EUROMED JUSTICE

A programme funded by the European Union

EUROMED JUSTICE

Analyse juridique et des écarts
Cybercriminalité

CrimEx
GROUPE D'EXPERTS EUROMED JUSTICE EN MATIÈRE PÉNALE

ALGÉRIE, ÉGYPTE, ISRAËL, JORDANIE, LIBAN, MAROC, PALESTINE, TUNISIE

Expert EuroMed Justice: M. Daniel Suter, Royaume-Uni

Lead Firm /Chef de file

FIIAPP COOPERACIÓN ESPAÑOLA

EIPA

CILC Center for International Legal Cooperation

JCI Justice Coopération Internationale

AUTEUR(S):
Cette Analyse a été écrite par M. Dan Suter (directeur de iJust International – Royaume Uni), en collaboration avec: M. David Mayor Fernandez (Espagne), M. Giel Franssen (Pays-Bas), et Professeur Mohamed Elewa Badar (Egypte – Royaume Uni).

EDITEUR ET COORDINATEUR:
Virgil Ivan-Cucu, Expert principal EuroMed Justice, conférencier à EIPA Luxembourg.

VERSIONS LINGUISTIQUES
Originale: EN
Manuscrit finalisé en mars 2018.

CLAUSE DE NON-RESPONSABILITÉ

Les informations contenues dans les Fiches EuroMed, Analyses juridiques et des écarts, et le Manuel reposent sur les recherches et informations fournies par les experts et les représentants des Pays Partenaires du Voisinage Sud et les membres du CrimEx dans le contexte des travaux réalisés dans le cadre du Projet Euromed Justice, à l'exception du Liban. Aucun des juges ni représentants libanais n'ont contribué à ce travail de quelque manière que ce soit.. Le Consortium chargé de la mise en œuvre du projet ne peut pas être tenu responsable de leur exactitude, de leur actualité ou de leur exhaustivité, ni rendu responsable des erreurs ou omissions éventuelles contenues dans ce document.

Cette publication a été réalisée avec le soutien de la Commission européenne. Le contenu de cette publication ne peut en aucun cas être interprété comme reflétant le point de vue de la Commission européenne.

COPYRIGHT

www.euromed-justice.eu

Contents

Abréviations

ADPIC	Accord sur les droits de propriété intellectuelle liés au commerce
AP	Autorité palestinienne
CB	Convention de Budapest sur la cybercriminalité du Conseil de l'Europe
CERT	Équipe de préparation aux cyberévénements
CITO	Convention arabe pour la lutte contre la cybercriminalité
CNUCTO	Convention des Nations Unies contre la criminalité transnationale organisée
CR	Commission rogatoire
CUA	Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel
DBA	Données de base relatives aux abonnés
DDoS	Déni de service distribué
EJ	Entraide judiciaire
FSC	Fournisseurs de services de communication
HIPCAR	Harmonisation des politiques, législations et procédures réglementaires en matière de TIC
ICMEC	Centre international pour les enfants disparus et exploités
INTERPOL	Organisation internationale de police criminelle
MMS	Service de messagerie multimédia
PE	Protocole d'entente
PPVS	Pays partenaire du Voisinage Sud
SMS	Service d'envoi de messages courts
TIC	Technologies de l'information et des communications
UA	Union africaine
UIT	Union internationale des télécommunications
URL	Localisateur de ressources uniforme

Glossaire

Données de base relatives aux abonnés (DBA)

Les Données de base relatives aux abonnés (DBA) peuvent prendre la forme de données informatiques ou autres, des dossiers et documents par exemple, et inclure des informations qui donnent l'identité d'une personne (par ex. le nom et l'adresse de l'abonné/titulaire du compte). Elles peuvent inclure des informations relatives à l'utilisation d'un service en ligne par une personne, à une date et à une heure spécifiques (par exemple, l'heure de la connexion au compte, la durée d'utilisation de ce service spécifique, etc.). «Abonné» désigne un large éventail de clients de fournisseurs de services: les personnes disposant d'abonnements payants ou de forfaits mais aussi toutes les personnes qui utilisent des services gratuits. Cela comprend également toutes les informations concernant des personnes autorisées à utiliser le compte de l'abonné.[1]

Botnet

Réseau d'ordinateurs infectés par des logiciels malveillants (virus informatiques). Ce type de réseau d'ordinateurs compromis ('zombies') peut être activé pour effectuer certaines actions spécifiques, telles que des attaques de systèmes d'informations (cyberattaques). Ces 'zombies' peuvent être maîtrisés (souvent à l'insu des utilisateurs de ces ordinateurs compromis) par un autre ordinateur. Cet ordinateur de «contrôle» est également connu sous le nom de «Centre de commande et de contrôle».[2]

Fournisseur de services de communication (FSC)

Un fournisseur de services de communication transporte des informations par voie électronique et englobe des sociétés qui offrent des services de télécommunications (avec et sans fil), Internet, câble, satellite et réseaux sociaux.

Système informatique

Désigne un dispositif ou un groupe de dispositifs interconnectés ou associés dont un ou plusieurs exécute(nt), sur la base d'un programme informatique, des traitements ou des enregistrements de données automatiques[3].

1. Paragraphe 177 du rapport explicatif de la Convention de Budapest
2. Notes explicatives du Comité de la Convention sur la cybercriminalité - 1ermars 2017 p. 6
3. Article 1, paragraphe a de la Convention de Budapest

Cryptomonnaie

Actif numérique conçu pour travailler comme moyen d'échange en utilisant la cryptographie pour sécuriser les transactions et contrôler la création d'unités de devise supplémentaires[4].

Cyberintimidation ou cyberharcèlement

L'intimidation ou harcèlement par des moyens de contact électroniques est devenu extrêmement courant, en particulier chez les adolescents.

Web invisible

Le Web invisible représente une petite partie du Web profond, la partie du World Wide Web non indexée par les moteurs de recherche.[5]

Déni de service distribué

Les attaques par déni de service (DoS) consistent à rendre un système informatique indisponible pour les utilisateurs par divers moyens. Cela comprend la saturation des ordinateurs ou réseaux ciblés par des demandes de communication externes, ce qui entrave le service pour les utilisateurs légitimes. Les attaques DDoS sont des attaques par déni de service exécutées par plusieurs ordinateurs en même temps. Il existe actuellement plusieurs moyens courants de mener des attaques DoS et DDoS, par exemple en envoyant des requêtes incorrectes à un système informatique, en dépassant le nombre maximal d'utilisateurs et en envoyant plus d'e-mails sur les serveurs électroniques que ce que le système peut accepter ou traiter[6].

Double incrimination

Ce terme indique que les actes reprochés sont considérés comme une infraction dans l'État requérant mais aussi dans l'État requis. Les éléments des infractions analogues n'ont pas besoin d'être identiques, mais ils doivent être suffisamment proches pour que la conduite soit considérée comme délictuelle dans les deux pays.

4. Andy Greenberg (20avril 2011) Crypto Currency
5. Andy Greenberg (19novembre 2014) Hacker Lexicon: What is the dark web?
6. Notes explicatives du Comité de la Convention sur la cybercriminalité - 1ermars 2017 p. 18

Chiffrement

Désigne le processus de codage d'un message ou d'informations permettant d'autoriser uniquement certaines parties à y accéder (voir également le chiffrement de bout en bout ci-après).

Chiffrement de bout en bout

Le chiffrement de bout en bout (E2EE) est un système de communication où seuls les utilisateurs qui communiquent peuvent lire les messages. L'E2EE a été conçu pour contrer toute tentative de surveillance ou de sabotage car aucun tiers ne peut déchiffrer les données communiquées ou stockées sur les serveurs. Les entreprises telles que WhatsApp par exemple, qui utilisent le chiffrement de bout en bout, ne peuvent pas transmettre le texte des messages de leurs clients aux autorités chargées de l'application de la loi.

Piratage

Violation des systèmes de sécurité permettant d'accéder illégalement à un système informatique.

Hacktaviste

Hacker qui utilise subversivement des ordinateurs et des systèmes informatiques pour défendre une idée politique ou un changement social.

Adresse IP

Une adresse de protocole Internet (adresse IP) est une étiquette numérique attribuée à chaque dispositif (p. ex. un ordinateur, une imprimante) installé sur un réseau informatique qui utilise le protocole Internet à des fins de communication. Une adresse IP présente deux fonctions principales: l'identification de l'interface hôte et du réseau et l'adressage basé sur l'emplacement.

Logiciel d'espionnage

L'enregistrement de frappe, souvent appelé espionnage ou capture de clavier, correspond à l'action d'enregistrer (logging) la frappe sur le clavier, généralement de manière dissimulée, à l'insu de la personne qui utilise le clavier et qui ne sait pas que ses actions sont contrôlées.[7]

Logiciel malveillant

Il existe actuellement de nombreuses formes de logiciels malveillants. Le «logiciel malveillant» a été défini par l'Organisation de développement et de coopération économique comme «un terme général décrivant un logiciel introduit dans un système informatique pour nuire à ce système ou à d'autres systèmes, ou pour le(s) saboter et détourner l'utilisation prévue par ses/leurs propriétaires»[8]. Les formes les plus courantes sont les vers, les virus et les chevaux de Troie. Les formes actuelles de logiciels malveillants peuvent voler des données en les copiant et en les envoyant à une autre adresse, les manipuler et saboter le fonctionnement des systèmes informatiques, notamment ceux qui contrôlent des infrastructures critiques. Les logiciels rançonneurs peuvent éliminer, supprimer ou bloquer l'accès aux données et les logiciels malveillants conçus spécialement peuvent cibler des systèmes informatiques spécifiques[9].

Métadonnées

Données fournissant des informations sur un ou plusieurs aspects des données, par exemple sur:

1. Les moyens de créer les données
2. L'objet des données
3. L'heure et la date de création
4. Le créateur et l'auteur des données
5. L'emplacement d'un réseau informatique où les données ont été créées
6. Les normes utilisées (c.-à-d. les critères techniques et d'ingénierie, les méthodes, les processus et les pratiques uniformes)

Hameçonnage

Tentative d'obtention d'informations sensibles telles que des noms d'utilisateur, des mots de passe et des informations sur les cartes de crédit (et indirectement des informations financières), souvent dans une

7. «*Keylogger*» Dictionnaires Oxford
8. http://www.oecd.org/internet/ieconomy/40724457.pdf
9. Notes explicatives du Comité de la Convention sur la cybercriminalité - 1ermars 2017 p. 22

intention malveillante, en se faisant passer pour une entité digne de confiance dans le cadre d'une communication électronique[10].

Logiciel rançonneur

Type de logiciel malveillant bloquant l'accès aux données de la victime ou menaçant de les publier ou de les supprimer jusqu'à ce qu'une rançon soit versée.

Réciprocité

Également connue sous le terme «mutualité», «réciprocité» signifie dans ce contexte que l'État requis reconnaît les mêmes procédures d'enquête et pénales que celles pouvant être utilisées par l'État requérant.

Sextage

Envoi, réception ou transfert de messages, de photos ou d'images sexuellement explicites.

Spam

Envoi de courrier indésirable en masse permettant d'envoyer un message à un grand nombre d'adresses électroniques. L'identité du destinataire est sans intérêt parce que le message vise indifféremment de nombreux autres destinataires sans distinction[11].

Harponnage

Le harponnage vise des individus ou des entreprises spécifiques - Cette technique est de loin la plus prospère aujourd'hui sur Internet, représentant 91% des attaques[12].

10. *Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.*
11. Notes explicatives du Comité de la Convention sur la cybercriminalité - 1ermars 2017 p. 24
12. Debbie *Stephenson (27juillet 2014) Spear Phishing: Who's Getting Caught?*

TOR

Logiciel gratuit permettant d'activer la communication anonyme – Le nom est dérivé de l'acronyme du projet d'origine du logiciel «The Onion Router»[13].

Données liées au trafic

Il s'agit d'informations comprenant les registres identifiant les personnes avec lesquelles un abonné a communiqué, les sites Internet qu'il a visités et les informations similaires à propos de l'activité en ligne d'un utilisateur.

Localisateur de ressources uniforme (URL)

Une URL est un identificateur de ressources uniforme: il s'agit du terme générique utilisé pour tous les types de noms et adresses se rapportant à des objets sur le World Wide Web.

13. Projet TOR: FAQ www.torproject.org

Introduction

Le cybercrime, ou criminalité informatique, est un crime impliquant un ordinateur et un réseau.[14]Un ordinateur peut avoir été utilisé pour commettre un crime, ou en être la cible.[15] Le réseau sera composé d'au moins deux systèmes informatiques[16] et peut être un réseau local ou un réseau plus étendu.

La cybercriminalité est un phénomène mondial qui résulte du nombre croissant de dispositifs TIC connectés à Internet. En 2016, on a estimé que le coût de la cybercriminalité pourrait atteindre 2100milliards de dollars US d'ici à 2019.[17] Jusqu'à 80% des actes de cybercriminalité semblent être associés à une certaine forme de crime organisé, avec des marchés noirs de cybercriminalité établis, des infections informatiques, la gestion de botnets, la récupération de données financières et personnelles, la vente de données et le 'retrait' d'informations financières.[18] Le 12mai2017, l'attaque du logiciel rançonneur Wannacry a prouvé l'impact mondial de la cybercriminalité. On estime à 200000 le nombre d'ordinateurs touchés dans 150pays.

La forte augmentation de la cybercriminalité est principalement due au fait qu'Internet crée de grandes opportunités pour les criminels organisés d'accumuler des bénéfices considérables par le biais de projets frauduleux. L'approche traditionnelle de l'arrestation d'un suspect, de l'obtention d'une admission, de l'inculpation et de la présentation au tribunal est obsolète. Avec la cybercriminalité, le suspect peut se trouver hors de la juridiction. Il conviendra donc d'examiner la recevabilité des preuves obtenues via des techniques spéciales d'enquête,[19] la ou les infraction/s à sanctionner, l'entraide judiciaire, l'extradition et les rapports d'expert. Ces recherches prennent du temps, sont complexes et coûteuses.Les cybercriminels profitent du fait que la loi pénale ne soit pas adaptée à l'environnement en ligne et que les agents de la force publique soient mal équipés et ne disposent pas des outils nécessaires pour enquêter correctement. Cet article examine le contexte de la cybercriminalité dans les Pays partenaires du Voisinage Sud (PPVS) et, en se fondant sur l'identification des lacunes juridiques, émet des recommandations en vue d'améliorer les cadres juridiques, les procédures de recherche et la coopération internationale.

Cybercriminalité dans les PPVS

Un examen de la cybercriminalité dans la région MENA en 2012[20] a permis d'identifier les principaux défis à relever:

1. **Responsabilité:** Aucune agence gouvernementale en particulier n'est chargée de rédiger ou de mettre à jour les lois en matière de cybercriminalité.

