentionné *supra*, la demande directe adressée par les services d'enquête s'accompagne de l'engagement de l'émission d'une demande d'entraide judiciaire, cette procédure est indispensable lorsque :

- Les preuves ne sont pas accessibles par des recherches en sources ouvertes.
- Les fournisseurs de services (SP) ne répondent pas à une demande directe de données de trafic ou d'information de base sur un abonné formé par les services d'enquête.
- Des données de contenu sont requises.
- Les données ne peuvent pas être préservées et doivent être obtenues rapidement pour éviter leur suppression.
- Les preuves électroniques obtenues par divulgation volontaire sont insuffisantes pour satisfaire aux exigences de l'État requérant en matière d'admissibilité des preuves électroniques.

A - LA DEMANDE D'ENTRAIDE JUDICIAIRE AFIN D'OBTENTION DE PREUVES ÉLECTRONIQUES

Une demande d'entraide est un document qui doit être aisément compréhensible et d'exécution aisée par l'Etat requis ; elle doit comporter tous les éléments permettant de décider si elle est exécutable et comment elle peut l'être.

a - Les bases légales de la demande

Les traités servent de base légale à la coopération judiciaire ; certains, propres à la lutte contre la cybercriminalité, ont été évoqués supra.

Dans l'hypothèse où ils ne trouveraient pas à s'appliquer faute d'avoir été signée par un des Etats, la demande peut également se référer à une éventuelle convention bilatérale ou à des conventions universelles telle la Convention des Nations Unies contre la criminalité organisée dont l'article 18 inclut dans les actes pouvant faire l'objet d'une demande le fait de « saisir des preuves… procéder à des perquisitions et saisies » ou tout autre mesure d'assistance ne violant pas la loi du pays requis. Les preuves numériques entrent bien dans ce champ, dès lors que l'infraction est le fait d'un groupe organisé.

S'agissant d'une demande en lien avec des faits de terrorisme, les Résolutions (2001), 2178 (2014) and 2322 (2016), 2396 (2017) de l'Assemblée générale des Nations Unies énoncent que les Etats doivent s'apporter la meilleure entraide possible.

Doivent également être mentionnés dans la demande les textes nationaux d'incrimination et de répression. Cette mention répond à la fois à la question de l'existence d'une base légale nationale à la demande, et permet à l'Etat requis d'évaluer la question de la double incrimination, comme celle *du minimis.*

b - Le résumé des faits et l'objet de la demande

Un simple résumé des faits est requis, mais il faut garder en mémoire que la demande d'entraide judiciaire est un document autonome : l'État requis ne disposera d'aucune autre information sur l'affaire.

Les faits présentés doivent permettre : d'identifier les preuves demandées, d'expliquer pourquoi elles sont nécessaires à l'autorité requérante, de répondre aux exigences légales de l'Etat requis.

Idéalement, ce résumé doit établir une apparence de preuve suffisante *(prima facie)* que chaque personne nommée a commis l'infraction ou, si les suspects ne sont pas encore identifiés, qu'une infraction a bien été commise.

En pratique, la demande d'entraide doit contenir des informations justificatives suffisantes pour convaincre et permettre aux autorités de l'État requis de contraindre légalement le fournisseur de services (SP) à fournir les preuves électroniques demandées.

Dans cette perspective, il est préférable que le rédacteur de la demande ait examiné les normes juridiques de l'État requis afin de déterminer quelles informations de soutien doivent y figurer. Il peut pour cela se rapprocher de l'ambassade du pays requis ; pour ce qui concerne les Etats-Unis, ils ont toujours un agent du FBI en mesure de donner ces informations.

Ces informations peuvent également être recherchées par consultation de site comme celui d'organisations internationales comme par exemple :

https://sherloc.unodc.org/cld/en/st/home.html

ou bien https://rm.coe.int/-4-3-1-3148cyberleg-global-state-jan-2023-public-v1680/1a99137

(CoE : L'état global des législations contre la cybercriminalité)

c - Spécificités de certains types de demandes d'entraide

Les développements ci-après constituent un guide de bonne pratique de l'émission d'une demande d'entraide.

i - Demande de données de base d'un souscripteur

Lorsque concernant un fournisseur de service relevant de la loi des Etats-Unis, la demande de donnée de base doit justifier que les éléments recherchés sont pertinents, liés à une investigation criminelle, Il ne suffit pas d'affirmer que le suspect a un compte email ; ce dernier doit avoir un lien avec l'infraction en cours d'investigation.

ii - Demande de données de trafic

L'obtention des données de trafic, est subordonnée à l'exposé de fait précis décrivant en quoi les relevés ou autres informations demandés sont pertinents et utiles à l'enquête pénale.

En effet, la loi américaine exige que les procureurs présentent au tribunal un résumé factuel de l'enquête et expliquent de quelle manière les documents demandés feront progresser cette enquête. Il s'agit d'une exigence intermédiaire, plus élevée que la simple pertinence, mais moins stricte que la norme de « probable cause » requise pour le contenu.

iii - Demande de données de contenu

Chaque appareil ou chaque compte pour lequel des données de contenu sont demandées est considéré comme un lieu distinct, au même titre qu'un domicile. Cela signifie que les éléments justificatifs figurant dans la demande d'entraide doivent être présentés compte par compte ou appareil par appareil, et qu'un raisonnement motivé doit être fourni pour chacun, conformément à la norme juridique applicable.

La demande d'entraide doit exposer des faits précis établissant que les éléments de preuve recherchés (le contenu) seront trouvés parmi les enregistrements du fournisseur de services (SP) et que ces éléments sont liés à une infraction pénale. Il s'agit du seuil de « probable cause » (motif raisonnable de poursuite), identique à celui exigé pour la perquisition d'un domicile ou d'un local professionnel aux États-Unis.

Doivent donc être décrits en détail :

- Le type de données de contenu à saisir (par exemple, une communication électronique ou un courriel) ;
- La raison pour laquelle ces données de contenu sont liées à l'infraction pénale faisant l'objet de l'enquête ;
- Inclure uniquement les faits relatifs à la preuve recherchée, en veillant à indiquer la source de chaque information incluse dans la demande.
- Attribution du compte au suspect en utilisant les éléments déjà disponibles dans le dossier, par exemple : témoignage attestant que le suspect utilise ce compte Gmail ou bien il résulte d'une demande directe adressée à Facebook pour obtenir les données d'abonné montre que le suspect a ouvert ce compte Facebook avec l'adresse électronique dont le contenu est demandé.
- Lien entre le suspect et le crime.

L'ensemble de ces éléments doit conduire l'autorité judiciaire requise, à constater l'existence d'une « probable cause » selon ses propres standards. Il faut donc démontrer qu'il y a des suspicions raisonnables de croire que le suspect ou l'accusé a commis l'infraction et que les données dont la production est sollicitée ont été utilisées pour la commettre.

iv - La forme de la preuve

Si une forme particulière de preuve est requise, il est recommandé d'inclure ces informations sous la rubrique « Assistance sollicitée et forme des preuves », car il s'agit souvent de la première étape de l'examen mené par l'Autorité centrale du pays requis, certaines exigences peuvent être négligées si elles ne sont pas précisées initialement.

Si des formes alternatives de présentation des preuves électroniques peuvent être acceptables pour l'État requérant — par exemple, lorsque plusieurs formats sont capables de satisfaire aux exigences d'admissibilité — ces formes alternatives acceptables peuvent être communiquées à l'État requis, accompagnées d'une indication précisant laquelle de ces formes de preuve est la plus souhaitable.

Dans certains accords internationaux d'entraide judiciaire (MLA), il est prévu que l'Autorité compétente d'exécution doive exécuter la demande selon la forme demandée, dans la mesure où cela n'est pas contraire à la législation de l'État requis.

II. LA PHASE CONTENTIEUSE

A - RÈGLES DE PRODUCTION DES PREUVES

Après la phase de recueil va s'ouvrir la phase d'analyse des preuves qui est celle où l'enquêteur explore les éléments collectés pour trouver des indices, reconstituer les évènements. Il s'agit d'analyser les journaux, rechercher les données cachées ou chiffrées, à l'aide d'outils d'analyse spécifiques. En lien avec l'autorité judiciaire, l'enquêteur va évaluer les preuves recueillies pour déterminer leur pertinence et leur fiabilité. Il est normalement procédé à une reconstitution de l'histoire de l'incident à partir des traces numériques trouvées.

C'est à la fin de cette phase que l'autorité de poursuite qui a accompagné l'enquête dans ses différentes phases, intervenant pour rendre les actes nécessaires, va décider ou non du renvoi de l'auteur présumé devant la juridiction à qui seront adressées les preuves réunies.

Dans l'hypothèse où l'enquête a conduit à la saisie du matériel de l'auteur, il est procédé par les enquêteurs à une copie du disque dur.

Dans tous les cas, la preuve numérique va être constituée par des données numériques conservées sur un support qui sera produit devant la juridiction et dont des images pourront lui être présentées (« copies écran »). Le recueil de preuve numérique obéissant aux mêmes règles que tous les autres modes de preuve quant à son admissibilité devant la juridiction, l'autorité de poursuite devra donc être particulièrement attentive à la :

- Traçabilité : la preuve doit être authentifiable et son origine vérifiable. Toute la chaîne de transmission, depuis le fournisseur de service jusqu'au dossier de renvoi doit être connue et reconstituable.
- Intégrité : la donnée produite ne doit pas être modifiée lors de la collecte ou de l'analyse.
- Légalité : elle doit être recueillie loyalement selon la procédure en vigueur, dans le respect des dispositifs de protection des données individuelles.
- Chaîne de transmission et de conservation qui doit être documentée.

B - LA QUESTION DE LA COMPÉTENCE ET DE L'IMPUTABILITÉ

a - La compétence

La première question que doit se poser l'autorité de poursuite est celle de la compétence de ses juridictions.

Le droit pénal classique a été conçu pour des infractions matérielles, territorialisées, ce que ne sont pas les cyber-infractions. Quelle juridiction est en effet compétente si le serveur est aux Etats-Unis, la victime en Europe et l'auteur en Afrique ?

L'article 22 de la Convention de Budapest règle la question dans le sens suivant :

« Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

a) sur son territoire ; ou

b) à bord d'un navire battant pavillon de cette Partie ; ou

c) à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou

d) par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat. »

Certains Etat ont également rajouté à ces principes, celui d'une compétence liée à la localisation de la victime de l'infraction, ce qui leur confère la capacité quasi systématique de poursuivre les auteurs, dès lors qu'il s'agit de protéger leurs résidents. Cette possibilité est autorisée par le §4 du même article qui se lit : « La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. »

Il n'en reste pas moins que dès lors que l'auteur se trouvera à l'étranger, il y aura un risque de conflit de compétence qui ne pourra être résolu, surtout si le pays dont il a la nationalité n'extrade pas ses nationaux, que par un transfert de procédure/dénonciation officielle faite par le pays de résidence de la victime vers le pays de nationalité de l'auteur.

Le §5 a anticipé cette situation en disposant que : « Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites. »

Cette situation est de fait très courante, les autorités du pays de résidence de l'auteur étant souvent sollicitées préalablement dans le cadre de demandes d'entraide aux fins de localisation du mis en cause, de son audition, de saisie des avoirs des auteurs présumés et donc informées du conflit potentiel.

b - La question de l'imputabilité

La presse se fait l'écho fréquemment d'intrusion dans des systèmes réputés protégés, à l'aide de malwares qui ont pénétré dans des failles informatiques ou ont été apportés par des opérateurs négligents internes à l'entité attaquée.

Il faut donc normalement imputer l'infraction révélée à une personne physique ou morale, qui sera renvoyée devant les juridictions de jugement.

Au long des conventions de lutte contre la cybercriminalité, il est répété que la responsabilité pénale des personnes physiques ne peut être engagée que si l'infraction a été commise intentionnellement[19] ce qui d'ailleurs est un principe de base du droit pénal. Il en est de même de la responsabilité des personnes morales puisse également l'être[20]. Cette restriction a pour effet d'épargner les fournisseurs de service d'accès, d'infrastructure, de se voir mis en cause, sauf à ce que soit démontrée leur participation volontaire.

Ont été évoqués dans le module relatif aux investigations, les subterfuges utilisés par les cybercriminels pour dissimuler leur identité, le plus simple consistant à utiliser une session dans un cybercafé sur un ordinateur à temps d'utilisation partagé. Ceux-là sont souvent identifiables par l'utilisation de moyens tels que l'OSINT.

Il en est de beaucoup plus complexes qui utilisent plusieurs couches de protection successives comme des sites web complices, des techniques d'anonymisation comme les proxies ou se cachent dans le cloud et rendent extrêmement difficile leur identification.