14. R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime
15. Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials
16. c.-à-d. un ordinateur opérationnel et complet. Les systèmes informatiques comprendront l'ordinateur ainsi que les logiciels et périphériques nécessaires à son fonctionnement http://www.webopedia.com/TERM/C/computer_system.html
17. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
18. ibid
19. L'article 20 de la Convention des Nations Unies contre la criminalité transnationale organisée (CNUCTO) fait référence aux techniques d'enquête spéciales, notamment «la surveillance électronique ou d'autres formes de surveillance et les opérations d'infiltration».
20. Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East

2. **Législation:** Non existante ou mal rédigée, elle ne tient pas compte de l'aspect international et des outils d'enquête spécifiques nécessaires.
3. **Capacités techniques:** Les autorités chargées de l'application de la loi comprennent mal l'intérêt de garantir l'intégrité des preuves en matière de cybercriminalité.
4. **Structure organisationnelle:** Il manque une agence dédiée à la mise en place de stratégies en matière de cybercriminalité et de développement pour l'avancée technologique.

   Éducation: Peu de campagnes sensibilisent à la prévalence de la cybercriminalité ou à la formation des forces de l'ordre afin de garantir qu'ils connaissent les tendances et menaces actuelles.

Certains PPVS ont relevé ces défis:

1. Israël dispose d'une Équipe nationale de préparation aux cyberévénements (CERT) (qui fait partie de l'Autorité nationale de cyberdéfense). Le pays a adhéré à la Convention de Budapest et dispose de lois spécifiques à la cybercriminalité (loi informatique de 1995).
2. Le Ministère public palestinien a défini une unité spécialisée en février 2017 et la Police palestinienne compte un service de repérage électronique de la cybercriminalité.
3. L'Égypte dispose d'un service de lutte contre les crimes informatiques et liés aux réseaux pour lutter contre les cyber-menaces.
4. La Jordanie a récemment mis sa législation à jour avec la loi sur la cybercriminalité n°27 de 2015.
5. L'Algérie dispose d'une agence gouvernementale, l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication établi par le Décret présidentiel n°15-261 du 8 octobre 2015 (Jour officiel 53 de l'année 2015). L'organe est responsable, inter alia, de proposer une stratégie nationale pour la prévention et la lutte contre les infractions liées aux technologies de l'information et de la communication et de participer à la mise à jour des standards juridiques en la matière.

Cyber-menaces

Un rapport sur les menaces liées à la cybercriminalité dans la région MENA dressé en 2014 a identifié que la plupart des cyberattaques visant les infrastructures TIC étaient le DDoS ou la dégradation des sites Web.[21] Le rapport souligne également la vulnérabilité aux cyberattaques à cause du manque de réglementation et de cadres légaux appropriés.[22] Par ailleurs, l'Afrique est un continent souvent considéré comme un lieu sûr pour les cybercriminels.[23]

Les défis à relever sont de plus en plus importants lorsque l'on sait que 55% des foyers interrogés dans le cadre du Rapport sur les médias sociaux dans le monde arabe (Arab Social Media Report) disposent de 2 à 5dispositifs connectés à Internet (autres que des ordinateurs de bureau et portables) et que 25% disposent de 6 à 10 dispositifs connectés à Internet.[24]

21. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
22. Ibid.
23. Eric Tamarkin, (20 January 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73
24. Arab Social Media Report 2017 www.arabsocialmediareport.com

Les États arabes comptaient 161millions d'utilisateurs Internet en 2016[25] et depuis le Printemps arabe, l'utilisation des réseaux sociaux a considérablement augmenté. Facebook compte 156millions d'utilisateurs, soit une augmentation de plus de 40millions depuis l'année dernière.[26] Les utilisateurs de Facebook ont augmenté de plus de 14millions en Égypte, de 9,3millions en Algérie et de 5,5millions au Maroc.[27] L'utilisation de Twitter est importante, avec 152millions de tweets par mois en Égypte et 71millions en Algérie.[28] Cette plus forte utilisation des réseaux sociaux favorise[29] l'usurpation d'identité, la cyberintimidation, le sextage et la radicalisation.[30] Les réseaux sociaux ont également fortement favorisé le financement du terrorisme, le recrutement, la propagande et l'utilisation de sources d'informations ouvertes[31] pour les attaques.

Dimensions internationales de la cybercriminalité

Pour enquêter sur la criminalité et pouvoir entamer des poursuites, une coopération étroite entre les États est requise. L'actuel système d'entraide judiciaire (EJ) peut être complexe et bureaucratique, entraînant des retards dans l'obtention des preuves. Cela n'est pas adapté à la nature rapide de la cybercriminalité, où Internet n'a pas de frontières. Par ailleurs, des problèmes juridictionnels ont été soulevés par l'informatique en nuage, nécessitant un examen attentif lorsque des demandes d'EJ sont envoyées à pour exécution.[32] La mise en place de procédures permettant d'obtenir des réponses rapides aux situations d'urgence, la conservation des preuves, ainsi que les demandes de coopération internationale, sont essentielles.[33]

25. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
26. Ibid p. 33
27. Ibid p. 37
28. Ibid p. 48
29. https://www.internetmatters.org/issues/
30. http://www.independent.co.uk/news/world/middle-east/what-makes-people-join-isis-expert-says-foreign-fighters-are-almost-never-recruited-at-mosque-a6748251.html
31. http://www.bbc.co.uk/news/world-middle-east-18532839
32. Dans le cadre d'un mandat de perquisition visant à examiner une messagerie électronique contrôlée et entretenue par Microsoft Corporation U.S., la Cour d'appel (deuxième instance) 14-2985 a décidé que le mandat de dépôt délivré pour examiner le contenu de la messagerie aux États-Unis ne s'appliquait pas parce que les données étaient stockées au niveau international et que le Ministère de la Justice devait se rapprocher du Gouvernement irlandais par le biais d'un traité d'entraide judiciaire existant pour accéder aux données.
33. Comprendre la cybercriminalité: Phénomène, difficultés et réponses juridiques (UIT) page 3

Méthodologie

les difficultés juridiques, techniques et institutionnelles posées par la cybercriminalité sont mondiales et peuvent être surmontées uniquement par la mise en place d'une stratégie cohérente, en tenant compte du rôle des différents acteurs et initiatives existantes,[34] dans un contexte de coopération internationale.[35] Cet article sera centré sur le cadre législatif et la coopération internationale, en conformité avec les normes internationales,[36] pour lutter contre la cybercriminalité dans les PPVS.

Cet article fournit une analyse juridique et une analyse des écarts en matière de cybercriminalité dans les PPVS, sur la base des éléments suivants:

1. Réponses à un questionnaire sur la cybercriminalité envoyé à chaque PPVS
2. Présentations des PPVS lors des sessions du CrimEx à Maastricht le 8 mai 2017
3. Recherche par des consultants scientifiques basée dans chaque PPVS
4. Recherches menées à partir de ressources en ligne[37]

Analyse juridique

Cet article a examiné la législation de chaque PPVS et la ratification des conventions régionales et internationales[38] portant sur la cybercriminalité et portera sur trois questions:

1. **Infractions:** Aux fins de cet article, les infractions suivantes seront examinées:

    a. Les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données ou systèmes informatiques

        – L'accès illégal à un système informatique
        – L'accès illégal, l'interception ou l'acquisition de données informatiques
        – L'atteinte à l'intégrité d'un système ou de données informatiques
        – La production, la distribution ou la détention d'outils informatiques utilisés à mauvais escient
        – La violation de mesures de protection de la confidentialité et des données

    b. Les actes de fraude informatique à des fins de profit ou de préjudice personnel ou financier

34. Voir les initiatives internationales ci-après.
35. Programme mondial cybersécurité de l'UIT/Groupe d'experts de haut niveau, Rapport stratégique mondial, 2008, page 14, disponible à l'adresse: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
36. Résolution adoptée par l'Assemblée générale des Nations Unies sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information, A/RES/64/211.
37. Cela comprend le Sherloc des Nations Unies et d'autres ressources et textes disponibles en ligne (voir la bibliographie).
38. La Convention de Budapest sur la cybercriminalité du Conseil de l'Europe, la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel et la Convention arabe pour la lutte contre la cybercriminalité

- La fraude ou la falsification informatique
- L'usurpation d'identité informatique
- Les infractions liées aux atteintes à la propriété intellectuelle ou aux marques dans le domaine informatique
- Les actes informatiques entraînant un préjudice personnel
- La sollicitation ou la manipulation psychologique des enfants par voie informatique

c. Les actes liés à des contenus informatiques

- Les actes informatiques impliquant des discours de haine
- La production, la distribution ou la détention informatique de pornographie enfantine
- Les actes informatiques soutenant le terrorisme

2. **Procédure:** Les autorités chargées de l'application de la loi ont besoin de pouvoir disposer des pouvoirs nécessaires à la lutte contre la cybercriminalité. Ces enquêtes peuvent s'avérer complexes et sophistiquées car les malfaiteurs ont recours à des techniques pour masquer leur identité. Ces défis signifient que les outils requis par les enquêteurs doivent être différents de ceux utilisés pour enquêter sur les crimes violents et acquisitifs classiques. Les procédures législatives actuelles permettant d'enquêter sur la cybercriminalité seront examinées.
3. **Coopération internationale:** La cybercriminalité peut couvrir de multiples juridictions, les malfaiteurs et les victimes peuvent provenir de différents États et les preuves peuvent être localisées avec les Fournisseurs de services de communication (FSC). Les processus permettant de conserver les contenus, de divulguer des données de trafic et de les intercepter en temps réel à des fins d'enquêtes transfrontalières, grâce à l'entraide judiciaire, seront examinés.

Analyse des écarts

Lorsque des lacunes auront été identifiées lors de l'analyse juridique, elles seront examinées sur la base de la Convention de Budapest sur la cybercriminalité, de la Convention arabe pour la lutte contre la cybercriminalité, de la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel et d'autres précédents tels que les modèles de lignes directrices politiques et de textes législatifs de l'HIPCAR ainsi que la législation type sur la pornographie enfantine et l'étude mondiale du Centre international pour les enfants disparus et exploités (ICMEC) (8ème édition 2016).

L'existence dans les code pénal ou criminel de dispositions relatives aux infractions substantielles telles que la fraude, ne signifie pas qu'elles soient applicables aux actes commis sur Internet. L'analyse des lois nationales actuelles a permis d'identifier les lacunes et d'émettre des recommandations concernant la législation existante dans la section Infractions.

Les recommandations permettant de mener des enquêtes nationales efficientes et efficaces, d'engager des poursuites et de réaliser des essais sont incluses dans la section Procédure.

Pour améliorer les enquêtes transfrontalières, des recommandations ont été émises dans la section Coopération internationale. Ces recommandations sont émises pour soutenir l'entraide judiciaire entre les PPVS et entre les PPVS et les États membres de l'Union européenne.

Il s'agit de simples suggestions de recommandations et les PPVS devront déterminer leur viabilité sur la base des ressources et priorités. La cybercriminalité évolue en permanence et les menaces augmentent car la société dépend de plus en plus de l'utilisation des technologies de l'information pour tous les aspects de la vie quotidienne. Le défi sur le plan législatif sera de répondre à ces risques accrus et d'équiper les autorités chargées de l'application de la loi des outils nécessaires pour enquêter et engager des poursuites.

Contexte

Approches internationales

Plusieurs organisations internationales travaillent en permanence sur l'analyse des développements les plus récents en matière de cybercriminalité:

Conseil de l'Europe

En 1996, le Comité européen pour les problèmes criminels a établi un comité d'experts[39] qui a rédigé, entre 1997 et 2000, une Convention sur la cybercriminalité. Ce comité est devenu la Convention de Budapest sur la cybercriminalité[40] et constitue le premier traité international sur les crimes commis via Internet et autres réseaux informatiques, qui gère en particulier les infractions liées aux atteintes à la propriété intellectuelle, à la fraude informatique, à la pornographie enfantine et aux violations de la sécurité des réseaux. Elle prévoit aussi une série de pouvoirs et procédures tels que la perquisition et l'interception de réseaux informatiques.[41] Son principal objectif, défini dans le préambule, est de mener une politique commune en matière criminelle visant à protéger la société contre la cybercriminalité, notamment en adoptant une législation appropriée et en encourageant la coopération internationale. Depuis mai 2017, 55 États ont ratifié la convention, quatre autres l'ont signée mais sans la ratifier[42]

La Convention est soutenue par des organisations internationales, telles qu'Interpol.[43] Bien que l'impact de la Convention de Budapest ait été remis en question[44] – seuls sept États hors du Conseil de l'Europe l'ont ratifiée[45] et en raison des limites de son application à l'environnement changeant de la cybercriminalité, par exemple l'interception de la voix sur IP (VoIP) – la recevabilité des preuves numériques[46] et les procédures pour traiter l'utilisation émergente de la technologie du chiffrement et des moyens de communication anonyme sont autant de problèmes. La Convention n'a pas été modifiée, à l'exception du premier protocole additionnel. [47]

39. Rapport explicatif de la Convention sur la cybercriminalité (185), n°10
40. Le texte complet de la Convention 185 (Convention sur la cybercriminalité), le premier protocole additionnel et la liste des signatures et ratifications sont disponibles à l'adresse suivante: www.coe.int
41. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
42. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Sv9dObc4
43. Interpol a souligné l'importance de la Convention sur la cybercriminalité dans la résolution de la 6è Conférence internationale sur la cybercriminalité du Caire: «*La Convention sur la cybercriminalité du Conseil de l'Europe sera recommandée comme norme procédurale et juridique internationale minimum pour lutter contre la cybercriminalité. Les pays seront invités à y adhérer. La Convention sera distribuée à tous les pays membres d'Interpol dans les quatre langues officielles*», disponible en anglais à l'adresse suivante: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp
44. Pour plus d'informations sur les réalisations et les lacunes, consulter l'ouvrage: Gercke, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et suivantes.
45. Australie (2013), Canada (2015), Chili (2017), Israël (2016), Japon (2012), Sri Lanka (2015) et États-Unis (2007). Parmi les PPVS, le Maroc a également été invité à y adhérer.
46. Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.
47. Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, ETS n°189, disponible à l'adresse suivante: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7836079 29 États sont parties et 13 l'ont signé, San Marino étant le dernier à l'avoir signé, le 19mai2017 https://www.coe.int/en/web/cybercrime/-/signature-san-marino-of-the-protocol-on-xenophobia-and-racism-

L'un des aspects fondamentaux de la Convention de Budapest est la mise en place d'un réseau 24h/24, 7j/7[48] afin de permettre des enquêtes efficaces et la conservation des preuves.[49] Deux études menées en 2008[50] et 2009[51] ont révélé que les Etats qui avaient ratifié la Convention devaient encore établir des points de contact, alors qu'il s'agit d'une condition obligatoire. Certains États peuvent rencontrer des difficultés à disposer d'un interlocuteur unique (SPOC) disponible à tout moment alors que l'investissement dans les enquêtes sur la cybercriminalité est minime. Malgré tout, étant donné la vitesse de développement de la cybercriminalité, l'interlocuteur unique constitue un élément essentiel d'un cadre international efficace.

Union africaine

Il a été décidé au cours de la conférence extraordinaire des ministres de l'Union africaine chargés des TIC, qui s'est tenue à Johannesburg en 2009, que la Commission de l'Union africaine devait, en collaboration avec la Commission économique des Nations Unies pour l'Afrique, développer un cadre juridique pour les pays africains qui porte sur les transactions électroniques, la cybersécurité et la protection des données.[52]

L'Union africaine (UA) a présenté le projet de Convention de l'Union africaine sur la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique en 2011.[53] En juillet 2014, l'UA a adopté la Convention sur la cybersécurité et la protection des données (CUA). Mi-2016, seulement 12 des 54pays africains avaient mis en place des dispositions en matière de droit matériel et procédural sur la cybercriminalité et les preuves électroniques. D'autres étaient en train de rédiger une législation en suivant le modèle des Conventions de l'Union africaine et de Budapest.

Une étude comparative de la CUA indique qu'elle criminalise certains comportements prévus dans la Convention de Budapest, mais pas tous. La plupart des infractions dans le cadre de la CUA manquent d'éléments prouvant l'intention criminelle et peuvent criminaliser le comportement légitime des autorités chargées de l'application de la loi et tout comportement légal en vertu des Bonnes pratiques internationales.[54] De plus, la CUA ne prévoit pas l'ensemble des pouvoirs procéduraux d'enquête, de poursuite de la cybercriminalité et d'obtention de preuves électroniques dans les enquêtes nationales: les ordonnances de production par exemple, qui sont essentielles pour obtenir des données des PPVS, ne sont pas incluses.[55] De plus, la CUA ne constitue pas une base légale pour la coopération internationale sur la cybercriminalité et les preuves électroniques.[56]

48. Article 35
49. Voir le Rapport explicatif de la Convention sur la cybercriminalité n°298
50. Verdelho (2008) The effectiveness of international cooperation against cybercrime
51. The Functioning of 24/7 points of contact for cybercrime, 2009
52. Pour plus d'informations, consulter la Déclaration d'Oliver Tambo, Union africaine, Johannesburg 2009, disponible à l'adresse suivante: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf
53. Le projet de Convention est disponible à l'adresse suivante: www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf
54. Étude comparative de la Convention de l'Union africaine de Malabo et de la Convention de Budapest sur la cybercriminalité du 20 novembre 2016
55. Ibid
56. Ibid

Ligue des États arabes et Conseil de coopération du Golfe

La Convention arabe pour la lutte contre la cybercriminalité («CITO») a été adoptée en décembre 2010 et est entrée en vigueur en février 2014. À ce jour, la Jordanie, les Émirats arabes unis, le Soudan, l'Irak, la Palestine, le Qatar, le Koweït et l'Égypte ont ratifié la CITO. La principale obligation de la CITO vise à mettre en œuvre la législation nationale pour criminaliser et les pouvoirs de procédure pour enquêter sur la cybercriminalité.

Comme indiqué ci-dessus, l'intention criminelle ne figure pas dans la CUA et la CITO pour certaines infractions. Par exemple les articles 6, 8,[57] 9[58] ne font pas référence à la notion de «*sans droit*».[59] L'article 6 criminalise l'«*accès illégal*» mais n'en donne pas de définition. La CITO ne comprend pas d'infraction de l'atteinte à l'intégrité du système,[60] qui vise à incriminer l'entrave intentionnelle à l'usage légitime de systèmes informatiques, y compris de systèmes de télécommunications, en utilisant ou en influençant des données informatiques.

En ce qui concerne la coopération internationale, l'article 34[61] fournit à la CITO la base de l'entraide judiciaire et l'article 31[62] la base de l'extradition s'il n'existe pas de traité bilatéral applicable. La double incrimination est une condition essentielle à la fourniture d'une entraide judiciaire en vertu de l'Article 32, paragraphe 5. Ceci est contraire aux normes internationales dans lesquelles la double incrimination propose une définition plus large de l'EJ[63] et où elle n'est pas requise en vertu de la Convention de Budapest[64] pour des pouvoirs moins intrusifs afin de garantir que les preuves de cybercriminalité sont conservées.

D'autres dispositions internationales importantes incluent la divulgation d'informations en vertu de l'article 33[65] par les autorités chargées de l'application de la loi à une autre partie de la CITO et qui peuvent être utilisées de façon proactive par un état receveur et en respectant la confidentialité associée à toute demande d'EJ.[66] Une disposition de l'article 43 indique «…*l'existence d'un réseau spécialisé et joignable vingt-quatre heures sur vingt-quatre heures, afin d'assurer une assistance immédiate aux fins d'enquêtes ou procédures concernant les infractions liées à des systèmes informatiques ou pour recueillir les preuves sous forme électronique d'une infraction spécifiée.*»[67]

La CITO n'inclut pas de disposition pour la récupération de données ou de contenus de trafic en temps réel par le biais de l'EJ.[68] Cela pourrait entraver les enquêtes internationales dans le cadre desquelles la récupération de l'adresse IP ou le contenu en temps réel peut révéler l'emplacement des malfaiteurs afin d'empêcher les cybercrimes. Cette lacune peut être comblée par l'adoption de l'article 34 de la Convention de Budapest.

57. Atteinte à l'intégrité des données: semblable à l'article 4 de la Convention de Budapest
58. Infraction ciblant l'utilisation abusive des technologies de l'information: semblable à l'article 6 de la Convention de Budapest sur l'Abus de dispositifs
59. L'article 2 de la Convention de Budapest fait allusion à un accès «sans droit» ou non autorisé, ce qui signifie que l'infraction serait une responsabilité sans faute et pourrait signifier que toute personne, qu'il s'agisse d'un agent de police ou toute autre personne qui accède aux données sans consentement commet une infraction.
60. Voir l'article 5 de la Convention de Budapest
61. Conforme à l'article 23 de la Convention de Budapest
62. Conforme à l'article 24 de la Convention de Budapest
63. Voir l'article 18, paragraphe 9, de la CNUCTO
64. Par exemple, l'article 29, paragraphe 3, pour la conservation des données informatiques enregistrées
65. Conforme à l'article 26 de la Convention de Budapest
66. L'article 34, paragraphe 7 et l'article 36 de la CITO sont conformes à l'article 28 de la Convention de Budapest
67. On ne sait pas si les PPVS qui ont ratifié la CITO (Jordanie, Palestine et Égypte) ont établi ce *réseau spécialisé*.
68. Voir les articles 33 et 34 de la Convention de Budapest

HIPCAR

L'amélioration de la compétitivité dans les Caraïbes par l'Harmonisation des politiques, législation et procédures réglementaires en matière de TIC a proposé une législation type en matière de cybercriminalité à 15 pays caribéens du Groupe des États d'Afrique, des Caraïbes et du Pacifique (ACP).[69] Le projet a été géré par l'Union internationale des télécommunications (UIT) et un comité de direction mondial composé de représentants de la Commission européenne. Les modèles de textes législatifs ont été rédigés après l'analyse juridique de la législation nationale, des Bonnes pratiques internationales des NU, de l'OCDE, de l'UE et de la législation du R.-U., de l'Australie, de Malte et du Brésil comme points de repère. Même si le modèle de texte législatif a été rédigé en tenant compte des besoins spécifiques des petits États insulaires, il constitue un guide utile pour les États qui disposent d'une législation limitée ou inexistante en matière de cybercriminalité.

ICMEC

La 8è édition de l'examen de la législation type à l'échelle mondiale de l'ICMEC[70] de 2016 prévoit un ensemble de critères qui permettront de procéder à une analyse juridique afin de confirmer:

1. S'il existe une législation nationale spécifique à la pornographie enfantine;
2. Si la législation nationale fournit une définition de la pornographie enfantine;
3. Si la législation nationale criminalise les délits informatiques;
4. Si la législation nationale criminalise la détention, en connaissance de cause, de pornographie enfantine, avec l'intention ou non de la distribuer; et
5. Si la législation nationale exige des PPVS qu'ils signalent tout soupçon de pornographie enfantine aux autorités chargées de l'application de la loi ou à d'autres autorités policières mandatées.

69. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf
70. https://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

Analyse juridique et analyse des écarts

Cette section offre une analyse juridique des lois nationales actuellement en vigueur et une analyse des écarts avec des recommandations émises pour chaque PPVS.[71]

Algérie

L'Algérie a ratifié la la Convention arabe pour la lutte contre la cybercriminalité (CITO).

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[72] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.	**Code pénal– 05-09-2009**[73] **Article 394 bis** (...) quiconque accède ou se maintient, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ou tente de le faire.	**Analyse juridique** La disposition nationale indique *«frauduleusement»*, ce qui semble suggérer que l'auteur a accédé aux données de façon malhonnête (alors que la CB utilise l'expression «sans droit» pour parler d'accès non autorisé). La CB évoque *«l'intention malhonnête»*, mais il s'agit du mens rea (intention criminelle) qui vise à obtenir les données, plutôt que l'acte illégal en lui-même. Actuellement, cette infraction nationale peut être commise uniquement si l'auteur affiche une intention malhonnête. En l'absence de définition du terme *«frauduleusement»*, on ne sait pas si cela exige un acte manifeste ou si chaque accès illégal est considéré comme frauduleux. Une définition du terme *«frauduleux»* s'avère donc nécessaire.

71. Pour obtenir un aperçu de la législation liée à la cybercriminalité dans les États membres et sa conformité avec les meilleures pratiques définies par la Convention sur la cybercriminalité, consulter les profils des pays disponibles sur le site Internet du Conseil de l'Europe, à l'adresse suivante: www.coe.int/cybercrime/
72. Article 6 de la CITO et article 29, paragraphe 1, de la CUA
73. https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 4 de l'HIPCAR – Accès illégal 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête. **Article5 de l'HIPCAR – Présence illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.		Le terme «système informatique» est défini à l'article 1 de la Loi 09-04 du 05-08-2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux TICs. L'infraction fait également référence à un «système de traitement automatisé de données», sans définir ce dernier. On ne sait pas si elle concerne également un «système informatique». La CITO, quant à elle, fait référence à «l'accès ou le maintien illégal et tout contact avec», sans définir ce que ces actes signifient. Le recours à la CB et à l'HIPCAR devrait donc être privilégié. **Analyse des écarts** **Recommandation:** La législation nationale pourrait inclure les programmes dans la définition des données, dans la mesure où certaines données incluent des programmes et d'autres non. En outre, pour faire preuve de cohérence par rapport à la CB/l'HIPCAR, il conviendrait d'évoquer un accès «sans droit» plutôt que «frauduleusement».

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[74] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. **Article6 de l'HIPCAR – Interception illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques: – toute transmission non publique vers, de, ou au sein d'un système informatique; ou – des émissions électromagnétiques provenant d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	La loi n°18-04 du 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électronique a introduit l'incrimination de la violation du secret des correspondancesémises par voie de communication électronique , l'article 164 de cette loi stipule « est punie d'un emprisonnement d'une année à cinq ans et une amende de 500.000 à 1.000.000 DA ,toute personne qui viole le secret des correspondances transmises par voie de poste ou par voie de communications électroniques ou divulgue leur contenu ou le publie ou l'utilise sans l'autorisation de l'expéditeur ou du destinataire ou révèle leur existence. ».	**Analyse juridique** Cette infraction est essentielle pour poursuivre en justice des transmissions non publiques de données informatisées en direction ou en provenance d'un système informatique qui pourraient avoir été interceptées de façon illégale afin d'obtenir des informations concernant la localisation d'une personne (pour viser cette personne par exemple).[75] **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 3 de la CB et de l'article 6 de l'HIPCAR comme guide (la terminologie de l'article 7 de la CITO convient également même s'il n'existe pas de définition des «*données informatiques*»).

74. Article 29, paragraphe 2, de la CUA
75. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut imposer que l'infraction soit commise avec une intention malhonnête ou en rapport avec un système informatique connecté à un autre système informatique ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique. **Article 7 de la CITO** **Interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques.		
Article 4 de la CB[76] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux. **Article7 de l'HIPCAR – Atteinte à l'intégrité des données** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants:	**Code pénal– 05-09-2009[77]** **Article 394c** (...) quiconque volontairement et frauduleusement: 1. conçoit, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique, et par lesquelles les infractions prévues par la présente section peuvent être commises, 2. détient, révèle, divulgue, ou fait un usage quelconque des données obtenues par l'une des infractions prévues par la présente section.	**Analyse juridique** L'utilisation du terme «frauduleusement» n'est pas cohérente (rentre en conflit) avec la règle posée par l'article 4, paragraphe 1, de la CB, c'est-à-dire «(...) le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques» (ou l'article 7 de l'HIPCAR) qui n'exige pas la preuve de l'existence d'une fraude. Cela signifie que le comportement qui constitue une atteinte à l'intégrité des données en vertu de l'article 4, paragraphe 1, de la CB (ou de l'article 7 de l'HIPCAR) ne serait pas criminalisé selon l'art. 394c. Ce dernier article n'englobe pas la suppression de données informatiques. **Analyse des écarts** **Recommandation:** Utiliser l'article 4 de la CB ou l'article 7 de l'HIPCAR comme guide pour la législation nationale.

76. Article 29, paragraphe 1, sous e) à f), de la CUA
77. https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes; • obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Article 8 de la CITO** **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 5 de la CB[78] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. **Article9 de l'HIPCAR – Atteinte à l'intégrité du système** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: • entrave ou porte atteinte au fonctionnement d'un système informatique; ou • entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Pas d'équivalent**	**Analyse juridique** Cette infraction contribuerait à lutter contre les programmes malveillants qui perturbent le fonctionnement d'un ordinateur (par exemple, les vers informatiques) ou les sous-groupes de programmes malveillants (comme les virus informatiques). Il s'agit de programmes informatiques auto-répliquants qui nuisent au réseau en lançant de multiples processus de transfert de données. Ils peuvent affecter les systèmes informatiques en entravant leur bon fonctionnement, en utilisant des ressources du système pour se reproduire sur Internet ou en générant du trafic sur le réseau susceptible d'interrompre la disponibilité de certains services (tels que des sites Internet). **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 5 de la CB ou de l'article 9 de l'HIPCAR comme guide pour la législation nationale. Examiner également si la prévention et la poursuite en justice des attaques contre des infrastructures critiques nécessitent l'instauration d'une autre infraction séparée ou aggravée (article 9, paragraphe 2, de l'HIPCAR), comme, par exemple, le fonctionnement d'un système informatique qui serait entravé à des fins terroristes (p. ex. l'entrave au système qui enregistre des registres de bourse et peut les rendre inexacts, ou l'entrave au fonctionnement des infrastructures critiques)).[79]

78. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
79. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		
Article 6 de la CB[80] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Pas d'équivalent**	**Analyse juridique** De la même façon que pour l'Accès illégal, la disposition n'utilise pas l'expression «sans droit». Cette infraction permettra de poursuivre en justice la production, la vente ou l'acquisition à des fins d'utilisation, ainsi que l'importation ou la distribution de codes d'accès et d'autres données informatiques utilisées pour commettre des cybercrimes. Il est par exemple possible d'accéder à un système informatique pour faciliter une attaque terroriste, en perturbant le réseau de distribution électrique d'un pays. L'infraction tiendra également compte des dispositifs qui présentent un intérêt légitime tout en étant utilisés à des fins criminelles («double usage»). Cela inclura la terminologie «principalement adapté» utilisée dans la CB.

80. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 6 de la CB ou de l'article 10 de l'HIPCAR comme guide pour la législation nationale. Il convient de noter que l'HIPCAR prévoit la possibilité de répertorier les dispositifs dans une annexe, si cela est jugé opportun. Une telle disposition pourrait s'avérer restrictive et exiger des mises à jour au fur et à mesure des progrès technologiques. La loi nationale devrait prévoir une excuse raisonnable, afin que les autorités chargées de l'application de la loi puissent utiliser des dispositifs pour les techniques d'enquête particulières (la terminologie de l'article 6, paragraphe 2 de la CB ou de l'article 10, paragraphe 2, de l'HIPCAR pourrait être utilisée comme guide).

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article10 de l'HIPCAR – Dispositifs illégaux 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Pas d'équivalent**	**Analyse juridique** L'incorporation de l'article 7 de la CB, de l'article 11 de l'HIPCAR ou de l'article 29, paragraphe 2, sous b) de la CUA, est conseillée pour lutter contre ce délit qui peut comprendre le hameçonnage et le harponnage. Par exemple, les données informatiques (telles que celles utilisées dans les passeports électroniques) peuvent être introduites, altérées, effacées ou supprimées dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.[81] L'article 11, paragraphe 2, de l'HIPCAR considère aussi l'envoi de plusieurs messages électroniques comme un délit aggravé.

81. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article11 de l'HIPCAR – Falsification informatique 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux. **Article 10 de la CITO** **Infraction de falsification** Utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques.		La terminologie utilisée à l'article 10 de la CITO ne fait pas référence à une intention malhonnête et requiert qu'un préjudice soit causé. La terminologie utilisée dans la CB et l'HIPCAR doit être privilégiée car elle ne requiert pas de préjudice. La CB et l'HIPCAR exigent uniquement la «*prise en compte*» des «*données non authentiques*». **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 7 de la CB, de l'article 11 de l'HIPCAR ou de l'article 29, paragraphe 2, sous b) de la CUA comme guide pour la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 29, paragraphe 2, sous b), de la CUA (...) 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. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.		
Article 8 de la CB[82] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes:	**Code pénal– 05-09-2009** **Article 394 ter** (...) quiconque introduit frauduleusement des données dans un système de traitement automatisé ou supprime ou modifie frauduleusement les données qu'il contient.	**Analyse juridique** Alors que le terme «*frauduleusement*» de l'article 394 de la législation nationale accorde un certain niveau de protection, la notion de commission de cette conduite sans autorisation fait défaut, ce qui peut semer la confusion. Le terme «*données informatiques*» est défini à l'article 1 de la Loi 09-04 du 05-08-2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux TICs. Il n'existe pas de définition du terme «*système de traitement automatisé de données*», ce qui peut créer de l'incertitude. La terminologie utilisée à l'article 11 de la CITO et à l'article 29, paragraphe 2, sous d) de la CUA, est floue. Elle ne renvoie à aucune intention malhonnête et requiert une certaine forme de «*préjudice*» (CITO) ou de «*bénéfice*» (CUA) sans définir ce dont il s'agit.

82. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse des écarts** **Recommandation:** Définir le terme *«système de traitement automatisé des données»* et inclure *«sans autorisation».* La terminologie utilisée par la CB ou par l'HIPCAR concernant cette infraction constitue un bon guide pour la législation nationale.
Article 9 de la CB[83] **Infractions se rapportant à la pornographie enfantine** **AJOUTER CONTENU ARTICLE** **Section 3(4) HIPCAR – definition of child pornography** 1. Child pornography means pornographic material that depicts presents or represents: a. a child engaged in sexually explicit conduct; b. a person appearing to be a child engaged in sexually explicit conduct; or c. images representing a child engaged in sexually explicit conduct; this includes, but is not limited to, any audio, visual or text pornographic material. **Article13 de l'HIPCAR – Pédopornographie ou pornographie infantile** **AJOUTER CONTENU ARTICLE**	**Code pénal– 05-09-2009** **Article 333 bis 1** (...) quiconque, représente, par quelque moyen que ce soit, un mineur de moins de dix-huit (18) ans s'adonnant à des activités sexuelles explicites, réelles ou simulées, ou représente des organes sexuels d'un mineur, à des fins principalement sexuelles, ou fait la production, la distribution, la diffusion, la propagation, l'importation, l'exportation, l'offre, la vente ou la détention des matériels pornographiques mettant en scène des mineurs.	**Analyse juridique** Il s'agit d'une infraction essentielle à la protection de l'enfance, qui sanctionne au pénal la diffusion, la transmission, la mise à disposition, la proposition, la production et la possession d'images indécentes représentant des enfants. **Analyse des écarts** **Recommandation:** L'examen de la législation type à l'échelle mondiale de l'ICMEC confirme que la législation nationale respecte les principaux critères.[84]

83. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA
84. Examen de la législation type à l'échelle mondiale de l'ICMEC page 18

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de la CB[85] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**Ordonnance 03-05 du 19-07-2003 relative aux droits d'auteur et aux droits voisins et Ordonnance 03-07 du 19-07-2003 relative aux brevets d'invention**	**Analyse juridique** Les autorités chargées de l'application de la loi utilisent au niveau international les infractions relatives à la violation des droits d'auteur numériques comme conduite criminelle pour enquêter et lancer des poursuites contre plusieurs formes de cybercriminalité (crimes tels que le hameçonnage, la fraude électronique, la falsification électronique, les sites Internet frauduleux et le vol/la violation de données). L'une des infractions sous-jacentes dans de nombreux dossiers semble être la violation des droits d'auteur numériques. La cyberattaque de Sony[86] constitue l'un des exemples récents où les infractions et les procédures associées à la cybercriminalité, au vol de données/à l'espionnage industriel et la violation des droits d'auteur se complètent mutuellement. L'absence de dispositions liées à la propriété intellectuelle constituerait un échec pour la protection de l'innovation du 21è siècle des PPVS, des entreprises et des citoyens. Les œuvres digitales, base de données et programmes informatiques sont protégées juridiquement par l'Ordonnance 03-05 du 19-07-2003 relative aux droits d'auteur et aux droits voisins et Ordonnance 03-07 du 19-07-2003 relative aux brevets d'invention

85. Pas d'équivalent dans la CUA et l'HIPCAR
86. https://en.wikipedia.org/wiki/Sony_Pictures_hack

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 17 CITO - Infractions relatives à la violation des droits d'auteur et des droits connexes La violation des droits tels que définis dans la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel et la violation des droits connexes afférents aux droits d'auteur tels que définis par la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel.		
Article 11 de la CB[87] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.	**Code pénal, article 394**	**Analyse juridique** La prise en compte des actes de tentative et de complicité d'autrui en vue de la commission de crimes s'avère essentielle pour poursuivre en justice ceux qui pourraient avoir aidé ou encouragé la perpétration d'actes relevant de la cybercriminalité. L'article 394 du Code pénal incrimine la tentative de commettre des infractions portant atteinte aux systèmes de traitement automatisé de données. L'article 394 du Code pénal incrimine la participation et la complicité en vue de la commission d'infractions portant atteinte aux systèmes de traitement automatisé de données **Analyse des écarts** **Recommandation:** Utiliser l'article 11 de la CB et l'article 19 de la CITO (absence de référence à la tentative) comme guide pour la législation nationale.

87. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2du présent article.		
Article 12 de la CB[88] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale.	**Code pénal, article 394**	**Analyse juridique** Cette disposition s'avère essentielle pour que la responsabilité pénale des personnes morales (par exemple les sociétés commerciales) puisse être engagée. La responsabilité des personnes morales pour la commission d'infractions portant atteinte aux systèmes de traitement automatisé de données est prévue par l'article 394 du Code pénal.

88. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[89] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.	**Pas d'équivalent**	**Analyse juridique** L'article 3, paragraphe 1, sous e), de la CUA comprend la création et le téléchargement d'éléments racistes et xénophobes par le biais d'un système informatique, plutôt que leur simple diffusion ou mise à disposition (mais sans inclure l'intention ou le fait de procéder de la sorte «sans droit»). La terminologie utilisée par la CB doit être privilégiée. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de la CB dans l'article 3 du Protocole additionnel comme guide pour la législation nationale.

89. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.		
Protocole additionnel **Article 4[90] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de la CB dans l'article 4 du Protocole additionnel comme guide pour la législation nationale.

90. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 5[91] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques. 2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 du Protocole additionnel comme guide pour la législation nationale.

91. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 6[92] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.		

92. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 du Protocole additionnel comme guide pour la législation nationale.
Infractions additionnelles à étudier		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction englobe la phase de préparation d'un délit de tromperie lié à l'identité. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est souhaitable.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne les violations des données et la divulgation d'informations sensibles susceptibles d'avoir des répercussions sur les enquêtes pénales. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est souhaitable.
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 2293 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		**Analyse juridique** Cette infraction concerne les personnes qui disposent d'éléments de preuve pertinents et qui refusent de coopérer. Souvent, les autorités chargées de l'application de la loi dépendent de ces personnes pour obtenir des éléments de preuve dans le cadre des enquêtes en matière de cybercriminalité. Le refus de fournir des mots de passe ou des codes d'accès à des dispositifs ou des données crypté(e)s (à savoir, *«des informations protégées par des clés de chiffrement»*) constitue une infraction séparée (l'article 53 de la loi britannique qui régit les pouvoirs d'enquête intitulée UK Regulation of Investigatory Powers Act 2000 (RIPA) [94] prévoit un délit pénal pour les personnes qui ne se conforment pas à l'article 49 de la RIPA Notice to disclose the *«key»* (Injonction de divulgation de la *«clé»*)). **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est souhaitable.

93. Perquisition et saisie, assistance et injonctions de produire
94. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne pénalement ceux qui harcèlent autrui en ligne (certains pays prévoient des sanctions pour les infractions liées au harcèlement non informatique) et cette sanction est souhaitable concernant les délits commis en ligne. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est souhaitable.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous.		**Analyse juridique** Pour que l'infraction néerlandaise soit établie, un rendez-vous visant une finalité sexuelle est exigé, avec l'existence d'éléments de preuve d'échanges en ligne avec une intention sexuelle; il doit également être prouvé qu'un rendez-vous a été prévu (à savoir la date et le lieu). La disposition canadienne vise à éviter le leurre d'enfants par des adultes prédateurs en ligne. Cette infraction n'exige pas qu'une agression sexuelle ait été perpétrée. Ceci implique que l'accusé ne doit pas nécessairement avoir rencontré la victime en personne. L'infraction est commise avant que toute mesure n'ait été adoptée en vue de perpétrer le délit en tant que tel. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est souhaitable en vue de criminaliser cette conduite préparatoire avant que l'infraction sexuelle soit commise.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Section 172.1** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[95] **Perquisition et saisie de données informatiques stockées** 1. 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	**Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication[96]**	**Analyse juridique** Le pouvoir de l'article 3 vise la perquisition et la saisie plutôt que l'accès. Dans le Rapport explicatif de la CB, «Perquisitionner» signifie chercher, lire, inspecter ou examiner des données. Cela comprend la notion de recherche de données et de perquisition (examen) des données. Le terme «accès» possède un sens neutre et reflète plus précisément la terminologie informatique.[97] L'article 5 fait référence à l'«*accès*», lequel doit être constamment visé à l'article 3. L'article 26 de la CITO renvoie également à l'«*accès*».

95. Article 3 de la CUA
96. https://www.unodc.org/res/cld/document/dza/2009/loi_n_09-04_du_14_chaabane_1430_correspondant_au_5_aout_2009_portant_regles_particulieres_relatives_a_la_prevention_et_a_la_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication_html/Loi_prevention_et_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication.pdf
97. Paragraphe 191 du Rapport explicatif de la CB

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou obtenir d'une façon similaire les données informatiques consultées selon les paragraphes 1 et 2. Ces mesures incluent les prérogatives suivantes:	**Article 3** Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des informations judiciaires en cours, à la mise en place de dispositifs techniques pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel de leur contenu ainsi qu'à **des perquisitions et des saisies dans un système informatique**. **Article 4** Les opérations de surveillance prévues par l'article 3 ci-dessus peuvent être effectuées dans les cas suivants: a. pour prévenir les infractions qualifiées d'actes terroristes ou subversifs et les infractions contre la sûreté de l'État;	«*système informatique*» et l'article 5 aux «*données informatiques stockées*» et à un «*système de stockage informatique*». Par conséquent, seules les données **stockées** peuvent être saisies. **Analyse des écarts** **Recommandations:** La législation nationale pourrait intégrer la terminologie pertinente de la CB et de l'HIPCAR, afin d'inclure les définitions des expressions *système informatique*[98] et *données informatiques*,[99] et utiliser systématiquement le terme *accès*. L'article 4 restreint les dispositions sur la perquisition et la saisie à certaines catégories d'infractions. En d'autres termes, de nombreux cybercrimes qui ne sont pas des crimes contre la sécurité nationale ou liés au terrorisme n'auront pas de pouvoirs de procédure pertinents pour perquisitionner et saisir (uniquement dans le contexte préventif).

98. Voir l'article 1, sous a), de la CB: «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» **ou** l'article 3, paragraphe 5, de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions».