La meilleure défense contre ces criminels dont l'identité personnelle est difficile à démasquer, ce d'autant qu'ils peuvent appartenir à des entités étatiques, est sans doute une attention forte au respect des règles de cyber-sécurité des STAD.

CONCLUSION

En 2016, le Groupe du Conseil de l'Europe sur la recherche de preuves dans le « cloud » observait, entre autres points, que « la cybercriminalité, le nombre de terminaux, de services et d'utilisateurs (notamment de terminaux et services mobiles) et, partant, le nombre de victimes ont atteint des proportions telles que seule une infime partie de la cybercriminalité ou autres infractions impliquant des preuves électroniques sera jamais enregistrée et donnera jamais lieu à des enquêtes. L'immense majorité des victimes ne peut pas s'attendre à ce que justice soit rendue »

Les principales difficultés mises en évidence par le groupe concernaient « l'identification des auteurs sur le cloud, la territorialité et la compétence » des juridictions et, de ce fait, la difficulté d'obtention d'un accès efficace aux preuves électroniques et à leur divulgation.

De fait, submergée par la masse des contentieux, la technicité des enquêtes, l'institution judiciaire est davantage observatrice que partie prenante à la course de vitesse engagée entre cyber-criminels et agences de sécurité.

Reste qu'il lui appartient d'utiliser au mieux les moyens qui lui sont donnés.

19 cf. i.e. art.29 Co. de Malabo.
20 cf. i.e. article 12 Co. de Budapest, art. 30 Co de Malabo.

LISTE DES ANNEXES :

- Annexe 1 : Glossaire des termes juridiques et techniques
- Annexe 2 : Le dispositif mauritanien de lutte contre la cybercriminalité
- Annexe 3 : Annexes du RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale
- CERTIFICAT D'INJONCTION EUROPÉENNE DE PRODUCTION (EPOC) CONCERNANT LA PRODUCTION DE PREUVES ÉLECTRONIQUES
- CERTIFICAT D'INJONCTION EUROPÉENNE DE CONSERVATION (EPOC-PR) CONCERNANT LA CONSERVATION DE PREUVES ÉLECTRONIQUES
- Annexe 4 : Cas pratique : exercice AP2 et sa solution
- Annexe 5 : Exercice sur le cadre conventionnel et sa solution

ANNEXE 1. GLOSSAIRE

I. DÉFINITIONS LÉGALES

A -TERMINOLOGIE UTILISÉE DANS LES CONVENTIONS INTERNATIONALES

a - « Système informatique »

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ, DITE CONVENTION DE BUDAPEST

Article 1 : définitions

- « l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;
- l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SECURITÉ ET LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL (dite convention de Malabo) :

- « Système informatique : Tout dispositif électronique, magnétique, optique, électrochimique ou tout autre dispositif de haut débit isolé ou interconnecté qui performe la fonction de stockage de données ou l'installation de communications. Ces communications sont directement liées à ou fonctionnent en association avec d'autre(s) dispositif(s) ».

DIRECTIVE 2013/40/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 12 AOÛT 2013 relative aux attaques contre les systèmes d'information

Article 2. a) «système d'information » : un dispositif isolé ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

b - Fournisseur de services

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ

Art. 1. « l'expression « fournisseur de services » désigne:

i) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii) toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SECURITÉ

- L'expression « fournisseur de services » désigne toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

Pour information : RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 12 JUILLET 2023

Article 3 : « fournisseur de services » : toute personne physique ou morale qui fournit une ou plusieurs des catégories de services suivantes, à l'exception des services financiers [.] :

a) des services de communications électroniques tels qu'ils sont définis à l'article 2, point 4), de la directive (UE) 2018/1972 ;

b) des services d'attribution de noms de domaine sur l'internet et de numérotation IP, tels que l'attribution d'adresses IP, les services du registre de noms de domaine, les services du bureau d'enregistrement de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire liés aux noms de domaine ;

c) d'autres services de la société de l'information visés à l'article 1er , paragraphe 1, point b), de la directive (UE) 2015/1535 qui :

i) permettent à leurs utilisateurs de communiquer entre eux ; ou

ii) permettent de stocker ou de traiter d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni, à condition que le stockage des données soit une composante déterminante du service fourni à l'utilisateur .

c - Données relatives au trafic

CONVENTION DU CONSEIL DE L'EUROPE SUR LA CYBERCRIMINALITÉ

Art.1 d. « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

CONVENTION DE L'UNION AFRICAINE SUR LA CYBER SECURITÉ

- L'expression « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent. »

RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 12 JUILLET 2023

Art. 3. 11) « données relatives au trafic »: les données relatives à la fourniture d'un service proposé par un fournisseur de services qui servent à fournir des informations contextuelles ou supplémentaires sur ce service et qui sont générées ou traitées par un système d'information du fournisseur de services, tels que la source et la destination d'un message ou un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service.

II. DÉFINITIONS TECHNIQUES

BPH (bulletproof hosting)

C'est un service d'hébergement web conçu pour protéger les activités illégales contre les interventions des autorités.

Les hébergeurs acceptent ou ignorent les activités interdites comme le phishing, les malwares, les spams, ou la vente de données volées. Ils sont souvent situés dans des pays où les lois sont sinon laxistes à tout le moins peu appliquées en matière de cybercriminalité.

Ils offrent des services qui masquent l'identité de leurs clients, comme le paiement en cryptomonnaie ou l'absence de vérification d'identité et ne coopèrent pas avec les autorités ou les fournisseurs de cybersécurité pour retirer les contenus malveillants.

Ce type d'hébergement est un pilier de l'infrastructure criminelle sur le web.

Un exemple célèbre de BPH est CyberBunker, un fournisseur basé dans un ancien bunker militaire aux Pays-Bas, connu pour héberger des contenus illégaux tout en résistant aux pressions des autorités.

BOTNET

Un botnet (abréviation de « robot network ») est constitué d'ordinateurs qui communiquent entre eux via Internet. Un centre de commande et de contrôle les utilise pour envoyer du spam, lancer des attaques par déni de service distribué (DDoS) et commettre d'autres infractions.

Dark Web

Le dark web est une partie d'Internet non accessible par les moteurs de recherche classiques

(comme Google, Bing ou Yahoo) et non accessible via les navigateurs ordinaires (comme Chrome, Firefox ou Safari, sauf s'ils sont configurés spécialement).

Le dark web est accessible via des navigateurs spécialisés, le plus connu étant Tor (The Onion Router). Les sites ont des adresses se terminant en ".onion" et la connexion passe par plusieurs couches de chiffrement pour protéger l'anonymat des utilisateurs.

DROPPER

Un dropper, aussi appelé *programme injecteur,* est un outil utilisé par les cybercriminels pour introduire discrètement des logiciels malveillants sur un appareil.

Il ne cause pas nécessairement de dommages lui-même, mais sert de vecteur pour des menaces plus graves comme des ransomwares, chevaux de Troie, ou logiciels espions.

Le dropper est souvent la première étape d'une intrusion. Il est conçu pour passer inaperçu et déposer la charge utile (le malware principal) sur le système. Il peut même supprimer sa propre trace pour éviter la détection. Il s'infiltre par :

- Hameçonnage
- Sites web infectés
- Fichiers joints dans des emails
- Exploitation de failles logicielles

Hébergeur

C'est une entreprise ou un service qui met à disposition des serveurs pour stocker et rendre accessibles des sites web, des applications, des fichiers ou des bases de données sur Internet.

L'hébergeur permet à un site ou une application d'être accessible 24h/24 depuis n'importe où dans le monde. Il s'occupe de :

- Stocker les fichiers du site (images, textes, code…)
- Gérer les bases de données
- Fournir une adresse IP ou un nom de domaine
- Assurer un gros débit internet
- Assurer la sécurité, la maintenance et la disponibilité du serveur

Les types d'hébergement

Type d'hébergement	Description
Hébergement mutualisé	Plusieurs sites partagent le même serveur
Serveur dédié	Un serveur entier réservé à un seul client
VPS (Virtual Private Server)	Serveur virtuel avec ressources dédiées (flexible)
Cloud hosting	Hébergement réparti sur plusieurs serveurs (scalable)
Hébergement WordPress	Optimisé pour les sites WordPress
Exemples d'hébergeurs connus en Afrique	TPE, HOSTAFRIQUE, NettaCompany, 101Gén, 20je…[1]

1 Top 10 des meilleurs hébergeurs web en Côte d›Ivoire (2025)

IP

Une adresse IP (Internet Protocol) est un identifiant numérique unique attribué à chaque appareil connecté à un réseau informatique, comme Internet. Elle permet d'identifier, localiser et de communiquer avec cet appareil sur le réseau.

Infostealer

Logiciel malveillant conçu pour voler automatiquement des informations sur un appareil infecté.

Malvertising

Publicité infectée redirigeant vers un site malveillant.

OpSec

Les manuels de sécurité opérationnelle **(OpSec)**, sont des guides qui expliquent comment protéger les informations sensibles contre les risques d'espionnage, de fuite ou d'exploitation malveillante. Le terme OpSec vient de l'anglais Operational Security, utilisé à l'origine dans les milieux militaires, mais aujourd'hui largement adopté en cybersécurité et dans les environnements professionnels.

OSINT

OSINT (Open Source Intelligence) signifie «Renseignement d'Origine Sources Ouvertes». Il s'agit de la collecte, l'analyse et l'exploitation d'informations accessibles au public dans le but d'en tirer des renseignements utiles.

Phishing

Le phishing, ou hameçonnage, est une technique de cybercriminalité qui consiste à tromper des personnes pour leur faire révéler des informations personnelles et bancaires sensibles en se faisant passer pour un tiers de confiance, comme une banque, une administration ou une entreprise, via des courriels, SMS ou appels frauduleux. L'objectif est d'usurper une identité afin de réaliser des escroqueries.

Proxy

C'est un intermédiaire entre un appareil client (ordinateur, smartphone, etc.) et Internet. Il agit comme un relais pour les requêtes web. L'utilisateur ne communique donc pas directement avec le site web, c'est le proxy qui le fait pour lui.

Le proxy offre :

- L'anonymat : masque l'adresse IP réelle, protège l'identité en ligne.
- Contournement de restrictions : permet d'accéder à des contenus bloqués dans certains pays ou réseaux (comme les réseaux d'entreprise ou scolaires).
- Filtrage et contrôle : permet de surveiller ou limiter l'accès à certains sites.
- Amélioration des performances : certains proxies stockent des copies de sites (cache) pour accélérer l'accès.

Il y a différents types de proxies, un VPN est un proxy sécurisé qui chiffre tous les types de trafic.

Serveur

C'est un ordinateur ou un programme informatique qui fournit des services à d'autres ordinateurs, appelés clients, sur un réseau. Un serveur attend des requêtes de clients, puis y répond en fournissant des données ou en exécutant des actions. Par exemple :

- Un serveur web héberge des sites Internet et envoie les pages aux navigateurs.
- Un serveur de messagerie gère l'envoi et la réception des emails.
- Un serveur de fichiers permet de stocker et partager des documents.

Types de serveur	Rôle principal
Serveur web	Fournit des pages web via HTTP/HTTPS
Serveur de base de données	Stocke et gère des données structurées
Serveur FTP	Permet le transfert de fichiers
Serveur DNS	Traduit les noms de domaine en adresses IP
Serveur de jeu	Héberge des parties multijoueurs en ligne
Serveur proxy	Sert d'intermédiaire entre client et Internet

Caractéristiques :

- Toujours actif : il doit être disponible en permanence.
- Puissant : souvent plus robuste qu'un ordinateur classique.
- Sécurisé : protégé contre les intrusions et les pannes.

SKIMMER

Un skimmer numérique est un outil utilisé par des cybercriminels pour voler discrètement des données bancaires sur des sites web.

Dans un premier temps les pirates insèrent un script dans un site web, souvent un site de commerce en ligne mal sécurisé. Ce script intercepte les informations saisies par les utilisateurs comme les numéros de carte bancaire, et autres données personnelles. Les données volées sont ensuite envoyées à un serveur contrôlé par les cybercriminels qui peuvent ensuite les utiliser ou les revendre.

STAD

Un Système de Traitement Automatisé de Données est un ensemble de moyens matériels et logiciels permettant de stocker, traiter, transmettre ou exploiter des données de manière automatisée.

Un STAD regroupe :

- Des unités de traitement : processeurs, serveurs, ordinateurs.
- Des mémoires : disques durs, SSD, bases de données.

- Des logiciels : systèmes d'exploitation, applications, programmes.
- Des données : informations numériques à traiter.
- Des organes d'entrée/sortie : claviers, écrans, imprimantes, interfaces réseau.
- Des liaisons : câbles, connexions sans fil, protocoles de communication.

Ces éléments interagissent pour produire un résultat déterminé, comme l'affichage d'une page web, le calcul d'un salaire ou la gestion d'un stock.

La notion de STAD est utilisée par certains droits nationaux.

ANNEXE 2. LE DISPOSITIF MAURITANIEN DE LUTTE CONTRE LA CYBERCRIMINALITÉ

DÉFIS ET PERSPECTIVES

Magistrat/MOCTAR HAWYA

Il est apparu que le **législateur national a manifesté un intérêt pour l'organisation de ce domaine à travers la loi d'orientation pour la société de l'information, adoptée le 20/01/2016, relative à la sécurité du cyberespace** et à la protection des données à caractère personnel, connue sous le nom de Convention de Malabo de 2014, signée par notre pays sous le numéro 06/2016.

En concrétisation de cet engagement, la loi n° 07/2016 relative à la cybercriminalité a été promulguée.

La ratification de la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel le 26/02/2015, approuvée par la loi n° 02/2023 en date du 19/01/2023, et entrée en vigueur le 08/06/2023 après le dépôt par notre pays de son instrument de ratification, en tant qu'État ayant permis d'atteindre le quorum requis pour son entrée en vigueur.

La signature de la Convention arabe sur la lutte contre les infractions liées aux technologies de l'information, signée par les ministres arabes de la Justice au Caire le 21/12/2010 et entrée en vigueur depuis le 29/06/2013, mais qui n'a pas encore été ratifiée par notre pays.

La participation active aux réunions du Comité spécial chargé de l'élaboration d'une convention internationale globale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles (Convention des Nations Unies sur la cybercriminalité).

I. DÉFINITION DE LA CYBERCRIMINALITÉ ET SES CATÉGORIES

La législation mauritanienne **n'a pas donné de définition de la cybercriminalité** et n'y a fait allusion, même de manière indirecte, sauf à travers la loi n° 07/2016, dans le cadre d'application définie au premier alinéa de son article 2, qui stipule :

« La présente loi concerne les crimes et délits liés aux technologies de l'information et de la communication… ».

Certains auteurs ont défini cette infraction comme suit :

« Une activité criminelle réalisée au moyen des technologies informatiques, des réseaux électroniques et des systèmes cybernétiques, visant à obtenir, manipuler ou détruire des informations, à nuire à des individus ou à des institutions, ou à porter atteinte aux systèmes cybernétiques. Elle se caractérise par sa rapidité et l'absence de preuves matérielles, ce qui rend difficile son enquête et la poursuite de ses auteurs. »

A - LES CATÉGORIES DE LA CYBERCRIMINALITÉ

On peut dire, de manière générale, que les systèmes informatiques **peuvent constituer soit la cible de la cybercriminalité, soit le moyen de sa commission.** Selon une étude globale préparée par l'**Office des Nations Unies contre la drogue et le crime** en 2013, l**es actes constitutifs de cybercriminalité peuvent être classés en trois catégories :**

1. Les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données ou des systèmes informatiques, tels que l'accès illicite à un système informatique.

2. Les actes liés à l'utilisation de l'ordinateur à des fins d'enrichissement personnel ou financier, ou dans une intention de nuire, tels que la fraude ou la falsification informatique.

3. Les actes liés au contenu informatique, tels que la diffusion de discours de haine ou de discrimination.

B -LA RESPONSABILITÉ PÉNALE DES PERSONNES MORALES

La loi n° 007/2016 a consacré la responsabilité pénale des personnes morales pour les infractions prévues par cette loi, et a déterminé leurs sanctions conformément aux articles 34 et 35, tout en excluant : l'État, les collectivités publiques locales.

L'engagement de la responsabilité pénale des personnes morales, selon cette loi, est subordonné aux conditions suivantes :

1. L'infraction doit être commise pour le compte de la personne morale.

2. L'auteur de l'infraction doit être une personne physique agissant **en qualité de gérant ou de représentant de la personne morale et exerçant une autorité en son sein, qu'il s'agisse** :

a. D'une autorité de décision au nom de la personne morale,

b. D'une autorité de gestion au sein de la personne morale,

c. D'une autorité de contrôle au sein de la personne morale.

Les sanctions applicables aux personnes morales consistent notamment en : la confiscation des biens ou des instruments utilisés pour commettre l'infraction ou issus de celle-ci, la dissolution de la personne morale, la fermeture temporaire ou définitive de l'établissement, l'interdiction

temporaire ou définitive d'exercer certaines activités, ainsi que l'exclusion des marchés publics pour une durée déterminée ou définitive.

II. LES RÈGLES PROCÉDURALES DE LA LOI

A - LES RÈGLES PROCÉDURALES DE LA LOI N° 07/2016 RELATIVE À LA CYBERCRIMINALITÉ

La loi n° 07/2016 relative à la cybercriminalité constitue la loi fondamentale en la matière. Elle contient des règles substantielles et procédurales.

Les règles de procédure qui y sont mentionnées s'articulent autour de trois types principaux de mesures procédurales :

1. Les mesures d'enquête,
2. Les mesures de perquisition, de saisie et de confiscation,
3. Les mesures de notification, de conservation des données, de collecte de preuves, d'expertise et d'appel.

a - Les mesures d'enquête

Selon l'article 42, le procureur de la République ou le juge d'instruction peut ordonner, lorsqu'il existe des indices laissant croire à l'existence d'éléments de preuve stockés dans un système informatique, leur saisie et leur confiscation par tout moyen technique approprié, de même que la saisie et la confiscation du support contenant ces données.

L'article 39 prévoit que si ces données sont stockées dans des serveurs situés à l'étranger, **le ministère public doit recourir aux mécanismes de coopération judiciaire internationale** conformément aux conventions internationales applicables en la matière.

b - La perquisition et la saisie

L'article 43 stipule que si les indices permettent de croire que des données électroniques contiennent des informations utiles à l'enquête et à la poursuite, leur perquisition et leur saisie sont autorisées.

c - L'obligation de signaler les données

L'article 44 impose à tout fournisseur de services nationaux ou à toute personne fournissant des services sur le territoire national de signaler aux autorités compétentes les infractions liées aux services qu'il fournit.

d - La conservation des données

L'article 45 oblige les fournisseurs de services à conserver, **pendant une durée déterminée,** les

données techniques disponibles et à les mettre à disposition des autorités compétentes en cas de besoin.

e - La collecte de preuves électroniques

L'article 46 prévoit que les **officiers de police judiciaire peuvent recourir à tout moyen technique disponible pour collecter les preuves électroniques, à condition de respecter les droits et libertés garantis par la Constitution et les lois en vigueur.**

f - L'appel et l'opposition

Les décisions prises au cours de l'enquête et de l'instruction, en vertu des dispositions de la présente loi ou de toute autre législation en vigueur, peuvent être contestées selon les règles et procédures prévues aux articles 47 et suivants du Code de procédure pénale.

B - LOI N° 014/2021 RELATIVE AUX SERVICES ET MOYENS DE PAIEMENT ÉLECTRONIQUE

Cette loi a été promulguée le 05/07/2021, abrogeant et remplaçant la loi n° 2006/031 du 23/08/2006 relative aux instruments de paiement et au commerce électronique, qui était jusqu'alors la référence dans ce domaine.

L'article 4 de cette loi définit les moyens de paiement comme :

« Tout instrument permettant à une personne de transférer des fonds, quel que soit le support ou le procédé technique utilisé, y compris la monnaie électronique. »

L'article 3 définit quant à lui les services de paiement électronique, en énumérant sept types tout en précisant les services qui en sont exclus.

Le chapitre IV de cette loi est consacré aux sanctions applicables en cas de non-respect de ses dispositions. Ces sanctions sont de deux types :

1. Sanctions administratives : émises par la Banque Centrale conformément aux dispositions de la loi n° 2018/036.

2. Sanctions pénales : prévues par les articles 105, 106 et 107, établissant une liste d'actes criminels, assortis de peines d'emprisonnement et d'amendes.

C - LOI N° 025/2013 RELATIVE AUX COMMUNICATIONS ÉLECTRONIQUES

Cette loi a été promulguée le 15 juillet 2013, puis modifiée et complétée par la loi n° 014/2022. Elle vise à définir le cadre juridique et les procédures nécessaires pour l'établissement et l'exploitation des réseaux et services de communications électroniques.

En vertu de cette loi une Autorité de régulation a été créée. Elle dispose de la personnalité morale de droit public, jouit de l'autonomie financière et de gestion, et est placée sous la tutelle du Premier ministre. Ses attributions sont définies à l'article 6 de la même loi.

Le chapitre XIII intitulé "Dispositions pénales" énumère dans les articles 101 à 104 les actes réprimés par la loi. Ces infractions sont punies de peines d'emprisonnement et d'amendes, ap-

plicables à toute personne ayant commis les actes incriminés.

En outre, des sanctions administratives et financières sont prévues à l'article 82 nouveau, et peuvent être prononcées par l'Autorité de régulation. Elles concernent les opérateurs ou gestionnaires d'infrastructures d'hébergement, en cas de violation des dispositions législatives ou réglementaires applicables à leur activité, conformément à cette loi.

D - LOI N° 022/2018 RELATIVE AUX ÉCHANGES ÉLECTRONIQUES

Cette loi a été promulguée le 12 juin 2018. Son article 2 précise qu'elle s'applique aux services fournis par voie électronique, conduisant à la conclusion de contrats pour l'acquisition de biens, la prestation de services, la fourniture d'informations ou la diffusion de publicités.

La loi stipule que la responsabilité civile ou pénale des prestataires de services exerçant une activité d'opérateur dans le domaine des communications électroniques ne peut être engagée que dans les cas suivants:

- S'ils sont à l'origine de la demande de communication objet du litige
- S'ils ont choisi le destinataire de la transmission
- S'ils ont sélectionné ou modifié les contenus transmis.

L'article 39 précise également que les éditeurs de services de communication au public en ligne sont soumis aux règles relatives à la liberté de la presse telles qu'organisées par l'ordonnance n° 017/2006 et les textes qui l'ont modifiée ainsi que par la loi n° 045/2010 relative à la communication audiovisuelle.

E - LOI N° 020/2017 RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Cette loi a été promulguée le 22 juillet 2017. Son article premier précise qu'elle a pour objectif de protéger la vie privée contre les atteintes pouvant résulter de l'utilisation des technologies de l'information et de la communication, et de fixer les conditions permettant à tout traitement de données à caractère personnel, quel qu'en soit le support, de respecter les droits et libertés fondamentaux des citoyens.

En vertu de cette loi, une Autorité de protection des données personnelles a été créée. Elle possède la personnalité morale de droit public, bénéficie de l'autonomie financière et de gestion, et est placée sous la tutelle du Premier ministre. Ses attributions sont définies à l'article 73 de ladite loi.

La section 3 du chapitre VI est consacrée aux procédures de contrôle ainsi qu'aux sanctions administratives et financières. Ces contrôles sont exercés par les agents de l'Autorité de protection des données personnelles, conformément aux articles 74 à 76.

Les sanctions administratives et financières sont émises par l'Autorité, conformément à l'article 77.

La section 4 est dédiée aux sanctions pénales. Lorsque l'auteur des infractions définies dans cette section est une personne physique, il est soumis aux peines prévues par les articles 84 à 94.

F - LOI N° 023/2018 RELATIVE À LA CRIMINALISATION DE LA DISCRIMINATION

Cette loi a été promulguée le 21 juin 2018 et vise à lutter contre la discrimination et les discours de haine tels que définis respectivement dans ses articles 1er et 2.

Elle considère que **ces deux infractions sont imprescriptibles** et autorise le procureur de la République à engager des poursuites d'office sans attendre une plainte de la victime.

L'article 12 prévoit que les propos écrits ou images à caractère raciste sont punis d'une peine d'emprisonnement de un à trois ans et d'une amende de 100 000 à 300 000 ouguiyas lorsqu'ils sont diffusés par tout moyen de communication de masse y compris Internet même si le site est hébergé à l'étranger, à condition que les contenus soient accessibles en Mauritanie.

L'article 15 dispose que l'incitation à la discrimination est punie d'un mois à un an de prison, si elle est réalisée par écrits imprimés ou non, images ou symboles, affichés, distribués, mis en vente ou exposés au public.

G - LOI N° 015/2020 RELATIVE À LA LUTTE CONTRE LA MANIPULATION DE L'INFORMATION

Cette loi a été promulguée le 23 juillet 2020. Elle vise à prévenir et réprimer les infractions liées à la manipulation de l'information, notamment pendant les périodes électorales, les crises sanitaires ou autres situations d'urgence, quelle qu'en soit la nature.

Elle définit la diffusion de fausses nouvelles comme :

« La publication de fausses informations par tout moyen de communication ou via une plateforme numérique sur Internet. »

Le chapitre II, intitulé « Infractions et sanctions », énumère plusieurs actes criminels, notamment :

- La diffusion de fausses informations ;
- La création d'identités numériques fictives ;
- La publication de fausses nouvelles ;
- La diffusion d'informations fabriquées ou manipulées.