99. Voir l'article 1, sous b), de la CB: «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» **ou** l'article 3, paragraphe 6, de l'HIPCAR: «Données informatiques désigne toute représentation de faits, de concepts, d'informations (textes, sons ou images), de codes ou d'instructions lisibles par une machine, dans un format permettant d'être traité par un système informatique, notamment un programme pouvant faire exécuter une fonction à un système informatique».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou	b. lorsqu il existe des informations sur une atteinte probable à un système informatique représentant une menace pour l'ordre public, la défense nationale, les institutions de l'État ou l'économie nationale; c. pour les besoins des enquêtes et des informations judiciaires lorsqu'il est difficile d'aboutir à des résultats intéressant les recherches en cours sans recourir à la surveillance électronique; d. dans le cadre de l'exécution des demandes d'entraide judiciaire internationale. Les opérations de surveillance ci-dessus mentionnées ne peuvent être effectuées que sur autorisation écrite de l'autorité judiciaire compétente. Lorsqu'il s'agit du cas prévu au paragraphe (a) du présent article, l'autorisation est délivrée aux officiers de police judiciaire relevant de l'organe visé à l'article 13 ci-après, par le procureur général près la Cour d'Alger,pour une durée de six (6) mois renouvelable, sur la base d'un rapport indiquant la nature du procédé technique utilisé et les objectifs qu'il vise. Sous peine des sanctions prévues par le code pénal en matière d'atteinte à la vie privée d'autrui, les dispositifs techniques mis en place aux fins désignées au paragraphe 1. du présent article doivent être orientés, exclusivement, vers la collecte et l'enregistrement de données en rapport avec la prévention et la lutte contre les actes terroristes et les atteintes à la sûreté de l'État.	Les articles 3 et 5 font aussi référence à un L'article 5 va au-delà de l'article 19 de la CB et de l'article 20 de l'HIPCAR dans le fait que les pouvoirs de perquisition des systèmes connectés peuvent être étendus à n'importe quel ordinateur dans le monde sur la base de la réciprocité. Cette disposition sera également restreinte sur la base du fait qu'elle s'appliquera uniquement à la catégorie d'infractions définies à l'article 4. Le pouvoir d'accès et de perquisition doit être plus large que la classification restreinte actuelle des délits afin d'inclure les infractions relatives à la cybercriminalité dans la Loi 09-04. L'article 6 vise à garantir la copie du contenu des données d'origine et l'intégrité des preuves saisies. Même en l'absence de référence au fait de rendre les données inaccessibles pour empêcher d'autres infractions. L'inclusion de la terminologie utilisée à l'article 19, paragraphe 3, sous d) de la CB pourrait être envisagée pour garantir que les données saisies sont rendues inaccessibles afin d'empêcher toute autre utilisation. L'article 5 fait référence à la «*réquisition*» d'un individu pour aider à fournir des informations concernant le fonctionnement d'un système informatique ou pour protéger des données. On ne sait pas ce que «*réquisition*» signifie et quels pouvoirs sont disponibles si cet individu ne coopère pas. L'article 21 de l'HIPCAR prévoit la législation nécessaire afin de garantir qu'une assistance sera apportée par ceux qui disposent de connaissances spécialisées concernant le lieu où se trouvent les éléments de preuve pertinents (il pourrait donc être utilisé comme guide). L'article 17 de l'HIPCAR aborde également les infractions dans le cadre desquelles l'assistance a été refusée sans excuse légitime. La législation nationale doit inclure une disposition pour «*sortir sur imprimante les données informatiques et saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques*». Voir la définition de «*saisir*» à l'article 3, paragraphe 16 de l'HIPCAR.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. ayant été obtenus par une personne suite à une infraction, le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à: i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays. 2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2.	**Article 5** Les autorités judiciaires compétentes ainsi que les officiers de police judiciaire, agissant dans le cadre du code de procédure pénale et dans les cas prévus par l'article 4 ci-dessus, peuvent, **aux fins de perquisition, accéder**, y compris à distance: **(A) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées**; **Ou (B) à un système de stockage informatique.** Lorsque, dans le cas prévu par le paragraphe (a) du présent article, l'autorité effectuant la perquisition a des raisons de croire que les données recherchées sont stockées dans un autre système informatique et que ces données sont accessibles à partir du système initial, **elle peut étendre, rapidement, la perquisition au système en question ou à une partie de celui-ci après information préalable de l'autorité judiciaire compétente.** **S'il est préalablement avéré que les données recherchées, accessibles au moyen du premier système, sont stockées dans un autre système informatique situé en dehors du territoire national, leur obtention se fait avec le concours des autorités étrangères compétentes conformément aux accords internationaux pertinents et suivant le principe de la réciprocité.**	Une définition du terme «*réquisition*» et des pouvoirs disponibles pour garantir la une assistance raisonnable est fournie. Utiliser l'article 21 de l'HIPCAR comme guide avec l'infraction à l'article 17.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article21 de l'HIPCAR – Assistance Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à: • fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; • accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; • obtenir et copier ces données informatiques; • utiliser l'équipement pour faire des copies; et • obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci;	**Les autorités en charge de la perquisition sont habilitées à réquisitionner toute personne connaissant le fonctionnement du système informatique en question ou les mesures appliquées pour protéger les données informatiques qu'il contient, afin de les assister et leur fournir toutes les informations nécessaires à l'accomplissement de leur mission.** **Article 6** Lorsque l'autorité effectuant la perquisition découvre, dans un système informatique, des données stockées qui sont utiles à la recherche des infractions ou leurs auteurs, et que la saisie de l'intégralité du système n'est pas nécessaire, les données en question de même que celles qui sont nécessaires à leur compréhension, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés dans les conditions prévues par le code de procédure pénale. L'autorité effectuant la perquisition et la saisie doit, en tout état de cause, veiller à l'intégrité des données du système informatique en question. Toutefois, elle peut employer les moyens techniques requis pour mettre en forme ou reconstituer ces données en vue de les rendre exploitables pour les besoins de l'enquête, à la condition que cette reconstitution ou mise en forme des données n'en altère pas le contenu.	

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. un milieu ou un support de stockage informatique dans, ou sur *lequel sont stockées des données informatiques.* 2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe 1 de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. enlever ou rendre inaccessibles ces données du système informatique consulté. 2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes 2 et 3 de l'article 26 de la présente Convention.		
Article 16 de la CB[100] **Conservation rapide des données informatiques stockées** 1. 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.	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir de procédure est important pour garantir la préservation des données vulnérables par rapport à la suppression ou la perte. **Analyse des écarts** **Recommandations:** Ce pouvoir rapide d'obtention de DBA, de métadonnées et de contenus transactionnels et stockés s'avère essentiel dans le cadre des enquêtes en matière de cybercriminalité, afin de s'assurer de la disponibilité des éléments de preuve à des fins de perquisition, d'accès, de saisie et d'analyse. La terminologie utilisée à l'article 16 de la CB, à l'article 23 de l'HIPCAR ou à l'article 23 de la CITO pourrait être utilisée. Il sera alors également nécessaire de définir les expressions *«données informatiques»*[101], *«données relatives aux abonnés ou DBA»*[102], *«données de trafic»* et *«Fournisseur de services de communication»*[103].

100. Pas d'équivalent dans la CUA
101. Voir l'article 1, sous b), de la CB **ou l'**article 3, paragraphe 6, de l'HIPCAR
102. Voir l'article 1, sous d), de la CB: «*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*» ou l'article 3, paragraphe 18, de l'HIPCAR: «Données relatives au trafic désigne les données informatiques: a. ayant trait à une communication passant par un système informatique; et b. générées par un système informatique en tant qu'éléments de la chaîne de communication; et c. indiquant l'origine, la destination, l'itinéraire, l'heure, la taille et la durée de la communication ou le type de services sous-jacents».
103. Voir l'article 1, sous c), de la CB.: «*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 entité traitant ou stockant des données informatiques pour ce service de communication ou* ses utilisateurs».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.		Il convient de noter que la CB et l'HIPCAR ne donnent pas de définition des DBA, contrairement à la CITO: [104] «Toutes informations existantes chez le fournisseur de services relatives aux utilisateurs de services à l'exception des informations à travers lesquelles on peut connaître: a. *le type de services de communications utilisés, les conditions techniques et la période desdits services;* b. *l'identité de l'utilisateur, son adresse postale ou géographique ou son téléphone, les renseignements de paiement disponibles sur la base d'un contrat ou d'un arrangement de services;* c. *Toutes autres informations sur le site de montage des équipements de communication sur la base d'un contrat de services*». Il conviendrait de prévoir une durée de conservation raisonnable selon les circonstances et permettre l'extension de la demande dans certaines circonstances exigeantes (la CB et la CITO prévoient 90jours et l'HIPCAR 7jours). L'expérience montre que le délai de 90jours est trop court en matière de cyber-enquêtes et qu'il devrait être plus près des 180 jours avec une possibilité d'extension.

104. Voir l'article 2, paragraphe 9, de la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article23 de l'HIPCAR – Conservation rapide Si un [agent de répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		
Article 17 de la CB[105] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir procédural s'avère particulièrement important pour garantir que les FSC mettent à disposition des adresses IP pouvant permettre de localiser l'auteur d'un cybercrime. **Analyse des écarts** **Recommandation :** Le pouvoir de conservation rapide et la divulgation des données de trafic devraient être inclus dans la législation, afin de contribuer à l'efficacité des enquêtes relevant de la cybercriminalité. La terminologie de l'article 17 de la CB, des articles 23 et 24 de l'HIPCAR et de l'article 24 de la CITO pourrait être utilisée à de tels effets. Il sera également nécessaire de définir les expressions «données de trafic» et *«Fournisseur de services de communication»*.[106]

105. Pas d'équivalent dans la CUA
106. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 23 de l'HIPCAR – Conservation rapide** Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de l'HIPCAR – Divulgation partielle des données de trafic Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. les fournisseurs de services Internet; et/ou b. l'itinéraire de la communication. **Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic** Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[107] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir:	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une disposition essentielle pour la réalisation d'enquêtes efficaces en matière de cybercriminalité, et son absence aura un impact sur les poursuites devant les tribunaux et la coopération internationale. **Analyse des écarts** **Recommandation:** Ce pouvoir d'enquête s'avère nécessaire pour s'assurer que les FSC opérant en Algérie fournissent les DBA, les données de trafic et les informations sur les contenus stockés. La définition des expressions *«données informatiques», «données relatives aux abonnés ou DBA», «données de trafic» et «Fournisseur de services de communication»* sera également nécessaire.[108] L'article 25 de la CITO est un modèle à utiliser et qui contient différentes définitions, notamment pour les expressions *«système informatique»,*[109] *«fournisseur de services»*[110] *et «données»*[111]. Il serait souhaitable de pouvoir également définir les expressions *«données relatives aux abonnés ou DBA» et «données de trafic»,* car différents types de preuves pourront être produits par les FSC. En outre, ce pouvoir exigera des personnes et de toutes les autres entités (sociétés commerciales, institutions financières et autres organisations) qui détiennent des données de les remettre aux autorités chargées de l'application de la loi. L'article 18 de la CB et l'article 22 de l'HIPCAR pourraient constituer des guides pour une application uniforme des définitions.

107. Pas d'équivalent dans la CUA
108. Voir les définitions ci-dessus
109. Article 2, paragraphe 1, de la CITO: «*tout moyen matériel ou moral, ou ensemble de dispositifs interconnectés ou non, utilisés pour stocker des informations, les classer, les organiser, les restituer, les traiter, les développer et les échanger suivant des commandes et des instructions qui y sont stockées et ceci comprend toutes les entrées et sorties câblées à elles ou non par un système ou un réseau*».
110. Article 2, paragraphe 2, de la CITO: «*toute personne physique ou morale, publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ou qui procède au traitement ou au stockage des informations pour le service de communication ou ses utilisateurs*».
111. Article 2, paragraphe 3, de la CITO: «tout ce qui peut être stocké, traité, émis et transmis au moyen d'un système informatique, tels que les chiffres, les l*ettres, les symboles et autres*».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: a. à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou b. à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[112] **Interception de données relatives au contenu** **Article 29 de la CITO - Interception de données relatives au contenu**	**Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication**	**Analyse juridique** L'article 3 permet la collection des données en temps réel. Il n'existe pas de garanties permettant de prévenir les intrusions collatérales ou d'évaluer si l'utilisation de cette technique spéciale d'enquête est nécessaire, proportionnelle et raisonnable. Cette mesure doit être ordonnée conformément aux dispositions du Code de procédure pénale sur autorisation du procureur ou du juge d'instruction. Cette autorisation doit comporter tous les renseignements permettant d'identifier les liaisons à intercepter, l'infraction motivant le recours à cette mesure, ainsi que sa durée (4 mois, renouvelable). Cette mesure ne peut pas porter atteinte au secret professionnel.

112. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	Article 3 Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des informations judiciaires en cours, à la mise en place de dispositifs techniques **pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel** de leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.	L'article 10 de la 'Loi 09-04 du 5 août 2009 portant les règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication' oblige les FSC à prêter leur assistance aux autorités chargées des enquêtes judiciaires pour la collecte ou l'enregistrement en temps réel des communication; sinon, ils peuvent être poursuivis pour obstruction de la justice ou violation du secret de l'enquête et de l'instruction. Les articles 1 et 2 de la 'Loi 09-04 du 5 août 2009 portant les règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication' étendent cette mesure à toutes les infractions commises ou facilitées par des systèmes informatiques ou de communications électroniques. **Analyse des écarts** **Recommandations:** Les standards minimaux suivants sont suggérés: 1. **Garantir de manière systématique que l'interception est justifiée et, en vue de prévenir toute intrusion collatérale, suivre le test suivant**: **Nécessité**: le procureur ou le juge d'instruction devrait être satisfait lorsque la mesure de surveillance proposée est absolument nécessaire aux fins de l'enquête, en démontrant que tous les autres moyens ont été épuisés ou sont inapplicables. **Raisonnabilité**: le procureur ou le juge d'instruction devrait être satisfait lors que la mesure de surveillance est la moins intrusive possible en vue de collecter les renseignements en question. **Proportionnalité**: En cas d'atteinte à la vie privée, le procureur ou juge d'instruction devrait être satisfait sir la surveillance est proportionnelle à la gravité de l'infraction – cela comprend la prise en compte de l'intrusion collatérale et minimiser les atteintes contre les tierces parties.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 20 de la CB[113] **Collecte en temps réel des données relatives au trafic** 1. 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. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 3. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	**Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication** **Article 3** Conformément aux règles prévues par le code de procédure pénale et par la présente loi et sous réserve des dispositions légales garantissant le secret des correspondances et des communications, il peut être procédé, pour des impératifs de protection de l'ordre public ou pour les besoins des enquêtes ou des informations judiciaires en cours, à la mise en place de dispositifs techniques **pour effectuer des opérations de surveillance des communications électroniques, de collecte et d'enregistrement en temps réel** *de* leur contenu ainsi qu'à des perquisitions et des saisies dans un système informatique.	**Analyse juridique** Il existe une autorité spécifique et indépendante en charge de la collecte de données relatives au trafic en temps réel, conformément aux dispositions contenues dans le Décret présidentiel 15-261 du 08-10-2015 fixant la composition, l'organisation et les modalités de fonctionnement de l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication (JORA n° 53 du 8 octobre 2015). **Analyse des écarts** **Recommandations:** Il devrait y avoir des garanties assurant que la collecte est légale, nécessaire, raisonnable et proportionnelle en l'espèce. Les standards minimum suivants sont suggérés: 1. **Nécessité**: le procureur ou le juge d'instruction devrait être satisfait lorsque la mesure de surveillance proposée est absolument nécessaire aux fins de l'enquête, en démontrant que tous les autres moyens ont été épuisés ou sont inapplicables. 2. **Raisonnabilité**: le procureur ou le juge d'instruction devrait être satisfait lors que la mesure de surveillance est la moins intrusive possible en vue de collecter les renseignements en question. 3. **Proportionnalité**: En cas d'atteinte à la vie privée, le procureur ou juge d'instruction devrait être satisfait sir la surveillance est proportionnelle à la gravité de l'infraction – cela comprend la prise en compte de l'intrusion collatérale et minimiser les atteintes contre les tierces parties. L'article 28 de la CITO ne mentionne pas la collecte en temps réel, mais rapide. L'article 31(3)(e) de la CUA autorise la collecte en temps réel, mais des garanties sont nécessaires. Par conséquent, l'article 20 de la CB et l'article 25 de l'HIPCAR devraient être utilisés comme guide.