H - LOI N° 015/2020 RELATIVE À LA LUTTE CONTRE LA MANIPULATION DE L'INFORMATION

L'article 11 prévoit des mesures d'urgence pour suspendre la diffusion de fausses informations en période électorale, par le biais de communications publiques via Internet. Cette compétence est confiée au Président de la chambre pénale du tribunal régional compétent.

I - LOI N° 021/2021 RELATIVE À LA PROTECTION DES SYMBOLES NATIONAUX ET À LA CRIMINALISATION DES ATTEINTES À L'AUTORITÉ DE L'ÉTAT ET À LA DIGNITÉ DU CITOYEN

Promulguée le 2 décembre 2021, cette loi vise à criminaliser et sanctionner les actes intentionnels commis à travers les technologies de l'information et de la communication, ainsi que les réseaux sociaux, qui portent atteinte :

- à la dignité de l'État et de ses symboles,
- à la sécurité nationale,
- à la paix sociale,
- à la cohésion nationale,
- à la vie privée,
- et à l'honneur du citoyen.

L'article 7 prévoit que le ministère public peut engager l'action publique d'office, mais peut également agir sur plainte de la personne lésée.

J - LOI N° 011/2024 RELATIVE À L'IDENTIFICATION DES ABONNÉS AUX SERVICES DE COMMUNICATIONS ÉLECTRONIQUES OUVERTES AU PUBLIC ET À L'UTILISATION DE CES SERVICES

Cette loi a été promulguée le 15 février 2024. Elle vise à compléter la réglementation en vigueur, notamment la loi sur les communications électroniques, en encadrant l'identification des abonnés aux services de communications électroniques ouverts au public et l'utilisation de ces services.

La loi définit l'abonné comme toute personne physique ou morale ayant souscrit à une offre de service auprès d'un opérateur de communications électroniques.

L'identification est définie comme la procédure permettant de connaître l'identité de la personne utilisant un service de communication électronique.

Le chapitre V énonce les sanctions applicables en cas de violation des dispositions de cette loi, visant :

1. L'opérateur, s'il ne procède pas à l'identification de ses abonnés ;
2. L'agent de l'opérateur, en cas de manquement délibéré à l'obligation d'identification ;
3. L'abonné, en cas de commission des actes mentionnés aux articles 20 à 23 de la même loi.

K - LOI N° 011/2024 RELATIVE À L'IDENTIFICATION DES ABONNÉS AUX SERVICES DE COMMUNICATIONS ÉLECTRONIQUES OUVERTES AU PUBLIC ET À L'UTILISATION DE CES SERVICES

Les sanctions prévues incluent **des peines d'emprisonnement et des amendes à l'encontre de l'abonné et de l'agent de l'opérateur.**

L'opérateur, quant à lui, **est soumis aux sanctions administratives et financières** prévues à l'article 82 nouveau de la loi n° 025/2013 relative aux communications télectroniques.

III. LA PREUVE ÉLECTRONIQUE

Certains auteurs considèrent que la preuve électronique (ou numérique) appartient à la catégorie des preuves matérielles.

Elle est définie comme suit :

« Un élément numérique permettant de présenter des informations sous différentes formes – écrits, images, sons, figures – en vue d'établir légalement un lien entre le crime, l'auteur et la victime, et pouvant être recevable devant les autorités chargées de l'application de la loi et les juridictions. »

A - LA LÉGALITÉ DE LA PREUVE ÉLECTRONIQUE

L'article 3 de la loi n° 07/2016 précise que les autorités prévues dans cette loi sont compétentes pour :

- Les infractions commises au titre de cette loi ;
- Toute infraction commise via un système informatique ;
- Et pour la collecte de preuves électroniques dans toute autre infraction.

Ce fondement juridique établit la légitimité de la preuve numérique en matière pénale.

B - LA FORCE PROBANTE DE LA PREUVE ÉLECTRONIQUE

Bien que la loi n° 07/2016 ne précise pas directement la valeur probante de la preuve électronique, celle-ci est mentionnée dans plusieurs textes juridiques, notamment :

- La loi n° 2011-03 portant Code de l'état civil ;
- La loi n° 2018-22 relative aux échanges électroniques.

Cette dernière contient un chapitre intitulé "La preuve électronique".

L'article 77 stipule que :" Un écrit sous forme électronique est admis comme preuve au même titre qu'un écrit sur support papier et possède la même force probante. "

Cela confère à la preuve numérique le statut de preuve légale, tel que prévu à l'article 386 du Code de procédure pénale, en tant que moyen d'établir une infraction.

IV. CONCLUSION

Il ressort de ce qui a été présenté que notre pays dispose d'un système législatif couvrant les principaux aspects nécessaires à la lutte contre la cybercriminalité, et ce à la lumière des principes énoncés dans la loi d'orientation relative à la société de l'information en Mauritanie.

Cependant, en raison de la nature particulière du domaine des technologies de l'information et de la communication, ainsi que de la spécificité du monde virtuel dans lequel ce type d'infractions est commis, d'importants défis demeurent. Leur prise en charge exige l'amélioration et la mise à jour de l'arsenal juridique, le renforcement des capacités des ressources humaines œuvrant dans ce secteur, ainsi que la diversification des mécanismes de coopération internationale afin de garantir une efficacité accrue dans la lutte contre ce phénomène.

Il est également nécessaire de créer un environnement propice où les efforts de tous les acteurs, tant du secteur public que du secteur privé, se conjuguent dans le cadre d'une vision globale anticipant les perspectives futures de la révolution numérique, laquelle connaît une expansion continue et des évolutions rapides et successives.

ANNEXE 3. ANNEXES DU RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 12 JUILLET 2023

ANNEXE I

CERTIFICAT D'INJONCTION EUROPÉENNE DE PRODUCTION (EPOC) CONCERNANT LA PRODUCTION DE PREUVES ÉLECTRONIQUES

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil ([1]), le destinataire du présent certificat d'injonction européenne de production (EPOC) doit exécuter celui-ci et transmettre les données demandées, dans les délais visés à la section C du présent EPOC, à l'autorité compétente mentionnée à la section L, point a), du présent EPOC.

Dans tous les cas, le destinataire doit, à la réception de l'EPOC, agir rapidement pour conserver les données demandées, à moins que les informations contenues dans l'EPOC ne permettent pas d'identifier ces données. La conservation des données doit être maintenue jusqu'à ce que les données soient produites ou jusqu'à ce que l'autorité d'émission ou, le cas échéant, l'autorité chargée de la mise en œuvre indique qu'il n'est plus nécessaire de conserver ni de produire les données.

Le destinataire doit prendre les mesures nécessaires pour garantir la confidentialité, le secret et l'intégrité de l'EPOC, ainsi que des données produites ou conservées.

SECTION A: Autorité d'émission/de validation

État d'émission: .....

Autorité d'émission: .....

Autorité de validation (le cas échéant): .....

NB: les coordonnées de l'autorité d'émission et de validation doivent être fournies à la fin du formulaire (sections I et J) .....

Numéro du dossier de l'autorité d'émission: .....

Numéro du dossier de l'autorité de validation: .....

SECTION B: Destinataire

Destinataire: .....

☐ Établissement désigné

☐ Représentant légal

☐ La présente injonction est émise dans un cas d'urgence à l'attention du destinataire indiqué parce que l'établissement désigné ou le représentant légal d'un fournisseur de services n'a pas réagi à l'EPOC dans les délais fixés à l'article 10 du règlement (UE) 2023/1543 ou n'a pas été désigné dans les délais fixés dans la directive (UE) 2023/1544 du Parlement européen et du Conseil ([2])

Adresse: .....

Téléphone/Télécopieur/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

([1]) Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

([2]) Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181).

SECTION C: Délais (cochez la case appropriée et complétez le cas échéant)

À la réception de l'EPOC, les données demandées doivent être produites:

☐ dès que possible et au plus tard dans un délai de dix jours (pas de notification à l'autorité chargée de la mise en œuvre);

☐ en cas de notification à l'autorité chargée de la mise en œuvre: à l'expiration du délai de dix jours, lorsque l'autorité chargée de la mise en œuvre n'a pas invoqué de motif de refus dans ce délai, ou lorsqu'elle confirme avant l'expiration du délai de dix jours qu'elle n'invoquera aucun motif de refus, dès que possible et au plus tard à la fin du délai de dix jours;

☐ sans retard injustifié et au plus tard dans un délai de huit heures dans un cas d'urgence impliquant:

☐ une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne;

☐ une menace imminente pour une infrastructure critique telle qu'elle est définie à l'article 2, point a), de la directive 2008/114/CE du Conseil ([3]) lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice des fonctions essentielles de l'État.

Précisez si des délais de procédure ou autres devraient être pris en compte pour l'exécution du présent EPOC: ....

Veuillez fournir des informations supplémentaires, s'il y a lieu: ....

SECTION D: Lien avec une demande de production ou de conservation antérieure (cochez et complétez le cas échéant et si ces informations sont disponibles)

☐ Les données demandées ont été totalement/partiellement conservées conformément à une demande de conservation

émise précédemment par ..... (indiquez l'autorité et le numéro de dossier)

le .... (indiquez la date d'émission de la demande)

et transmise le ..... (indiquez la date de transmission de la demande)

à ..... (indiquez le fournisseur de services/le représentant légal/l'établissement désigné/l'autorité compétente à qui la demande a été transmise et, s'il est disponible, le numéro de dossier attribué par le destinataire).

☐ Les données demandées sont liées à une demande de production

émise précédemment par ..... (indiquez l'autorité et le numéro de dossier)

le .... (indiquez la date d'émission de la demande)

et transmise le ..... (indiquez la date de transmission de la demande)

à ..... (indiquez le fournisseur de services/le représentant légal/l'établissement désigné/l'autorité compétente à qui la demande a été transmise et, s'il est disponible, le numéro de dossier attribué par le destinataire).

Autres informations utiles: ....

([3]) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

SECTION E: Informations à l'appui de l'identification des données demandées (complétez dans la mesure où ces informations sont connues et nécessaires pour identifier les données)

Adresse(s) IP et horodatages (y compris date et fuseau horaire): .....

Numéro de téléphone: ....

Adresse(s) électronique(s): ....

Numéro(s) IMEI: ....

Adresse(s) MAC: ....

Utilisateur(s) ou autre(s) identifiant(s) unique(s) tels que le ou les noms d'utilisateur, le ou les identifiants de connexion ou le ou les noms du compte: ....

Nom(s) du ou des services concernés: ....

Autre: ....

S'il y a lieu, la période couverte par les données pour lesquelles la production est demandée:

....

☐ Informations supplémentaires si nécessaire: ....

SECTION F: Preuves électroniques à produire

Le présent EPOC concerne (cochez la ou les cases appropriées):

a) ☐ des données relatives aux abonnés:

☐ le nom, la date de naissance, l'adresse postale ou géographique et les coordonnées (adresse électronique, numéro de téléphone) de l'utilisateur/du titulaire de l'abonnement et d'autres informations pertinentes permettant de l'identifier

☐ la date et l'heure du premier enregistrement, le type d'enregistrement, la copie du contrat, les moyens de vérification de l'identité utilisés au moment de l'enregistrement et des copies des documents fournis par l'abonné

☐ le type de service et sa durée, y compris le ou les identifiants utilisés par l'abonné ou qui lui a/ont été fourni(s) au moment du premier enregistrement ou de la première activation (par exemple numéro de téléphone, numéro de carte SIM, adresse MAC) et dispositif(s) associé(s)

☐ des informations relatives au profil (par exemple nom d'utilisateur, pseudonyme, photo de profil)

☐ des données sur la validation de l'utilisation du service, comme une adresse électronique de substitution fournie par l'utilisateur/le titulaire de l'abonnement

☐ des informations relatives à une carte de débit ou de crédit (fournies par l'utilisateur à des fins de facturation), y compris d'autres moyens de paiement

☐ des codes PUK

☐ autre: .....

b) ☐ des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543:

☐ les enregistrements des connexions IP, par exemple les adresses IP/journaux/numéros d'accès ainsi que tout autre identifiant technique, tel que les ports de provenance, l'horodatage ou équivalent, l'identifiant de l'utilisateur et l'interface utilisée dans le cadre de l'utilisation du service; veuillez préciser, si nécessaire: .....

☐ la période couverte par les données pour lesquelles la production est demandée (si elle est différente de la section E): ....