113. Article 31, paragraphe 3, sous e), de la CUA – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de l'HIPCAR - Collecte des données de trafic 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche. 2. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligation de divulgation et clés de chiffrement Dans la mesure où les terroristes et les criminels organisés utilisent systématiquement des applications de messagerie cryptée,[114] on pourrait envisager un pouvoir viable permettant d'ordonner la remise des clés pour les mots de passe afin de déverrouiller les dispositifs.[115] **Analyse des écarts** **Recommandation:** Nous ne sommes pas parvenus à déterminer si de tels pouvoirs existaient en Algérie (mais ce pouvoir permettrait aux autorités chargées de l'application de la loi de contraindre les propriétaires à déverrouiller les dispositifs).
		Obligations en matière de conservation des données[116] Ledit pouvoir pourrait permettre aux autorités chargées de l'application de la loi de: 1. retracer et identifier la source d'une communication; 2. identifier la destination d'une communication; 3. identifier la date, l'heure et la durée d'une communication, et 4. identifier le type de communication. L'Algérie ne prévoit pas une telle obligation.[117]

114. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, n°24 (15juin2015): 16-18. Academic Search Premier, EBSCOhost (consulté le 29 février 2016).
115. Pour obtenir un exemple, se reporter à l'article 49 de la loi britannique qui régit les pouvoirs d'enquête intitulée Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49
116. En 2006, l'UE a publié une directive relative à la conservation des données (les États membres de l'UE devaient stocker les données afférentes aux télécommunications électroniques pendant au moins six mois et tout au plus 24mois, à des fins de recherche, de détection et de poursuite des infractions graves). En 2014, la Cour de justice de l'UE a annulé la directive relative à la conservation des données, estimant qu'elle ne prévoyait pas suffisamment de garanties contre les ingérences dans les droits à la vie privée et à la protection des données. En l'absence de directive valable de l'UE portant sur la conservation des données, les États membres peuvent toujours mettre en place un régime applicable à la conservation des données. Les régimes nationaux sont disponibles à l'adresse suivante: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
117. Examen de la législation type à l'échelle mondiale de l'ICMEC page 18

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB[118] **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État. 2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.	**Pas d'équivalent**	**Analyse juridique** En l'absence de champ d'application clairement défini en matière de cyber-crimes, de nature internationale, toute législation sera restreinte. **Analyse des écarts** **Recommandation:** La législation nationale doit garantir que la compétence est définie selon les termes utilisés à l'article 22 de la CB, à l'article 19 de l'HIPCAR ou à l'article 30 de la CITO. En cas de conflit de compétence, il conviendrait de tenir compte des lignes directrices relatives à la détermination de la juridiction compétente pour juger une infraction (voir le document intitulé Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (révisé en 2016)).[119]

118. Pas d'équivalent dans la CUA
119. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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. **Article 19 de l'HIPCAR – Juridiction** La présente loi s'applique à tout acte ou omission commis: a. sur le territoire de [État prenant les dispositions]; b. sur un bateau ou un avion immatriculé en [État prenant les dispositions]; c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition. 3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 43 de la CITO **Autorité spécialisée**[120] 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. 2. a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'un mécanisme essentiel pour disposer de capacités d'enquête efficaces en matière de cybercriminalité. **Analyse des écarts** **Recommandation:** Cette mesure ne devrait pas exiger l'adoption de législation de mise en œuvre, et sous réserve des ressources, elle devrait être établie en tant que priorité. Les coordonnées de contact devraient être partagées concernant le point de contact unique désigné (SPOC), dans le pays, avec les autorités centrales à l'international et INTERPOL. Il conviendrait d'envisager la rédaction d'un protocole d'entente avec les agences nationales, de façon à ce que le SPOC dispose de l'autorité nécessaire pour entreprendre les actions requises dans le cadre d'une enquête internationale sur la cybercriminalité, en application du droit national et des traités. Le protocole d'entente devrait porter aussi bien sur les demandes entrantes que sur les demandes sortantes, et assurer un processus efficient et efficace.

120. Article 35 de la CB et article 25, paragraphe 2, de la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35. 3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.	**Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication** **Article 16** Dans le cadre des investigations ou des informations judiciaires menées pour la constatation des infractions comprises dans le champ d'application de la présente loi et la recherche de leurs auteurs, **les autorités compétentes peuvent recourir à l'entraide judiciaire internationale pour recueillir des preuves sous forme électronique.** **En cas d'urgence, et sous réserve des conventions internationales et du principe de réciprocité, les demandes d'entraide judiciaire visées à l'alinéa précédent sont recevables si elles sont formulées par des moyens rapides de communication, tels que la télécopie ou le courrier électronique pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification.**	**Analyse juridique** L'Algérie a ratifié la CITO au travers du Décret présidentiel 14-252 du 08-09-2014 (Journal officiel 0 57-2014). L'article 32 de la CITO garantit qu'elle puisse être utilisée en tant qu'instrument facilitant l'entraide judiciaire[121] et prévoit la conservation rapide de données informatiques stockées[122], la conservation et divulgation partielle rapides de données relatives au trafic[123], ainsi que la divulgation de données stockées[124] et de données relatives au trafic[125] aux États membres de la CITO. La Convention arabe pour la lutte contre la criminalité transnationale organisée de 2010 comporte une disposition spécifique dans son article 21, concernant l'utilisation illicite des systèmes d'information, et pourrait ainsi constituer une base à l'établissement de la double incrimination. La loi n° 09-04 du 14 Chaâbane 1430 ne prévoit pas de dispositions sur les demandes urgentes et l'envoi des éléments de preuve à l'État requérant par courrier électronique. Il s'agit néanmoins du mécanisme nécessaire pour une coopération internationale efficace et permettant de fournir des outils d'enquête spécifiques à la cybercriminalité (comme les injonctions de produire et la conservation). La Convention arabe pour la lutte contre la criminalité transnationale organisée de 2010 comporte une disposition spécifique dans son article 21, concernant l'utilisation illicite des systèmes d'information, et pourrait ainsi constituer une base à l'établissement de la double incrimination.

121. Il n'existe pas de disposition équivalente dans la CUA.
122. Article 29 de la CB et Article 37 de la CITO
123. Article 30 de la CB et Article 38 de la CITO
124. Article 31 de la CB et Article 39 de la CITO
125. Article 33 de la CB et Article 41 de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.	**Article 17** **Les demandes d'entraide tendant à l'échange d'informations ou à prendre toute mesure conservatoire sont satisfaites conformément aux conventions internationales pertinentes, aux accords bilatéraux et en application du principe de réciprocité.** **Article 18** *L'exécution de la demande d'entraide est refusée si elle est de nature à porter atteinte à la souveraineté nationale ou à l'ordre public.* La satisfaction des demandes d'entraide peut être subordonnée à la condition de conserver la confidentialité des informations communiquées ou à la condition de ne pas les utiliser à des fins autres que celles indiquées dans la demande.	**Analyse des écarts** **Recommandation:** L'adoption d'une législation nationale s'avère nécessaire en matière de conservation rapide des données informatiques stockées et de conservation et divulgation partielle rapides des données relatives au trafic, mais aussi concernant les injonctions de produire. La CB, l'HIPCAR et la CITO peuvent servir de précédents concernant la conservation rapide des données informatiques stockées,[126] la conservation et la divulgation partielle rapides des données relatives au trafic,[127] la divulgation des données stockées[128] et la collecte rapide de données relatives au trafic[129]. Il conviendrait également d'envisager des dispositions applicables à l'interception en temps réel des données de trafic et des contenus[130]. En outre, un cadre est nécessaire en matière de coopération dans le contexte des enquêtes liées à la cybercriminalité, par le biais des conventions multilatérales, notamment l'article 27 de la CB et l'article 32 de la CITO.[131]

126. Article 29 de la CB, article 23 de l'HIPCAR et article 37 de la CITO
127. Article 30 de la CB, articles 23 et 24 de l'HIPCAR et article 38 de la CITO
128. Article 31 de la CB et article 39 de la CITO
129. Article 41 de la CITO
130. Articles 33 et 34 de la CB et articles 25 et 26 de l'HIPCAR
131. Il n'existe pas de dispositions équivalentes sur la procédure d'entraide judiciaire dans la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles; c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires. 6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL. c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		
Article 26 de la CB[132] **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une procédure importante qui permet d'aider un autre État à empêcher la cybercriminalité et à enquêter en la matière. L'article 18, paragraphes 4 et 5, de la CNUCTO, prévoit le partage spontané d'informations dans le cadre des affaires répondant à la définition d'infractions graves[133], transnationales[134] et impliquant un groupe criminel organisé135. Sans répondre à cette définition. Une requête officielle devra être envoyée en empruntant les canaux de l'entraide habituels. Étant donné l'évolution rapide de la cybercriminalité, il s'agit d'un moyen efficace de coopérer avec d'autres États, et son absence empêche toute collaboration internationale efficace. Des échanges informels d'informations peuvent avoir lieu alors qu'une demande d'entraide est en cours, par le biais du recours au magistrat de liaison[136] mais il n'existe pas de base législative nationale pour le partage spontané avec un autre État à des fins de preuve dans le cadre des affaires de cybercriminalité.

132. Il n'existe pas de disposition équivalente dans la CUA.
133. Au sens de l'article 2, sous b), de la CNUCTO, l'expression «Infraction grave» désigne «un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde».
134. Article 3, paragraphe 1, de la CNUCTO
135. Au sens de l'article 2, sous a), de la CNUCTO, l'expression ««groupe criminel organisé» désigne un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves ou infractions établies conformément à la présente Convention, pour en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel».
136. Les questionnaires en matière d'entraide de l'Algérie constituent un exemple de contact entre les magistrats de liaison français et algériens.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières. **Article 33 de la CITO - Informations spontanées reçues** 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		**Analyse des écarts** **Recommandation:** *Utiliser* l'article 18, paragraphes 4 et 5, de la CNUCTO comme base pour le partage spontané d'informations (avec des garanties concernant l'utilisation des éléments de preuve ou la divulgation d'informations sensibles à des tiers (y compris un autre État)).[137] Envisager également l'adoption d'une législation fondée sur l'article 33 de la CITO ou l'article 26 de la CB.

137. Voir l'article 33, paragraphe 2, de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. **Article 27 de l'HIPCAR – Logiciel de criminalistique** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes:	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir de procédure permet à un État d'obtenir des contenus stockés dans un autre État dans des circonstances limitées. L'article 32, sous b), de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permettent un accès transfrontalier unilatéral sans besoin d'entraide, s'il existe un consentement ou si les informations sont accessibles au public. Exemples de recours à ce pouvoir de procédure dans le cadre de l'article 32, sous b), de la CB: le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données.[138] Un individu suspecté de terrorisme est arrêté dans les règles alors que son courrier électronique (révélant probablement des preuves d'un délit) est ouvert sur sa tablette, son smartphone ou un autre dispositif. Si le suspect consent volontairement à ce que la police accède à son compte, et si cette dernière est certaine que les données de la boîte de messagerie sont localisées dans un autre État, elle peut y avoir accès en vertu de l'article 32, sous b).

138. Paragraphe 294 du Rapport explicatif de la CB

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le suspect de l'infraction, si possible avec ses nom et adresse; et b. une description du système informatique ciblé; et c. une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et d. les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner a. le moyen technique utilisé ainsi que la date et l'heure de l'application; b. l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et c. toute information obtenue. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect.		**Analyse des écarts** **Recommandation:** Prévoir ce pouvoir restreint de collecte unilatérale d'éléments de preuve dans la législation avec des garanties visant à assurer que les contenus seront légalement obtenus auprès de l'utilisateur.[139] La terminologie utilisée peut être celle de l'article 32 de la CB et de l'article 40 de la CITO. L'article 32, sous b), a été vivement critiqué et on pourrait envisager de demander le consentement de l'État dans lequel les données informatiques stockées sont localisées en plus de celui de l'utilisateur. L'article 27 de l'HIPCAR prévoit des logiciels de criminalistique, lesquels pourraient permettre d'accéder à un ordinateur situé dans un autre État. Plusieurs restrictions empêchent l'obtention des éléments de preuve par d'autres moyens. Une décision judiciaire est requise et ne peut s'appliquer qu'à certaines infractions, pendant une durée restreinte (3mois). L'obtention du consentement de l'autre État doit être envisagée lorsque des logiciels criminalistiques sont susceptibles de faire intrusion.

139. Il conviendrait également d'envisager les situations telles que l'absence de disponibilité de l'utilisateur (en cas de décès par exemple) et la possibilité d'obtenir le consentement dans un autre État.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20. 6. 6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. 7. [Liste des infractions]. 8. 8. Un pays peut décider de ne pas mettre en œuvre l'article27. **Article 40 de la CITO - Accès transfrontière à des données informatiques** Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité.		

Égypte

L'Égypte a ratifié la CITO. Le 14 août 2018, l'Égypte a adopté la loi n° 175/2018 relative à la lutte contre les infractions liées aux technologies de l'information. Cette loi de lutte contre la cybercriminalité réglemente les activités en ligne et, selon des déclarations officielles, vise à compléter la nouvelle loi portant sur la presse et les médias, laquelle pénalise entre autres les activités en lignes non-autorisées et les violations relatives au contenu, comme les 'fake news'. L'équipe EuroMed Justice s'efforce de maintenir les informations mises à jour et correctes. Néanmoins, en dépit de nos efforts, et en raison des limitations temporelles et de ressources du projet en cours, une analyse des nouvelles dispositions législatives de 2018 ne sera possible que dans le cadre de la prochaine phase.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[140] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 4 de l'HIPCAR – Accès illégal** 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		Étude juridique Le CITO mentionne *«l'accès illégal à, la présence dans ou le contact avec»* sans définir ce que ces actes signifient. La CB mentionne «sans droit» dans l'Article 2 sur la base de la non autorisation de l'accès. Le Rapport explicatif de la CB a confirmé la dérivation de l'expression *«sans droit»* comme *«une conduite entreprise sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou une conduite autrement non couverte par des défenses, des excuses, des justifications ou des principes pertinents juridiques établis dans le cadre de la loi nationale.».*[141]

140. Article 6 de la CITO et article 29, paragraphe 1, de la CUA
141. Paragraphe 38, page 8 du Rapport explicatif à la Convention sur la cybercriminalité – N°185 https://rm.coe.int/16800cce5b

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête. **Article5 de l'HIPCAR – Présence illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.	**Aucun équivalent**	Les sections Commentaires[142] sur le modèle de projet de loi HIPCAR fournissent une explication quant à l'exigence de «l›absence de justification ou d›excuse légitime» de la manière suivante, «*L'accès à un système informatique ne peut être poursuivi conformément à la Section 4, que s'il se produit en «l'absence de justification ou d'excuse légitime». Cela nécessite que le contrevenant agisse sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) et que la conduite ne soit pas couverte autrement par des défenses, excuses, justifications ou principes pertinents juridiques établis. L'accès à un système permettant un accès libre et ouvert au public ou l'accès à un système avec l'autorisation du propriétaire ou d'un autre détenteur de droits n'est en conséquence pas de nature criminelle. Les administrateurs réseau et les entreprises de sécurité qui testent la protection des systèmes informatiques afin d'identifier des lacunes éventuelles dans les mesures de sécurité ne commettent pas un acte criminel.*» L'article 6 du CITO mentionne «l›accès illégal à, la présence dans ou le contact avec» sans définir ce que ces actes signifient – par conséquent, il convient de privilégier la CB et l'HIPCAR. **Analyse des lacunes** **Recommandation:** La législation nationale peut contenir un langage approprié provenant de l'Article 2 de la CB/sections 4 et 5 de l'HIPCAR afin d'inclure des définitions d'un *système informatique* et l'inclusion des programmes dans la définition des *données* car certaines données contiennent des programmes et d'autres non. En outre, afin de se conformer aux normes internationales, la législation devrait désigné l'accès «sans droits» plutôt que *frauduleusement*. Il convient également de prendre en compte une infraction distincte consistant à rester dans un système informatique conformément à la section 5 HIPCAR.