☐ autre: .....

c) ☐ les données relatives au trafic:

i) pour la téléphonie (mobile):

☐ les identifiants sortants (A) et entrants (B) (numéro de téléphone, IMSI, IMEI)

☐ l'heure et la durée de la ou des connexions

☐ la ou les tentatives d'appel

☐ l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion

☐ le support/téléservice utilisé (par exemple UMTS, GPRS)

☐ autre: .....

ii) pour l'internet:

☐ les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur, informations de l'en-tête de courrier électronique, identité du message]

☐ l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la ou des connexions

☐ le volume de données

☐ la date et l'heure de la ou des connexions

☐ la durée de la connexion ou de la ou des sessions d'accès

☐ autre: .....

iii) pour l'hébergement:

☐ les fichiers-journaux

☐ les tickets

☐ autre: .....

iv) autre:

☐ l'historique d'achats

☐ l'historique de rechargement du solde prépayé

☐ autre: .....

d) ☐ les données relatives au contenu:

☐ dump d'une boîte de messagerie (internet)

☐ dump d'un stockage en ligne (données générées par l'utilisateur)

☐ dump de pages

☐ un journal/une sauvegarde de messages

☐ dump d'une messagerie vocale

☐ un contenu de serveurs

☐ une sauvegarde d'appareil

☐ une liste de contacts

☐ autre: .....

☐ Informations supplémentaires si nécessaire pour préciser ou limiter (davantage) l'éventail des données demandées: .....

SECTION G: Informations sur les conditions sous-jacentes

a) Le présent EPOC concerne (cochez la ou les cases appropriées):

☐ une procédure pénale concernant une ou des infractions pénales;

☐ l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

b) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC est émis ainsi que la disposition légale applicable ([4]):

....

c) Le présent EPOC est délivré pour des données relatives au trafic qui ne sont pas demandées à la seule fin d'identifier l'utilisateur, ou pour des données relatives au contenu, ou les deux, et concerne (cochez la ou les cases appropriées, s'il y a lieu):

☐ une ou plusieurs infractions pénales passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans dans l'État d'émission;

([4]) Pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté en ce qui concerne des données relatives au trafic, qui ne sont pas demandées à la seule fin d'identifier l'utilisateur, ou des données relatives au contenu, veuillez indiquer aux points b) et c) l'infraction pour laquelle la peine a été imposée.

☐ une ou plusieurs des infractions suivantes, commises totalement ou partiellement au moyen d'un système informatique:

☐ une ou plusieurs des infractions définies aux articles 3 à 8 de la directive (UE) 2019/713 du Parlement européen et du Conseil ([5]);

☐ une ou plusieurs des infractions définies aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil ([6]);

☐ une ou plusieurs des infractions définies aux articles 3 à 8 de la directive 2013/40/UE du Parlement européen et du Conseil ([7]);

☐ des infractions pénales telles qu'elles sont définies aux articles 3 à 12 et à l'article 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil ([8]);

d) Responsable du traitement/sous-traitant:

Les injonctions européennes de production sont adressées aux fournisseurs de services agissant en qualité de responsables du traitement. À titre exceptionnel, l'injonction européenne de production peut être adressée directement au fournisseur de services qui traite les données pour le compte du responsable du traitement.

Cochez la ou les cases appropriées:

☐ Le présent EPOC est adressé au fournisseur de services agissant en qualité de responsable du traitement.

☐ Le présent EPOC est adressé au fournisseur de services qui traite ou, dans les situations où le responsable du traitement ne peut pas être identifié, qui pourrait traiter les données pour le compte du responsable du traitement, car:

☐ le responsable du traitement ne peut être identifié malgré des efforts raisonnables de la part de l'autorité d'émission;

☐ le fait de s'adresser au responsable du traitement pourrait nuire à l'enquête.

Si le présent EPOC est adressé au fournisseur de services traitant des données pour le compte du responsable du traitement:

☐ le sous-traitant informe le responsable du traitement de la production des données;

☐ le sous-traitant n'informe pas le responsable du traitement de la production des données jusqu'à nouvel ordre, car cela nuirait à l'enquête. Veuillez fournir une brève justification ([9]):

e) Autres informations utiles: ....

SECTION H: Informations à l'utilisateur

En tout état de cause, le destinataire s'abstient d'informer la personne dont les données sont demandées. Il incombe à l'autorité d'émission d'informer cette personne de la production des données, sans retard injustifié.

([5]) Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (JO L 123 du 10.5.2019, p. 18).

([6]) Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

([7]) Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

([8]) Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

([9]) L'autorité d'émission doit indiquer les raisons du retard dans le dossier, seule une brève justification doit être ajoutée dans l'EPOC.

Veuillez noter que (cochez la ou les cases appropriées):

☐ l'autorité d'émission retardera l'information de la personne dont les données sont demandées, aussi longtemps qu'une ou plusieurs des conditions suivantes sont remplies:

☐ il est nécessaire d'éviter d'entraver des enquêtes, des recherches ou des procédures officielles ou judiciaires;

☐ il est nécessaire d'éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

☐ il est nécessaire de protéger la sécurité publique;

☐ il est nécessaire de protéger la sécurité nationale;

☐ il est nécessaire de protéger les droits et libertés de tiers.

SECTION I: Coordonnées de l'autorité d'émission

Type d'autorité d'émission (cochez la ou les cases appropriées):

☐ juge, juridiction ou juge d'instruction;

☐ procureur;

☐ autre autorité compétente déterminée par l'État d'émission.

Si une validation est nécessaire, veuillez également compléter la section J.

Veuillez noter que (cochez le cas échéant):

☐ Le présent EPOC a été émis pour des données relatives aux abonnés, ou pour des données demandées à la seule fin d'identifier l'utilisateur, dans un cas d'urgence dont l'existence est établie de manière valable sans validation préalable, parce que la validation n'aurait pas pu être obtenue à temps, ou pour les deux catégories de données. L'autorité d'émission confirme qu'elle pourrait émettre une injonction sans validation dans le cadre d'une procédure nationale similaire, et qu'elle demandera la validation ex post sans retard injustifié, au plus tard dans les 48 heures (veuillez noter que le destinataire ne sera pas informé).

Coordonnées de l'autorité d'émission ou de son représentant, ou des deux, certifiant que le contenu de l'EPOC est exact et correct:

Nom de l'autorité: .....

Nom de son représentant: .....

Fonction (titre/grade): .....

Numéro de dossier: .....

Adresse: .....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: .....

Langue(s) parlée(s): ....

Si elle ou il diffère de ceux indiqués précédemment, autorité/point de contact (par exemple l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC:

Nom de l'autorité/nom: ....

Adresse: ....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: ....

Signature de l'autorité d'émission ou de son représentant certifiant que le contenu de l'EPOC est exact et correct:

Date: ....

Signature ([10]):

SECTION J: Coordonnées de l'autorité de validation (complétez le cas échéant)

Type d'autorité de validation

☐ juge, juridiction ou juge d'instruction

☐ procureur

Coordonnées de l'autorité de validation ou de son représentant, ou des deux, certifiant que le contenu de l'EPOC est exact et correct:

Nom de l'autorité: ....

Nom de son représentant: ....

Fonction (titre/grade): ....

Numéro de dossier: ....

Adresse: ....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: ....

Langue(s) parlée(s): ....

([10]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

Date: ....

Signature ([11]):

SECTION K: Notification et coordonnées de l'autorité chargée de la mise en œuvre à qui une notification est adressée (le cas échéant)

☐ Le présent EPOC est notifié à l'autorité chargée de la mise en œuvre suivante:.....

Veuillez indiquer les coordonnées de l'autorité chargée de la mise en œuvre à qui une notification est adressée (si elles sont disponibles):

Nom de l'autorité chargée de la mise en œuvre: ....

Adresse: ....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: ....

SECTION L: Transfert de données

a) Autorité à qui les données doivent être transférées

☐ autorité d'émission

☐ autorité de validation

☐ autre autorité compétente (par exemple autorité centrale)

Nom et coordonnées de contact: ....

b) Format privilégié dans lequel les données doivent être transférées ou moyen de transfert privilégié (le cas échéant): ....

SECTION M: Informations complémentaires à inclure (à ne pas envoyer au destinataire — à fournir à l'autorité chargée de la mise en œuvre dans le cas où la notification à l'autorité chargée de la mise en œuvre est requise)

Motifs qui permettent d'établir que l'injonction européenne de conservation remplit les conditions de la nécessité et de la proportionnalité:

....

Description succincte de l'affaire:

....

([11]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

L'infraction pour laquelle l'injonction européenne de production est émise est-elle passible dans l'État d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans et figure-t-elle dans la liste d'infractions ci-dessous (cochez la ou les cases appropriées)?

☐ participation à une organisation criminelle;

☐ terrorisme;

☐ traite d'êtres humains;

☐ exploitation sexuelle des enfants et pédopornographie;

☐ trafic de stupéfiants et de substances psychotropes;

☐ trafic d'armes, de munitions et d'explosifs;

☐ corruption;

☐ fraude, y compris la fraude et les autres infractions pénales portant atteinte aux intérêts financiers de l'Union définies dans la directive (UE) 2017/1371 du Parlement européen et du Conseil ([12]);

☐ blanchiment des produits du crime;

☐ faux monnayage et contrefaçon de monnaie, y compris de l'euro;

☐ cybercriminalité;

☐ crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;

☐ aide à l'entrée et au séjour irréguliers;

☐ homicide volontaire ou coups et blessures graves;

☐ trafic d'organes et de tissus humains;

☐ enlèvement, séquestration ou prise d'otage;

☐ racisme et xénophobie;

☐ vol organisé ou à main armée;

☐ trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;

☐ escroquerie;

☐ racket et extorsion de fonds;

☐ contrefaçon et piratage de produits;

☐ falsification de documents administratifs et trafic de faux;

☐ falsification de moyens de paiement;

☐ trafic de substances hormonales et d'autres facteurs de croissance;

([12]) Directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO L 198 du 28.7.2017, p. 29).

☐ trafic de matières nucléaires et radioactives;

☐ trafic de véhicules volés;

☐ viol;

☐ incendie volontaire;

☐ crimes relevant de la compétence de la Cour pénale internationale;

☐ détournement d'aéronefs ou de navires;

☐ sabotage.

Le cas échéant, veuillez ajouter toute information supplémentaire dont l'autorité chargée de la mise en œuvre pourrait avoir besoin pour évaluer la possibilité d'invoquer des motifs de refus:

… ....

ANNEXE II

CERTIFICAT D'INJONCTION EUROPÉENNE DE CONSERVATION (EPOC-PR) CONCERNANT LA CONSERVATION DE PREUVES ÉLECTRONIQUES

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire du présent certificat d'injonction européenne de conservation (EPOC-PR) doit, sans retard injustifié après réception de l'EPOC-PR, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne prolonge ce délai de 30 jours supplémentaires ou ne confirme qu'une demande de production ultérieure a été émise. Si l'autorité d'émission confirme dans ces délais qu'une demande de production ultérieure a été émise, le destinataire doit conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande de production ultérieure aura été reçue.

Le destinataire doit prendre les mesures nécessaires pour garantir la confidentialité, le secret et l'intégrité de l'EPOC-PR, ainsi que des données conservées.

SECTION A: Autorité d'émission/de validation

État d'émission: ....

Autorité d'émission: ....

Autorité de validation (le cas échéant): ....

NB: les coordonnées de l'autorité d'émission et de validation doivent être fournies à la fin du formulaire (sections F et G)

Numéro du dossier de l'autorité d'émission: ....

Numéro du dossier de l'autorité de validation: ....

SECTION B: Destinataire

Destinataire: ....

☐ Établissement désigné

☐ Représentant légal

☐ La présente injonction est émise dans un cas d'urgence à l'attention du destinataire indiqué parce que l'établissement désigné ou le représentant légal d'un fournisseur de services n'a pas réagi à l'EPOC-PR dans les délais ou n'a pas été désigné dans les délais fixés dans la directive (UE) 2023/1544 du Parlement européen et du Conseil [2]

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

[2] Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181).

Adresse: .....

Téléphone/Télécopie/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

SECTION C: Informations à l'appui de l'identification des données dont la conservation a été demandée (complétez dans la mesure où ces informations sont connues et nécessaires pour identifier les données)

☐ Adresse(s) IP et horodatages (y compris date et fuseau horaire): .....

☐ Numéro de téléphone: .....

☐ Adresse(s) électronique(s): .....

☐ Numéro(s) IMEI: .....

☐ Adresse(s) MAC: .....

☐ Utilisateur(s) du service ou autre(s) identifiant(s) unique(s) tels que le ou les noms d'utilisateur, le ou les identifiants de connexion ou le ou les noms du compte .....

☐ Nom(s) du ou des services concernés: .....

☐ Autres informations: .....

S'il y a lieu, la période couverte par les données pour lesquelles la conservation est demandée: .....

☐ Informations supplémentaires si nécessaire: .....

SECTION D: Preuves électroniques à conserver

Le présent EPOC-PR concerne (cochez la ou les cases appropriées):

a) ☐ des données relatives aux abonnés:

☐ le nom, la date de naissance, l'adresse postale ou géographique et les coordonnées (adresse électronique, numéro de téléphone) de l'utilisateur/du titulaire de l'abonnement et d'autres informations pertinentes permettant de l'identifier

☐ la date et l'heure du premier enregistrement, le type d'enregistrement, la copie du contrat, les moyens de vérification de l'identité utilisés au moment de l'enregistrement, des copies des documents fournis par l'abonné

☐ le type de service et sa durée, y compris le ou les identifiants utilisés par l'abonné ou qui lui a/ont été fourni (s) au moment du premier enregistrement ou de la première activation (par exemple numéro de téléphone, numéro de carte SIM, adresse MAC) et dispositif(s) associé(s)

☐ des informations relatives au profil (par exemple nom d'utilisateur, pseudonyme, photo de profil)

☐ des données sur la validation de l'utilisation du service, comme une adresse électronique de substitution fournie par l'utilisateur/le titulaire de l'abonnement

☐ des informations relatives à une carte de débit ou de crédit (fournies par l'utilisateur à des fins de facturation), y compris d'autres moyens de paiement

☐ des codes PUK

☐ autre: ....

b) ☐ des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543:

☐ les enregistrements des connexions IP, par exemple les adresses IP/journaux/numéros d'accès ainsi que tout autre identifiant, tel que les ports de provenance, l'horodatage ou équivalent, l'identifiant de l'utilisateur et l'interface utilisée dans le cadre de l'utilisation du service, strictement nécessaire à des fins d'identification; veuillez préciser, si nécessaire: ....

☐ la période couverte par les données pour lesquelles la conservation est demandée (si elle est différente de la section C):..... .....

☐ autre: ....

c) ☐ les données relatives au trafic;

i) pour la téléphonie (mobile):

☐ les identifiants sortants (A) et entrants (B) (numéro de téléphone, IMSI, IMEI)

☐ l'heure et la durée de la ou des connexions

☐ la ou les tentatives d'appel

☐ l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion

☐ le support/téléservice utilisé (par exemple UMTS, GPRS)

☐ autre: ....

ii) pour l'internet:

☐ les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur, informations de l'en-tête de courrier électronique, identité du message]

☐ l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la ou des connexions

☐ le volume de données

☐ la date et l'heure de la ou des connexions

☐ la durée de la connexion ou de la ou des sessions d'accès

☐ autre: ....

iii) pour l'hébergement:

☐ les fichiers-journaux

☐ les tickets

☐ autre: ....

iv) autre

☐ l'historique d'achats

☐ l'historique de rechargement du solde prépayé

☐ autre: ....

d) ☐ des données relatives au contenu:

☐ dump d'une boîte de messagerie (internet)

☐ dump d'un stockage en ligne (données générées par l'utilisateur)

☐ dump de pages

☐ un journal/une sauvegarde de messages

☐ dump d'une messagerie vocale

☐ un contenu de serveurs

☐ une sauvegarde d'appareil

☐ une liste de contacts

☐ autre: ....

☐ Informations supplémentaires si nécessaire pour préciser ou limiter (davantage) la période couverte par les données demandées:..... .....

SECTION E: Informations sur les conditions sous-jacentes

a) Le présent EPOC-PR concerne (cochez la ou les cases appropriées):

☐ une procédure pénale concernant une infraction pénale;

☐ l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

b) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC-PR est émis ainsi que la disposition légale applicable ([3]):..... .....

SECTION F: Coordonnées de l'autorité d'émission

Type d'autorité d'émission (cochez la ou les cases appropriées):

☐ juge, juridiction ou juge d'instruction;

☐ procureur;

☐ autre autorité compétente telle qu'elle est déterminée par le droit de l'État d'émission.

Si une validation est nécessaire, veuillez également compléter la section G.

Veuillez noter que (cochez le cas échéant):

☐ Le présent EPOC-PR a été émis pour des données relatives aux abonnés, ou pour des données demandées à la seule fin d'identifier l'utilisateur, dans un cas d'urgence dont l'existence est établie de manière valable, sans validation préalable, parce que la validation n'aurait pas pu être obtenue à temps, ou pour les deux catégories de données. L'autorité d'émission confirme qu'elle pourrait émettre une injonction sans validation dans le cadre d'une procédure nationale similaire et qu'elle demandera la validation ex post sans retard injustifié, au plus tard dans les 48 heures (veuillez noter que le destinataire ne sera pas informé).

Ce cas d'urgence renvoie à une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, ou une menace imminente pour une infrastructure critique, telle qu'elle est définie à l'article 2, point a), de la directive 2008/114/CE du Conseil ([4]), lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice des fonctions essentielles de l'État.

Coordonnées de l'autorité d'émission et/ou de son représentant certifiant que le contenu de l'EPOC-PR est exact et correct:

Nom de l'autorité:..... .....

Nom de son représentant:..... .....

Fonction (titre/grade):..... .....

([3]) Pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté, veuillez indiquer l'infraction pour laquelle la peine a été imposée.

([4]) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes (JO L 345 du 23.12.2008, p. 75).

Numéro de dossier: .....

Adresse: .....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: .....

Langue(s) parlée(s): .....

Si elle ou il diffère de ceux indiqués précédemment, autorité/point de contact (par exemple l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom de l'autorité/nom: .....

Adresse: .....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: .....

Signature de l'autorité d'émission ou de son représentant certifiant que le contenu de l'EPOC-PR est exact et correct:

Date: .....

Signature ([5]): .....

SECTION G: Coordonnées de l'autorité de validation (complétez le cas échéant)

Type d'autorité de validation:

☐ juge, juridiction ou juge d'instruction

☐ procureur

Coordonnées de l'autorité de validation ou de son représentant, ou des deux, certifiant que le contenu de l'EPOC-PR est exact et correct:

Nom de l'autorité: .....

Nom de son représentant: .....

Fonction (titre/grade): .....

([5]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

Numéro de dossier: .....

Adresse: .....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: .....

Langue(s) parlée(s): .....

Date: .....

Signature ([6]): .....

([6]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE III

INFORMATIONS CONCERNANT L'IMPOSSIBILITÉ D'EXÉCUTER UN EPOC/EPOC-PR

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], lorsque le destinataire n'est pas en mesure de respecter son obligation de conserver les données demandées en vertu d'un EPOC-PR ou de les produire en vertu d'un EPOC, n'est pas en mesure de respecter le délai spécifié ou ne fournit pas les données de manière exhaustive, il convient que le destinataire remplisse le présent formulaire et le renvoie, sans retard injustifié, à l'autorité d'émission ainsi que, si une notification a eu lieu et dans les autres cas où cela s'impose, à l'autorité chargée de la mise en œuvre visée dans l'EPOC.

Dans la mesure du possible, le destinataire conserve les données requises, même lorsque des informations supplémentaires sont nécessaires pour identifier les données de manière précise, sauf si les informations qui figurent dans l'EPOC/EPOC-PR ne sont pas suffisantes à cet effet. Si des éclaircissements de la part de l'autorité d'émission sont nécessaires, le destinataire les demande, sans retard injustifié, au moyen du présent formulaire.

SECTION A: Certificat concerné

Les informations suivantes concernent:

☐ un certificat d'injonction européenne de production (EPOC)

☐ un certificat d'injonction européenne de conservation (EPOC-PR)

SECTION B: Autorité ou autorités concernées

Autorité d'émission:.....

Numéro du dossier de l'autorité d'émission:.....

Le cas échéant, autorité de validation:.....

Le cas échéant, numéro du dossier de l'autorité de validation:.....

Date d'émission de l'EPOC/EPOC-PR:.....

Date de réception de l'EPOC/EPOC-PR:.....

Le cas échéant, autorité chargée de la mise en œuvre:.....

Numéro du dossier de l'autorité chargée de la mise en œuvre, s'il est disponible:.....

SECTION C: Destinataire de l'EPOC/EPOC-PR

Destinataire de l'EPOC/EPOC-PR:.....

Numéro du dossier du destinataire:.....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION D: Raisons de la non-exécution

a) L'EPOC/EPOC-PR ne peut pas être exécuté ou ne peut pas être exécuté dans le délai spécifié pour la ou les raisons suivantes:

☐ il est incomplet;

☐ il contient des erreurs manifestes;

☐ il ne contient pas suffisamment d'informations;

☐ il ne concerne pas des données stockées par le fournisseur de services ou pour le compte de celui-ci au moment de la réception de l'EPOC/EPOC-PR;

☐ autres motifs d'impossibilité de fait due à des circonstances qui ne sont pas imputables au destinataire ou au fournisseur de services au moment de la réception de l'EPOC/EPOC-PR;

☐ l'injonction européenne de production/l'injonction européenne de conservation n'a pas été émise ou validée par une autorité d'émission mentionnée à l'article 4 du règlement (UE) 2023/1543;

☐ l'injonction européenne de production visant à obtenir des données relatives au trafic qui ne sont pas demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543, ou visant à obtenir des données relatives au contenu, a été émise pour une infraction qui n'est pas visée à l'article 5, paragraphe 4, du règlement (UE) 2023/1543;

☐ le service n'est pas couvert par le règlement (UE) 2023/1543;

☐ les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias qui empêchent l'exécution de l'injonction européenne de production ou de l'injonction européenne de conservation;

☐ le respect de l'injonction européenne de production entrerait en conflit avec le droit applicable d'un pays tiers. Veuillez également compléter la section E.

b) Veuillez préciser les raisons de la non-exécution visée au point a) et, si nécessaire, indiquez et expliquez toute raison autre que celles énumérées au point a):

… ....

SECTION E: Obligations en conflit découlant du droit d'un pays tiers

En cas d'obligations en conflit découlant du droit d'un pays tiers, veuillez fournir les informations suivantes:

— intitulé du ou des actes juridiques du pays tiers:

… ....

— disposition(s) légale(s) applicable(s) et texte de la ou des dispositions pertinentes:

… ....

— nature de l'obligation en conflit, y compris l'intérêt protégé par le droit du pays tiers:

☐ droits fondamentaux des particuliers (veuillez préciser):

… ....

☐ intérêts fondamentaux du pays tiers liés à la sécurité et à la défense nationales (veuillez préciser):

… ....

☐ autres intérêts (veuillez préciser):

… ....

— veuillez expliquer pourquoi le droit est applicable en l'espèce:

… ....

— veuillez expliquer pourquoi vous estimez qu'il y a conflit en l'espèce:

… ....

— veuillez expliquer le lien entre le fournisseur de services et le pays tiers en question:

… ....

— conséquences possibles du respect de l'injonction européenne de production pour le destinataire, y compris les sanctions auxquelles il s'expose:

… ....

Veuillez ajouter toute information supplémentaire pertinente: ....

SECTION F: Demande d'informations supplémentaires/d'éclaircissements (veuillez compléter le cas échéant)

Des informations supplémentaires sont requises de la part de l'autorité d'émission afin que l'EPOC/EPOC-PR soit exécuté:

… ....

SECTION G: Conservation des données

Les données demandées (cochez la case appropriée et complétez):

☐ ont été conservées jusqu'à ce que les données soient produites, ou jusqu'à ce que l'autorité d'émission ou, le cas échéant, l'autorité chargée de la mise en œuvre, indique qu'il n'est plus nécessaire de conserver ni de produire les données, ou jusqu'à ce que l'autorité d'émission fournisse les informations nécessaires pour permettre de circonscrire les données à conserver/produire;

☐ n'ont pas été conservées (cela ne devrait s'appliquer qu'à titre exceptionnel, par exemple si le fournisseur de services ne détient pas les données à la réception de la demande ou ne peut pas suffisamment identifier les données demandées).

SECTION H: Coordonnées de l'établissement désigné/du représentant légal du fournisseur de services

Nom de l'établissement désigné/du représentant légal du fournisseur de services:
.....

Nom du point de contact: ....

Poste occupé: .....

Adresse: .....

Numéro de téléphone: (indicatif du pays) (indicatif de zone ou urbain) .....

Numéro de télécopieur: (indicatif du pays) (indicatif de zone ou urbain) .....

Adresse électronique: .....

Nom de la personne autorisée: ....

Date: .....

Signature ([2]): .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE IV

CATÉGORIES D'INFRACTIONS VISÉES À L'ARTICLE 12, PARAGRAPHE 1, POINT D)

1) participation à une organisation criminelle;

2) terrorisme;

3) traite des êtres humains;

4) exploitation sexuelle des enfants et pédopornographie;

5) trafic de stupéfiants et de substances psychotropes;

6) trafic d'armes, de munitions et d'explosifs;

7) corruption;

8) fraude, y compris la fraude et les autres infractions pénales portant atteinte aux intérêts financiers de l'Union définies dans la directive (UE) 2017/1371 du Parlement européen et du Conseil ([1]);

9) blanchiment des produits du crime;

10) faux monnayage et contrefaçon de monnaie, y compris de l'euro;

11) cybercriminalité;

12) crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;

13) aide à l'entrée et au séjour irréguliers;

14) homicide volontaire ou coups et blessures graves;

15) trafic d'organes et de tissus humains;

16) enlèvement, séquestration ou prise d'otage;

17) racisme et xénophobie;

18) vol organisé ou à main armée;

19) trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;

20) escroquerie;

21) racket et extorsion de fonds;

22) contrefaçon et piratage de produits;

([1]) Directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO L 198 du 28.7.2017, p. 29).

23) falsification de documents administratifs et trafic de faux;

24) falsification de moyens de paiement;

25) trafic de substances hormonales et d'autres facteurs de croissance;

26) trafic de matières nucléaires et radioactives;

27) trafic de véhicules volés;

28) viol;

29) incendie volontaire;

30) crimes relevant de la compétence de la Cour pénale internationale;

31) détournement d'aéronefs ou de navires;

32) sabotage.

ANNEXE V

CONFIRMATION DE L'ÉMISSION D'UNE DEMANDE DE PRODUCTION À LA SUITE D'UNE INJONCTION EUROPÉENNE DE CONSERVATION

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire de l'EPOC-PR doit, après réception et sans retard injustifié, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne prolonge ce délai de 30 jours supplémentaires ou ne confirme qu'une demande de production ultérieure a été émise au moyen du formulaire figurant dans la présente annexe.

À la suite de cette confirmation, le destinataire doit conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande de production ultérieure aura été reçue.

SECTION A: Autorité d'émission de l'EPOC-PR

État d'émission: .....

Autorité d'émission: .....

Si elle ou il diffère du point de contact indiqué dans l'EPOC-PR, autorité/point de contact (par exemple, l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom et coordonnées de contact: .....

SECTION B: Destinataire de l'EPOC-PR

Destinataire: .....

Adresse: .....

Téléphone/télécopie/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION C: Informations sur l'EPOC-PR

Les données sont conservées conformément à l'EPOC-PR émis le..... (indiquez la date d'émission de la demande) et transmis le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier).

☐ Le délai a été prolongé de 30 jours par l'autorité d'émission …, numéro de dossier … le … (veuillez cocher la case et compléter, le cas échéant).

SECTION D: Confirmation

Le présent document confirme que la demande de production suivante a été émise (veuillez cocher la case appropriée et compléter, le cas échéant):

☐ Certificat d'injonction européenne de production émis par ..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmis le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmis à..... (indiquez le fournisseur de services/l'établissement désigné/le représentant légal/l'autorité compétente à qui il a été transmis et, s'il est disponible, le numéro de dossier attribué par le destinataire).

☐ Décision d'enquête européenne émise par..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmise le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmise à..... (indiquez l'État et l'autorité compétente à qui elle a été transmise et, s'il est disponible, le numéro de dossier attribué par les autorités requises).

☐ Demande d'entraide judiciaire émise par ..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmise le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmise à..... (indiquez l'État et l'autorité compétente à qui elle a été transmise et, s'il est disponible, le numéro de dossier attribué par les autorités requises).

Signature de l'autorité d'émission et/ou de son représentant:

Nom: .....

Date: .....

Signature ([2]): .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE VI

PROLONGATION DE LA CONSERVATION DE PREUVES ÉLECTRONIQUES

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire du certificat d'injonction européenne de conservation (EPOC-PR) doit, après réception et sans retard injustifié, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne confirme que la demande de production ultérieure a été émise. Dans le délai de 60 jours, l'autorité d'émission peut prolonger la durée de conservation de 30 jours supplémentaires, le cas échéant, pour permettre que la demande de production ultérieure soit émise, au moyen du formulaire figurant dans la présente annexe.

SECTION A: Autorité d'émission de l'EPOC-PR

État d'émission: … .....

Autorité d'émission: … .....

Numéro du dossier de l'autorité d'émission: …..... .

Si elle ou il diffère du point de contact indiqué dans l'EPOC-PR, autorité/point de contact (par exemple, l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom et coordonnées de contact: …..... .....

SECTION B: Destinataire de l'EPOC-PR

Destinataire: …..... .....

Adresse: … ....

Téléphone/télécopieur/adresse électronique (s'ils sont connus): …..... .....

Personne de contact (si elle est connue): …..... .....

Numéro du dossier du destinataire (s'il est connu): … .....

Fournisseur de services concerné (s'il est différent du destinataire): …..... .....

Autres informations utiles: …..... .....

SECTION C: Informations sur l'EPOC-PR préalable

Les données sont conservées conformément à l'EPOC-PR émis le …..... (indiquez la date d'émission de la demande) et transmis le … ..... (indiquez la date de transmission de la demande) avec le numéro de dossier … ..... (indiquez le numéro de dossier) et transmis à …..... .....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION D: Prolongation de l'injonction de conservation préalable

L'obligation de conserver les données au titre de l'EPOC-PR visé à la section C est prolongée par la présente de trente jours supplémentaires.

Signature de l'autorité d'émission et/ou de son représentant:

Nom: … .....

Date: … .....

Signature ([2]): … .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE 4. CAS PRATIQUE : EXERCICE AP2 ET SA SOLUTION

I. ENONCÉ

Une personne est kidnappée dans un état dénommé République Fédérale d'Agonlin (RFA), partie à la convention sur la cybercriminalité et son 2ème protocole additionnel. Le ravisseur utilise un compte de courrier électronique fourni par une société d'un autre pays pour communiquer avec la famille de la victime et demander une rançon. La police connaît l'adresse électronique mais, dans l'espoir d'établir son identité, elle a également besoin de l'adresse IP et d'autres données associées au compte.

Le ravisseur a demandé un transfert de la rançon sur un compte spécifique fourni par une société fintech d'un autre pays.

Quelles sont les possibilités d'obtenir des données susceptibles d'aider à établir l'identité du ravisseur ?

II. RÉSOLUTION CAS AP2

Présentation synthétique des possibilités opérationnelles pour obtenir des données utiles à l'identification du ravisseur.

a - Demande urgente de préservation auprès du fournisseur de messagerie et de la fintech

But : empêcher la suppression automatique ou volontaire des logs, courriels ou données de paiement.

Quelles données à préserver :

- pour le compte e-mail : logs de connexion (IP, horodatages), journaux d'activité, adresses IP source et relais (en têtes complets des courriels), métadonnées, cookies/identifiants de sessions, éventuels fichiers joints, données d'inscription (KYC si existant).
- pour le compte de paiement : données KYC/identification du titulaire du compte, historiques de transactions, origines/destinations de fonds, métadonnées des transactions, adresses IP liées aux connexions.

Comment : via le canal 24/7 de la Convention de Budapest si le pays destinataire y participe, ou via une demande écrite à l'hébergeur/fintech en vertu de leurs procédures (si la société accepte de coopérer directement).

Urgence : agir immédiatement — les logs sont souvent conservés peu de temps.

b - Production de données par le fournisseur (par voie directe ou via MLA)

Voie directe (si possible) :

- Le 2e protocole additionnel vise à faciliter certaines formes de coopération transfrontalière directe (par ex. demandes adressées directement aux fournisseurs situés à l'étranger) — mais ceci n'est possible que si le pays requérant et le pays du fournisseur ont ratifié et implémenté ces dispositions dans leur droit interne.
- Si la société a une politique d'assistance aux forces de l'ordre (et le cadre légal local le permet), elle peut fournir directement certaines données après examen d'une demande conforme (subpoena, ordonnance, etc.).

Voie MLAT / commission rogatoire :

- Si la voie directe n'est pas possible, la police doit demander la production via la Mutual Legal Assistance (MLA) (commission rogatoire internationale) vers l'État où est domiciliée la société. Ce processus est plus long mais fournit une base légale formelle pour obtenir des données protégées par secret bancaire ou par la législation locale.

Éléments à demander formellement :

- copies des en têtes complets des courriels (full headers),
- journaux de connexion (adresse IP, dates/heures UTC, identifiants d'appareils),
- logs applicatifs (sessions, resets, modifications),
- KYC/PII du titulaire du compte,
- logs de paiements (n° comptes, IBAN, wallet IDs), provenance des fonds,
- toute pièce permettant de relier un wallet/compte à une personne ou à un autre service (ex. adresses crypto liées, comptes relais).

c - Coopération financière et saisie et gel opéré sur le compte (blocs de fonds)

Contact via Cellule de Renseignement Financier (CRF ou en anglais Financial Intelligence Unit : FIU) / banques locales :

- Si la rançon a été dirigée sur un compte géré par une fintech étrangère, alerter la Financial Intelligence Unit (FIU) nationale et demander assistance internationale (gel temporaire de fonds, renseignements KYC).
- Les fintech doivent souvent respecter les règles AML/KYC : la fintech peut fournir l'identité du bénéficiaire, documents d'ouverture de compte, adresses IP liées, méthodes d'encaissement.

Possibilité de gel / injonction :

Selon le droit du pays du prestataire, une injonction judiciaire locale ou une demande MLA peut permettre le gel/RTO des fonds en attente de poursuites.

d - Données techniques à rechercher et leur utilité

- **Adresse IP(s) et horodatages** -> localisation géographique approximative, fournisseur d'accès, corrélation d'événements.
- **Full e mail headers** -> route des messages, serveurs relais, possibilité d'identifier une adresse IP d'origine.

- **Logs d'authentification multi facteurs** -> numéro de téléphone, adresse e-mail de secours, device IDs.
- **KYC / documents d'identité** -> nom légal, adresse, pièces justificatives.
- **Données de paiement** -> destinataire final, chaîne de transferts, comptes intermédiaires.
- **Métadonnées d'appareil** -> OS, version, identifiants matériels qui peuvent mener à des enquêteurs locaux.

e - Obstacles juridiques et pratiques

- **Protection des données / secret bancaire :** de nombreux États exigent une ordonnance judiciaire/MLA pour délivrer les données sensibles.
- **Différences de délais et procédures** : MLAT peut être long ; c'est pourquoi la préservation urgente est cruciale.
- **Coopération commerciale variable :** certaines plateformes répondent vite (si elles ont présence locale ou politique de LEO assistance), d'autres refusent sans ordonnance.
- **Cryptomonnaies et fintechs non régulées :** si la fintech est hors du cadre AML/KYC strict, il peut être difficile d'obtenir l'identité du titulaire.
- **Risque de destruction de preuves** par le ravisseur s'il détecte la pression ; importance d'approche discrète.

f - Mesures opérationnelles concrètes et ordre recommandé d'actions

- **Préservation immédiate :** adresser une demande écrite (ou via le 24/7) à l'hébergeur de messagerie et à la fintech pour qu'ils conservent toutes les données (logs, en têtes, KYC, transactions) pendant la durée maximale possible.
- **Collecte des éléments disponibles :** récupérer les e-mails (avec en têtes), captures d'écran, fils de discussion, coordonnées bancaires communiquées par le ravisseur, tout message vocal/vidéo, preuves de menace, etc.
- **Engager FIU / unité financière :** signaler le mouvement de fonds pour un gel ou une enquête sur l'origine/destination des fonds.
- **Lancer MLA / commission rogatoir**e vers les pays du fournisseur et de la fintech si nécessaire (préparer dossier avec preuve d'urgence, qualification pénale locale et française/béninoise selon compétences).
- **Message aux fournisseurs :** si possible, formuler des demandes conformes aux règles du fournisseur (format, pièces jointes) pour accélérer la coopération.
- **Exploiter les canaux internationaux :** INTERPOL/Europol si cross border et quand pertinents.
- **Analyse forensique** : à réception des logs, faire corrélations IP/timestamp, géolocalisation, recoupements avec d'autres infractions ou comptes.

g - Si le 2e protocole additionnel est applicable (points pratiques)

Il peut prévoir des mécanismes facilitant la requête directe auprès des fournisseurs et des procédures d'exécution plus rapides.

- **Condition :** il faut vérifier si l'État requérant (Bénin ? France ?) et l'État où se trouvent les entreprises ont ratifié et transposé le protocole. Si oui, le service d'enquête pourra utiliser ces voies directes plus rapides au lieu d'attendre la MLA longue.
- **Checklist pratique (modèle de données à demander dans la demande)**
    - Identification légale de la société (fournisseur e-mail / fintech).
    - Période à préserver (dates/heures UTC précises).
    - Type de données : full headers des courriels, logs d'accès (IP, user agent), logs d'authentification MFA, fichiers joints, données KYC (copies de pièces d'identité, adresse, mail, téléphone), historique des transactions, retraits et transferts du compte, adresses IP associées aux transferts, logs API, IP des nœuds d'accès, cookies/session IDs.
    - Motif / justification pénale (kidnapping et extorsion) + référence du dossier.
    - Coordonnées du contact judiciaire/police et exigences pour la remise des données (format, canal sécurisé).

ANNEXE 5. CAS PRATIQUE : LE CADRE CONVENTIONNEL

(Ce cas peut être résolu sous forme de question simple ou sous forme d'une dissertation juridique).

Les cybercriminels exploitent une vulnérabilité de Windows pour déployer un ransomware qui chiffre les fichiers de plus de 400 000 ordinateurs répartis dans plus de 60 municipalités de l'État dénommé « COVÈ ». Ils exigent un paiement en Eutherom en échange de la clé de déchiffrement.

La propagation du malware s'est effectuée via le réseau Internet et a causé d'importants dommages. Malgré le paiement de la rançon, tous les ordinateurs sont restés chiffrés.

1. À la lumière de la Convention sur la cybercriminalité, adoptée à Budapest (Hongrie) en 2001, quels sont les crimes commis par ces cybercriminels ?
2. A la lumière de la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel, adoptée à Malabo (Guinée Equatoriale) en 2014, quels sont les crimes commis par ces cybercriminels ?

a -Solution du cas pratique « Cadre conventionnel »

RÉSOLUTION DU CAS

Résumé des faits :

Des cybercriminels :

- exploitent une vulnérabilité de Windows,
- déploient un **ransomware,**
- **chiffrent illégalement des fichiers** sur 400 000 ordinateurs dans plus de 60 municipalités,
- **exigent une rançon en crypto-monnaie (Eutherom),**
- ne restituent pas les données malgré le paiement.

CRIMES COMMIS SELON LA CONVENTION DE BUDAPEST :

La Convention énumère plusieurs infractions que ce cas de figure permet d'illustrer.

1. Accès illégal à un système informatique

Article 2

Entrer sans autorisation dans un système informatique constitue un crime, même sans altération des données.

-> Les cybercriminels ont accédé sans autorisation aux ordinateurs des municipalités : c'est une infraction.

2. Interception illégale de données

Article 3

L'interception non autorisée de données, notamment en transit, est aussi un crime.

-> S'il y a eu interception de communications (e-mails, données en transit), cette infraction est également constituée.

3. Atteinte à l'intégrité des données

Article 4

L'altération, la suppression ou la détérioration de données informatiques est illégale.

-> Le chiffrement forcé des fichiers est une forme de détérioration illégale de données : cette infraction est remplie.

4. Atteinte au fonctionnement d'un système informatique

Article 5

Le fait d'entraver intentionnellement le fonctionnement d'un système informatique.

-> Le ransomware a rendu les ordinateurs inutilisables. Cela constitue une atteinte à leur fonctionnement.

5. Usage abusif d'un dispositif

Article 6

La création, la diffusion ou la possession d'un programme conçu pour commettre des infractions.

-> Le ransomware est un outil malveillant utilisé pour commettre ces crimes. Sa création ou diffusion est elle-même un crime.

6. Fraude informatique

Article 8

Le fait d'obtenir un gain économique indu par manipulation ou altération de données.

-> L'exigence d'une rançon (même non honorée) constitue une tentative de fraude informatique.

7. Extorsion (non expressément mentionnée mais relevant du droit pénal commun)

Bien que non explicitement mentionnée dans la Convention, l'extorsion par menace (ex : perte de données si non-paiement) est également un crime selon les législations nationales.

-> Les cybercriminels exigent une rançon sous menace : c'est une extorsion.

Résumé des infractions commises selon la Convention de Budapest :

N°	Infractions	Articles de la Convention
1	Accès illégal à un système informatique	Article 2
2	Atteinte à l'intégrité des données	Article 4
3	Atteinte au fonctionnement du système	Article 5
4	Usage abusif d'un dispositif (ransomware)	Article 6
5	Fraude informatique (rançon)	Article 8
6	Extorsion (droit pénal national)	Non Conventionnel

RÉSOLUTION SOUS FORME DE DISSERTATION JURIDIQUE DU CAS :

À la lumière de la Convention sur la cybercriminalité adoptée à Budapest (Hongrie) en 2001, quels sont les crimes commis par ces cybercriminels ?

INTRODUCTION

La transformation numérique des sociétés modernes s'accompagne de nouveaux risques, notamment ceux liés à la cybercriminalité. Pour y faire face, la Convention sur la cybercriminalité, adoptée à Budapest en 2001 sous l'égide du Conseil de l'Europe, établit le premier cadre juridique international à vocation mondiale destiné à harmoniser les législations nationales, faciliter la coopération internationale, et définir des infractions spécifiques liées à l'usage abusif des technologies de l'information.

Dans le cas présent, des cybercriminels ont exploité une vulnérabilité du système d'exploitation Windows pour déployer un **ransomware** qui a chiffré les fichiers de plus de 400 000 ordinateurs dans plus de 60 municipalités d'un État fictif nommé « COVÈ ». Ces attaques ont été accompagnées d'une demande de rançon en crypto-monnaie. Malgré le paiement, les fichiers sont demeurés inaccessibles.

Dès lors, **quelles infractions pénales peuvent être retenues à l'encontre de ces cybercriminels au regard des dispositions de la Convention de Budapest ?**

Pour répondre à cette question, il convient d'identifier les différentes infractions prévues par la Convention applicables aux faits (I), avant d'examiner les éventuelles qualifications complémentaires relevant du droit pénal général (II).

I. Les infractions spécifiques prévues par la Convention de Budapest

A. L'accès illégal à un système informatique (article 2)

La Convention qualifie d'infraction l'accès intentionnel, sans droit, à tout ou partie d'un système informatique. En s'introduisant dans les ordinateurs des municipalités, les auteurs des faits ont

violé cette disposition, même en l'absence de vol ou de destruction initiale de données.

B. L'atteinte à l'intégrité des données et des systèmes (articles 4 et 5)

Le **chiffrement forcé** des fichiers par le ransomware constitue une **altération** des données informatiques. Il s'agit d'une atteinte à leur intégrité au sens de l'article 4.

Par ailleurs, en empêchant les ordinateurs de fonctionner normalement, les cybercriminels ont entravé le bon fonctionnement des systèmes informatiques, ce qui est expressément incriminé par l'article 5.

C. L'usage abusif de dispositifs (article 6)

L'article 6 réprime la création, la détention ou la distribution de dispositifs conçus pour commettre les infractions visées par la Convention. Le ransomware utilisé dans ce cas est un programme malveillant entrant directement dans cette catégorie.

D. La fraude informatique (article 8)

La demande de rançon vise à obtenir un avantage financier illégal. Il s'agit là d'une tentative de fraude informatique, telle que définie à l'article 8, dès lors que les auteurs ont manipulé un système informatique pour obtenir une crypto-monnaie en contrepartie d'une promesse de restitution des données.

II. Les infractions complémentaires relevant du droit pénal général

A. L'extorsion

Même si la Convention de Budapest ne traite pas explicitement de **l'extorsion**, cette infraction est reconnue par la plupart des systèmes juridiques nationaux. Le fait d'exiger un paiement sous la menace et de ne pas restituer les données s'apparente clairement à **une extorsion de fonds,** notamment par voie électronique.

B. La tentative et la récidive

Dans certains cas, même en l'absence de gain effectif (par exemple, si le paiement de la rançon n'a pas abouti), les actes peuvent être qualifiés de tentative d'escroquerie ou de fraude, ce qui est également punissable dans de nombreux États.

Enfin, si les cybercriminels ont mené plusieurs attaques similaires, **la récidive** ou la commission en **bande organisée** peut aggraver les peines encourues.

CONCLUSION

Les faits rapportés révèlent une pluralité d'infractions informatiques caractérisées au regard de la Convention de Budapest, notamment l'accès illégal à des systèmes informatiques, l'altération de données, l'usage de logiciels malveillants et la fraude. À cela s'ajoutent des infractions de droit commun, telles que l'extorsion ou la tentative de fraude, qui viennent renforcer la responsabilité pénale des auteurs.

La Convention de Budapest joue ici un rôle central en fournissant un socle juridique commun aux

États parties, facilitant ainsi la coopération judiciaire internationale face à des attaques transfrontalières de plus en plus fréquentes et sophistiquées.

RÉSOLUTION DU CAS EN TENANT COMPTE DE LA CONVENTION DE MALABO

Résumé des faits

Des cybercriminels ont :

- Exploité une faille Windows pour déployer un ransomware.
- Chiffré illégalement les fichiers de plus de **400 000 ordinateurs** dans **plus de 60 municipalités** de l'État fictif de COVÈ.
- Exigé une rançon **en crypto-monnaie (Eutherom)** pour fournir une clé de déchiffrement.
- Les victimes sont restées privées d'accès, même après paiement.

Problématique juridique

Quels crimes ont été commis par les cybercriminels selon les dispositions de la **Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) ?**

Plan proposé

1. Qualification des infractions au regard de la Convention de Malabo
2. Violations spécifiques liées à la protection des données à caractère personnel

I. Qualification des infractions en matière de cybersécurité

La **Section III** (articles 25 à 30) de la Convention de Malabo définit **les infractions pénales liées aux technologies de l'information et de la communication (TIC)**. Les cybercriminels de l'affaire présentée ont commis plusieurs de ces infractions.

A. Accès illégal à un système informatique

Article 25(1)(a)

Constitue une infraction le fait d'accéder frauduleusement à tout ou partie d'un système informatique.

-> L'introduction non autorisée dans les ordinateurs municipaux de l'État de COVÈ remplit les critères de cet article.

B. Atteinte à l'intégrité des données et à leur disponibilité

Article 25(1)(c)

Est également un crime le fait d'altérer, supprimer, détériorer ou rendre indisponibles des données informatiques.

-> Le **chiffrement** imposé par le ransomware rend les fichiers **inaccessibles** aux utilisateurs légitimes : atteinte à la disponibilité des données.

C. Entrave au fonctionnement d'un système informatique

Article 25(1)(d)

Toute action perturbant volontairement le fonctionnement normal d'un système est punissable.

-> Le ransomware a paralysé les services municipaux : cette infraction est constituée.

D. Usage, production ou diffusion d'outils malveillants

Article 26(1)(a)

Est incriminée la fabrication, possession ou diffusion de programmes conçus pour commettre des infractions.

-> Le **ransomware** utilisé est un outil conçu pour paralyser et extorquer : son utilisation est illicite.

E. Extorsion via TIC

Article 27

Toute tentative d'obtenir un bien, un service ou un avantage en menaçant de détruire, altérer ou bloquer des données constitue une infraction.

-> Exiger un paiement (en Eutherom) en échange de la clé de déchiffrement est **une extorsion numérique,** clairement visée par la Convention.

II. Atteinte à la protection des données à caractère personnel

La **Section IV** de la Convention de Malabo traite spécifiquement de **la protection des données personnelles**, notamment en cas de traitement illégal ou non autorisé.

A. Traitement illicite des données

Article 29

Est sanctionné le traitement non autorisé de données à caractère personnel.

-> Même si les données n'ont pas été volées, le chiffrement non consenti constitue **un traitement illicite** (usage malveillant sans autorisation).

B. Atteinte à la sécurité des données

Article 30

Le responsable du traitement doit garantir la sécurité des données.

-> L'attaque montre une **faille de cybersécurité** du côté des municipalités (nécessitant des mesures de sécurité plus robustes), mais **la faute principale incombe aux cybercriminels,** qui ont intentionnellement compromis la sécurité des systèmes et des données.

Résumé des infractions commises (Convention de Malabo)

Type d'infraction	Article de la Convention
Accès illégal à un système informatique	Article 25(1)(a)
Altération / chiffrement illégal de données	Article 25(1)(c)
Blocage du fonctionnement du système	Article 25(1)(d)
Usage d'outils criminels (ransomware)	Article 26(1)(a)
Extorsion par TIC	Article 27
Traitement illicite de données personnelles	Article 29
Atteinte à la sécurité des données	Article 30

CONCLUSION

Les faits décrits dans le cas étudié relèvent d'une série d'infractions clairement définies par la **Convention de Malabo**, notamment en matière de cybersécurité (intrusion, altération, extorsion), mais également de protection des données à caractère personnel.

Cette Convention, adoptée par l'Union africaine, représente un outil juridique essentiel pour les États africains dans la lutte contre la cybercriminalité. Elle permet de qualifier juridiquement ces actes, de poursuivre les auteurs et d'encourager les États membres à renforcer leurs infrastructures de cybersécurité.

Loïc Guérin, Expert Justice International

12/2025

MIS EN OEUVRE PAR

EXPERTISE FRANCE
GROUPE AFD

FINANCÉ PAR

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

Mise en page : 202 www.kao-com.com