142. Page 30 Section Commentaires du modèle de projet de loi HIPCAR

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[143] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. **Article6 de l'HIPCAR – Interception illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques: a. toute transmission non publique vers, de, ou au sein d'un système informatique; ou b. des émissions électromagnétiques provenant d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code de procédure pénale n° 58/1937** **Article 309 bis** **Loi sur les communicationsn° 10/2003** **Article 73**	Étude juridique Cette infraction est essentielle afin de poursuivre les transmissions de données informatiques vers, depuis ou au sein d'un système informatique qui peuvent être interceptées illégalement afin d'obtenir des informations (par ex. wikileaks ou Panama Papers). L'article du Code pénal 309 bis n'est pas spécifique à la cyber-technologie. L'article 309bis peut être utilisé, conjointement à la Loi sur les communications n° 10/2003, Articles 73B par le Ministère public et les Tribunaux de commerce pour l'interception informatique illégale. **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'Article 3, l'HIPCAR section 6 comme guide - la terminologie de l'article 7 de la CITO est appropriée – bien qu'il n'existe pas de définition de *«données des technologies de l'information»*

143. Article 29, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut imposer que l'infraction soit commise avec une intention malhonnête ou en rapport avec un système informatique connecté à un autre système informatique ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique. **Article 7 de la CITO** **Interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques.		
Article 4 de la CB[144] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.	**Aucun équivalent**	Étude juridique De la même manière que ci-dessus, pour l'accès illégal, il n'est pas fait référence dans la CITO à *«sans droits»* et cela n'inclut pas la suppression des données informatiques, qui constitue un élément d'hameçonnage afin d'obtenir un accès illégal en installant un enregistreur de frappe pour obtenir des informations sensibles.[145] **Analyse des lacunes** **Recommandation:** L'absence de certains éléments clés associés à cette infraction dans la CITO peut être corrigée en utilisant la terminologie de l'article 4 de la CB ou de la section 7 de l'HIPCAR.

144. Article 29, paragraphe 1, sous e) à f), de la CUA
145. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article7 de l'HIPCAR – Atteinte à l'intégrité des données 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants: • endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes; • obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Article 8 de la CITO** **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 5 de la CB[146] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. **Article9 de l'HIPCAR – Atteinte à l'intégrité du système** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: • entrave ou porte atteinte au fonctionnement d'un système informatique; ou • entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Aucun équivalent**	Étude juridique Cette infraction empêcherait les logiciels malveillants qui interfèrent avec le fonctionnement d'un ordinateur – par exemple des vers informatiques - un sous-groupe des logiciels malveillants (comme les virus informatiques). Il existe des programmes informatiques à réplication automatique qui entravent le réseau en initiant de multiples processus de transfert de données. Ils peuvent influencer les systèmes informatiques en entravant le bon fonctionnement du système informatique, en utilisant des ressources du système pour se répliquer sur Internet ou en générant du trafic réseau qui peut rendre certains services (notamment des sites Internet) indisponibles. **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 ou la section 9 de l'HIPCAR comme guide pour la législation nationale. Il convient également de s'interroger pour savoir si la prévention et la poursuite des attaques contre l'infrastructure critique nécessitent une infraction distincte ou aggravée (Section 9(2) de l'HIPCAR) par exemple, le fonctionnement d'un système informatique peut être entravé à des fins terroristes (par ex. entraver le système qui stocke des dossiers de bourse peut les rendre inexacts ou entraver le fonctionnement d'une infrastructure critique).[147]

146. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
147. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		
Article 6 de la CB[148] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Aucun équivalent**	Étude juridique Comme ci-dessus, concernant l'accès illégal, aucune référence n'est faite à *«sans droits»* Cette infraction permettra les poursuites pour la production, la vente, l'obtention pour utilisation, l'importation, la distribution de codes d'accès et autres données informatisées pour commettre des cybercrimes - par exemple l'accès à des systèmes informatiques pour faciliter une attaque terroriste en perturbant le réseau électrique d'un pays. Toute infraction devra également tenir compte des appareils légitimes utilisés à des fins criminelles *(«double usage»)* – elle devra inclure la terminologie de la CB de *«principalement adapté»* **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 ou la section 10 de l'HIPCA comme guide pour la législation nationale.

148. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		Veuillez noter que l'HIPCAR propose l'option de lister les appareils dans un calendrier si cela est opportun – cela pourrait être restrictif et nécessite une mise à jour en fonction des avancées technologiques. La loi nationale doit fournir une excuse raisonnable pour que les autorités policières puissent utiliser les appareils pour des techniques d'enquêtes spéciales – voir la terminologie de l'article 6.2. de la CB ou la section 10(2) de l'HIPCAR pour guide.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article10 de l'HIPCAR – Dispositifs illégaux 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Loi sur les communicationsn° 10/2003** **Article 73** Quiconque commet l'un quelconque des actes suivants pendant la réalisation de son travail dans le domaine des communications ou en raison de celui-ci, est passible d'une peine d'emprisonnement pendant une période supérieure à trois mois et d'une amende supérieure à cinq milles livres et inférieure à cinquante milles livres ou l'une de ces peines: 1. Proclamation, publication ou enregistrement du contenu de tout message de communication ou d'une partie de celui-ci sans aucune base juridique	Étude juridique Le cadre de l'article 73 est étroit en comparaison avec les Bonnes pratiques internationales, car il criminalise uniquement l'acte de falsification informatique pour les individus commettant cette infraction alors qu'ils travaillent dans le domaine des communications. L'intégration de l'article 7 de la CB, la section 11 de l'HIPCAR ou la section 29(2)(b) de l'AUC est recommandée pour assurer une protection contre cette infraction qui pourrait inclure un hameçonnage et un harponnage. Par exemple, les données informatiques (telles que les données utilisées dans les passeports électroniques) peuvent être entrées, altérées, effacées ou supprimées, entraînant la prise en compte ou l'utilisation de données non authentiques à des fins juridiques, comme si elles étaient authentiques.[149]

149. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article11 de l'HIPCAR – Falsification informatique 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux. **Article 10 de la CITO** **Infraction de falsification** Utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques.	2. Dissimulation, modification, obstruction ou altération de tout message de communication reçu ou d'une partie de celui-ci. 3. Abstention de transmission de tout message de communication après avoir reçu l'ordre de le distribuer. 4. Divulgation sans droit en bonne et due forme de toute information concernant les utilisateurs des réseaux de communication ou leurs communications entrantes ou sortantes.	La Section 11(2) de l'HIPCAR vise également l'envoi de multiples messages de courrier électronique comme une infraction aggravée. Le langage dans l'article 10 de la CITO ne fait pas référence à toute intention malhonnête et nécessite que des dommages soient causés – le langage dans la CB et l'HIPCAR doit être préféré car il ne nécessite pas que des dommages soient causés. La CB et l'HIPCAR nécessitent uniquement que les données «données non authentiques» soient «prises en compte» **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 7, section 11 de l'HIPCAR ou 29(2)(b) de l'AUC comme guide pour la législation nationale

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 29, paragraphe 2, sous b), de la CUA (...) 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. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.		
Article 8 de la CB[150] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques;	**Aucun équivalent**	Étude juridique La terminologie de l'article 11 de la CITO et 29(2)(d) de l'AUC est vague, sans référence à toute intention malhonnête et nécessite une forme de *«dommages»* (CITO) ou *«bénéfice»* (AUC) sans définir ce que ces termes couvrent **Analyse des lacunes** **Recommandation:** Fournir des définitions pour *«données»* et *"«système de traitement* automatisé» et incluant «sans autorisation» – la terminologie dans la CB ou l'HIPCAR pour cette infraction constitue un bon guide pour la législation nationale

150. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		
Article 9 de la CB[151] **Infractions se rapportant à la pornographie enfantine** **AJOUTER CONTENU ARTICLE Section 3(4) HIPCAR – definition of child pornography** 1. Child pornography means pornographic material that depicts presents or represents: a. a child engaged in sexually explicit conduct; b. a person appearing to be a child engaged in sexually explicit conduct; or c. images representing a child engaged in sexually explicit conduct; this includes, but is not limited to, any audio, visual or text pornographic material. **Article13 de l'HIPCAR – Pédopornographie ou pornographie infantile** **AJOUTER CONTENU ARTICLE**	**Amendement de la Loi sur les enfants n° 126/2008** **Article 116 bis (a)** Toute personne important, émettant, produisant, préparant, affichant, imprimant, promouvant, acquérant ou diffusant tout matériel pornographique impliquant des enfants ou associé à l'exploitation sexuelle des enfants .... En dépit d'une peine plus sévère stipulée dans toute autre loi, la même peine est appliquée pour les infractions suivantes: 1. Quiconque utilise l'ordinateur, Internet ou une animation pour préparer, conserver, traiter, afficher, publier, imprimer ou promouvoir tout matériel pornographique ou toute activité pornographique associé(e) à l'incitation ou l'exploitation des enfants à la prostitution et la pornographie ou pour diffamer ou vendre lesdits enfants 2. Quiconque utilise l'ordinateur, Internet ou une animation pour inciter les enfants à errer, commettre des crimes ou se livrer à des activités illégales ou à de la pornographie, même si aucun crime n'a été commis	Étude juridique Cette infraction n'inclut pas la possession ou l'offre ou la mise à disposition ou la fourniture à une autre personne. Il n'existe pas de définition de *«matériel pornographique» ou «ordinateur»* – il n'est pas explicitement précisé si cela comprend également un système informatique ou un *«support de stockage informatique»?* Cela pourrait signifier que si la pornographie infantile est stockée sur une clé USB (ou tout autre support de stockage), l'infraction n'est pas avérée. **Analyse des lacunes** **Recommandation:** La terminologie de l'article 9.2 de la CB ou la section 3(4) de l'HIPCAR constitue un guide pour la définition de la pornographie infantile L'article 9.1.d et e. de la CB ou la section 13 de l'HIPCAR est un guide pour les infractions consistant à se procurer pour soi-même ou une autre personne et à stocker sur un système informatique ou un support de stockage informatique.

151. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de la CB[152] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**Loi de protection de la PI no. 82/2002** **Article 181**	Étude juridique Celle-ci est protégée de manière adéquate par la législation nationale

152. Pas d'équivalent dans la CUA et l'HIPCAR

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 11 de la CB[153] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention. **Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions** 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2du présent article.	**Code de procédure pénale n° 58/1937** **Articles 40 et 41**	Étude juridique Aider et encourager d'autres à commettre des crimes est essentiel afin de poursuivre ceux qui peuvent avoir apporté une assistance ou avoir encouragé la réalisation de cybercrimes. Les articles 40 et 41 du Code Pénal constituent les règles générales pour l'aide et l'encouragement et la tentative. Ces dispositions peuvent être appliquées à d'autres lois du droit matériel. **Analyse des lacunes** **Recommandation:** Tandis que le Code Pénal inclut déjà l'aide et l'encouragement et la tentative, l'article 11 de la CB et l'article 19 de la CITO sont recommandés comme guide pour inclusion dans une loi nationale sur la cybercriminalité, il ne fait donc aucun doute que l'assistance, l'encouragement et la tentative sont criminalisés.

153. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 12 de la CB[154] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale. 2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.	**Aucun équivalent**	Étude juridique Cette disposition constitue un élément essentiel afin que des personnes morales (par ex. des entités professionnelles) agissant pour le compte de personnes physiques disposent d'une responsabilité pénale **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 12 comme guide pour la législation nationale

154. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[155] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.	**Code de procédure pénale n° 58/1937** **Article 161 bis** Toute personne commettant un acte ou s'abstenant de commettre un acte qui entraînerait une discrimination entre des individus ou un groupe de personnes pour des motifs de sexe, d'origine, de langue, de religion ou de croyance, est passible d'emprisonnement et d'une amende supérieure à trente milles livres et inférieure à cinquante mille livres. Et cette discrimination a conduit la perte du principe d'opportunités égales, de justice sociale ou de paix générale. La peine devra être l'emprisonnement pendant une période supérieure à trois mois et une amende supérieure à cinquante mille livres et inférieure à cent milles livres ou l'une de ces peines si le crime visé au premier paragraphe du présent article est commis par un fonctionnaire, un agent de l'État ou toute personne à laquelle un service public est confié.	Étude juridique Les articles 161 bis et 76(2) ne désignent pas spécifiquement l'utilisation de dissémination via des systèmes informatiques, mais ces infractions pourraient être appliquées par le Ministère public si du matériel raciste ou xénophobe était disséminé. L'article 3(1)(e) de l'AUC qui inclut la création et le téléchargement de matériel raciste et xénophobe par le biais d'un système informatique plutôt que de simplement disséminer ou mettre à disposition un tel matériel n'inclut pas d'intention ou «*sans droits*» – la terminologie de la CB doit lui être préférée. **Analyse des lacunes** **Recommandation:** *Bien* qu'il n'existe pas de dispositions générales dans les articles 161 bis et 76(2), il est recommandé que la terminologie de la CB dans l'article 3 du Protocole Supplémentaire soit utilisée comme guide pour la législation nationale, afin de criminaliser un tel comportement par le biais d'un système informatique.

155. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.	**Loi sur les communicationsn° 10/2003** **Article 76(2)** Peines pour utilisation frauduleuse de communication Sans préjudice au droit à indemnité appropriée, une peine de confinement en prison et une amende supérieure à cinq cents livres et inférieure à vingt milles livres ou l'une des deux peines doivent être appliquées à quiconque: 1. Utilise ou aide à l'utilisation de moyens non autorisés pour mener une correspondance de communication. 2. Perturbe ou harcèle avec préméditation un tiers en utilisant de manière frauduleuse un équipement de communication.	
Protocole additionnel **Article 4[156] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Code de procédure pénale n° 58/1937** **Article 161 bis** **Loi sur les communicationsn° 10/2003** **Article 76(2)**	Étude juridique Les articles 161 bis et 76(2) ne désignent pas spécifiquement les menaces à caractère raciste ou xénophobe via des systèmes informatiques, mais ces infractions pourraient être appliquées par le Ministère public dans une telle situation **Analyse des lacunes** **Recommandation:** Bien qu'il n'existe pas de dispositions générales dans les articles 161 bis et 76(2), il est recommandé que la terminologie de la CB dans l'article 4 du Protocole Supplémentaire soit utilisée comme guide pour la législation nationale, afin de criminaliser un tel comportement par le biais d'un système informatique.

156. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 5[157] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques. 2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Code de procédure pénale n° 58/1937** **Article 161 bis** **Loi sur les communicationsn° 10/2003** **Article 76(2)**	Étude juridique Les Articles 161 bis et 76(2) ne désignent pas spécifiquement les insultes à caractère raciste ou xénophobe via des systèmes informatiques, mais ces infractions pourraient être appliquées par le Ministère public dans une telle situation **Analyse des lacunes** **Recommandation:** Bien qu'il n'existe pas de dispositions générales dans les articles 161 bis et 76(2), il est recommandé que la terminologie de la CB dans l'article 5 du Protocole Supplémentaire soit utilisée comme guide pour la législation nationale, afin de criminaliser un tel comportement par le biais d'un système informatique.

157. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 6[158] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie. 2. Une Partie peut:	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 du Protocole Supplémentaire comme guide pour la législation nationale

158. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions supplémentaires à examiner		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		Étude juridique Cette infraction couvre la phase préparatoire d'un crime de malhonnêteté lié à l'identité– **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Articles 85(2), 189, 190 et 193**	Étude juridique L'infraction HIPCAR sanctionne les violations de données et la divulgation d'informations sensibles qui pourraient affecter les enquêtes criminelles La législation nationale, bien qu'elle ne vise pas les violations de données de façon explicite – criminaliserait les violations des procédures d'enquête, qui devraient inclure les violations d'informations sensibles et de données.
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22159 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		Étude juridique Cette infraction concerne les personnes, ayant une connaissance spécifique de preuve tangible, qui refusent d'apporter leur aide. Fréquemment, les autorités policières se fient à de telles personnes pour collecter les preuves lors d'enquêtes de cybercrimes. Une infraction séparée est constituée par le défaut de fourniture de mots de passe ou d'accès à des codes vers des données ou des appareils cryptés (c'est-à-dire *«une clé vers des informations protégées»)* – la section 53 de la loi anglaise régissant les pouvoirs d'enquête de 2000 (RIPA) [160] prévoit de caractériser en infraction pénale les personnes qui ne se conforment pas à une section 49 de la RIPA Avis de divulgation de la *«clé»* **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

159. Perquisition et saisie, assistance et injonctions de produire
160. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		Étude juridique Cette infraction criminalise ceux qui harcèlent des personnes en ligne– certaines juridictions peuvent prévoir des infractions de harcèlement non liées à l'informatique – mais cette infraction est recommandée pour les crimes commis en ligne. **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous.		Étude juridique Pour prouver l'infraction néerlandaise, un rendez-vous à des fins sexuelles est requis pour apporter la preuve de l'historique de discussion en ligne à caractère sexuel, une demande de rendez-vous avec preuve de la planification (c'est-à-dire la date et le lieu). Le but de la loi canadienne est d'empêcher la préparation des adultes prédateurs des enfants en ligne. Cette infraction ne nécessite pas la commission de l'infraction sexuelle. Cela signifie que l'accusé n'a pas besoin de s'être réellement présenté au rendez-vous pour rencontrer la victime en personne. L'infraction est commise avant que toute action n'ait lieu pour commettre l'infraction substantielle. **Analyse des lacunes** **Recommandation:** Nous recommandons l'inclusion dans la législation nationale pour criminaliser ce comportement prédateur avant qu'une infraction sexuelle ne soit commise

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Section 172.1** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a.)soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[161] **Perquisition et saisie de** **données informatiques stockées** 1. 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.	**Code de procédure pénale n° 150/1950** **Articles 95, 206 et 206 bis** **Loi sur les communicationsn° 10/2003** **Articles 19 et 64**	Étude juridique Les dispositions contenues dans le Code de procédure pénale et la loi sur les communications ne font pas référence aux ordinateurs ou aux systèmes informatiques ou autres supports d'enregistrement informatiques et s'appliquent plus à l'interception (voir ci-dessous) Il s'agit d'un pouvoir d'enquête essentiel et doit faire référence à *«obtenir l\accès»* plutôt qu'à *«la recherche»*. Dans le Rapport explicatif de la CB, *«recherche»* signifie chercher, lire, inspecter ou examiner des données. Cela inclut la notion de recherche de données et de recherche (examen) dans des données. Le mot *«accès»* a une signification neutre et reflète la terminologie informatique de manière plus précise.[162]

161. Article 3 de la CUA
162. Rapport explicatif de la CB, paragraphe 191

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou obtenir d'une façon similaire les données informatiques consultées selon les paragraphes 1 et 2. Ces mesures incluent les prérogatives suivantes: a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;		**Analyse des lacunes** **Recommandation:** La législation nationale pourrait inclure la terminologie pertinente de la CB et l'HIPCAR afin d'inclure les définitions d'un *système informatique*[163] et *de données informatiques*[164] et mentionner l'*accès* de manière cohérente Il convient d'ajouter une définition de «saisir» pour garantir l'intégrité et pour des procédures spécifiques - section 3(16) de l'HIPCAR «*Saisir inclut:* • *activer tout système informatique sur site et tout support de stockage de données informatiques;* • *réaliser et conserver une copie de données informatiques, y compris par l'utilisation d'équipement sur site;* • *entretenir l'intégrité des données informatiques stockées pertinentes;* • *rendre inaccessibles ou supprimer les données informatiques sur le système informatique utilisé;* • *garder une impression de sortie des données informatiques; ou* • *saisir ou se procurer de manière similaire un système informatique, en tout ou en partie, ou un dispositif de stockage de données informatiques.*» La section 21 de l'HIPCAR prévoit une législation afin de garantir que de l'aide est apportée par ceux disposant d'une connaissance spécialiste du site des preuves pertinentes – cela peut être utilisé comme guide – voir également la section 17 de l'HIPCAR pour une infraction si l'aide est refusée sans excuse légitime

163. Voir article 1.a. de la CB: «tout dispositif ou un groupe de dispositifs interconnectés ou associés dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques»ou la section 3(5) de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou associés, y compris par Internet, dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques ou toute autre fonction».

164. Voir article 1.b. de la CB: «toute représentation de faits, informations ou notions sous une forme adaptée pour leur traitement dans le cadre d›un système informatisé, y compris un programme permettant à un système informatique de réaliser une fonction»ou la section 3(6) de l'HIPCAR: «Les *données informatiques signifient toute représentation de faits, notions, informations (qu'il s'agisse de textes, sons ou images), instructions ou code lisibles par machine, sous une forme adaptée pour leur traitement dans le cadre d'un système informatisé, y compris un programme permettant à un système informatique de réa*liser une fonction.»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou b. ayant été obtenus par une personne suite à une infraction,		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à: i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays. 2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article21 de l'HIPCAR – Assistance Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à: • fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; • accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; • obtenir et copier ces données informatiques; • utiliser l'équipement pour faire des copies; et • obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques. 2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe 1 de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. enlever ou rendre inaccessibles ces données du système informatique consulté. 2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes 2 et 3 de l'article 26 de la présente Convention.		
Article 16 de la CB[165] **Conservation rapide des données informatiques stockées** 1. 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.		Étude juridique Ce pouvoir d'enquête est important pour garantir que les données vulnérables à la suppression ou la perte sont préservées **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré de conserver les BSI, les métadonnées et le contenu enregistré et transactionnel est essentiel dans le cadre des enquêtes sur la cybercriminalité pour s'assurer que des preuves sont disponibles pour la recherche, l'accès, la saisie et la vérification. La terminologie de l'article 16 de la CB, section 23 de l'HIPCAR ou l'article 23 de la CITO pourrait être utilisée. Il convient également d'ajouter des définitions de *«données informatiques»*,[166] *«informations d›abonnés ou BSI»*, *«données de trafic»*[167] et *«Fournisseur de service de communication»*[168]

165. Pas d'équivalent dans la CUA
166. Voir Article 1.b. de la CB **ou** section 3(6) de l'HIPCAR
167. Voir Article 1.d de la CB: «toutes les données informatiques associées à la communication par le biais d›un système informatique, générées par un système informatique faisant partie intégrante d›une chaîne de communication, indiquant l›origine de la communication, sa destination, sa voie, l›heure, la date, la taille, la durée ou le type de service sous-jacent» **ou** la section 3(18) de l'HIPCAR: «Le trafic de données *désigne toutes les données informatiques qui: a. sont associées à la communication par le biais d'un système informatique; et b. sont générées par un système informatique faisant partie intégrante d'une chaîne de communication; et c. indiquent l'origine de la communication, sa destination, sa voie, l'heure, la date, la taille, la durée ou le type de service sous-jacent.»*
168. Voir Article 1.c. de la CB: «*i toute entité publique ou privée qui fournit aux utilisateurs de son service la capacité de communiquer par le biais d'un système informatique et ii toute autre entité qui traite ou stocke des données informatiques pour le compte de tels services de communication ou utilisateurs de* tels services.»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.		Il convient de noter que la CB et l'HIPCAR ne fournissent pas de définition de BSI – mais la CITO en fournit une pour informations d'abonnés:[169] «*Toute information à disposition du fournisseur de service concernant les abonnés au service, à l'exception des informations par le biais desquelles les éléments suivants peuvent être connus:* a. *le type de service de communication utilisé, les exigences techniques et la période de service.* b. *L'identité de l'abonné, son adresse postale ou géographique ou son numéro de téléphone et les informations de paiement disponibles en vertu du contrat ou de l'arrangement de service* c. *Toute autre information sur le site d'installation de l'équipement de communication en vertu du contrat de service.*» Il convient de tenir compte que la durée de conservation jugée raisonnable dans les circonstances et permettant une demande de prolongation dans des circonstances particulières – la CB et la CITO prévoient 90 jours et l'HIPCAR 7 jours. D'après l'expérience, 90 jours est trop court dans une enquête de cybercriminalité, le chiffre devrait se rapprocher de 180 jours puis être soumis à prolongation.

169. Voir article 2(9) de la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 23 de l'HIPCAR – Conservation rapide Si un [agent de répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.	**Aucun équivalent**	
Article 17 de la CB[170] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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	**Aucun équivalent**	Étude juridique Ce pouvoir procédural est particulièrement important pour s'assurer que les FSC fournissent les adresses IP pouvant localiser l'auteur d'un cybercrime. **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré concernant la divulgation de données de trafic devrait être inclus dans la législation pour permettre des enquêtes efficaces sur les cybercrimes. La terminologie de l'article 17 de la CB, sections 23 et 24 de l'HIPCAR ou l'article 24 de la CITO pourrait être utilisée. Des définitions de *«données de trafic» et «Fournisseur de service de communication»* seraient également requises[171]

170. Pas d'équivalent dans la CUA
171. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 23 de l'HIPCAR – Conservation rapide** Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de l'HIPCAR – Divulgation partielle des données de trafic Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. les fournisseurs de services Internet; et/ou b. l'itinéraire de la communication. **Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic** Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[172] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir:	**Code de procédure pénale n° 150/1950** **Articles 95, 206 et 206 bis** **Loi sur les communicationsn° 10/2003** **Articles 19 et 64**	Étude juridique Il existe une disposition cruciale pour une enquête efficace en matière de cybercrime et son absence affectera les poursuites et la coopération internationale. Les dispositions contenues dans le Code de procédure pénale et la loi sur les communications ne font pas référence aux ordinateurs ou aux systèmes informatiques ou autres supports d'enregistrement informatiques et s'appliquent plus à l'interception (voir ci-dessous). **Analyse des lacunes** **Recommandation:** Ce pouvoir crucial est nécessaire pour garantir que les FSC en Égypte fournissent les BSI, les données de trafic et les données du contenu stocké. Il convient également d'ajouter des définitions de *«données informatiques», «informations d›abonnés ou BSI», «données de trafic» et «Fournisseur de service de communication».*[173] L'article 25 de la CITO est un modèle qui pourrait être utilisé et utilise différentes définitions incluant *«technologie de l›information»,*[174] *«fournisseur de service»*[175] et *«données»*[176] *– nous recommandons d'ajouter des définitions pour «informations d›abonnés ou BSI», «données de trafic»* car il existe différents types de preuves pouvant être fournies par les FSC. En outre, ce pouvoir obligera les individus et les tiers (tels que les entreprises, les institutions financières et les autres organismes) qui détiennent des données à les produire aux autorités policières. L'article 18 de la CB et la section 22 de l'HIPCAR pourraient constituer un guide avec une application cohérente des définitions

172. Pas d'équivalent dans la CUA
173. Voir les définitions ci-dessus
174. Article 2(1) de la CITO: «*tout matériel ou moyen virtuel ou groupe de moyens interconnectés utilisés pour stocker, trier, disposer, développer et échanger des informations conformément à des commandes et des instructions stockées à l'intérieur. Cela inclut toutes les entrées et sorties associées, au moyens de câbles ou sans fil, dans un système ou un réseau.*»
175. Article 2(2) de la CITO: «toute personne physique ou morale, publique ou privée, qui fournit à des abonnés les services nécessaires pour communiquer par le biais de la technologie de l'information ou pour traiter ou stocker des informations pour le compte du service de communication ou de ses utilisateurs.»
176. Article 2(3) de la CITO: «tout ce qui peut être stocké, traité, généré et transféré par le biais de la technologie de ›information, comme des nombres, lettres, symboles, etc…»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: a. à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou b. à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[177] **Interception de données relatives au contenu** **Article 26 HIPCAR** **Article 29 de la CITO - Interception de données relatives au contenu**	**Code de Procédure Pénale** **Articles 95, 206 et 206 bis** **Article 95** Le juge d'instruction peut ordonner la saisie de l'ensemble des lettres, correspondances, journaux, publications et paquets trouvés dans les bureaux de poste, ainsi que des télégrammes trouvés dans les bureaux destinés aux télégrammes ou peut ordonner la surveillance des télécommunications ou l'enregistrement des conversations ayant lieu à un endroit spécifique dès qu'il le juge nécessaire pour révéler la vérité dans un crime ou une infraction passible d'incarcération pendant une période supérieure à trois mois.	*Étude juridique* Le juge d'instruction /ou le ministère public (par le biais d'un décret judiciaire émis par un juge) peut émettre un ordre pour enregistrer des conversations filaires et sans fil dans certaines circonstances conformément aux articles 95, 206 et 206 bis. Le Code de procédure pénale ne vise par les conversations établies par Internet ou par des ordinateurs, et la question n'a pas été statuée par la Cour égyptienne de cassation. Les demandes d'entraide judiciaire sont envoyées au bureau de coopération internationale au Ministère public. Si le Procureur général approuve la requête, elle est envoyée au Service de l'information et de la documentation au Ministère égyptien de l'Intérieur, qui traite la demande d'interception avec des officiers de police formés. Ces officiers doivent préparer un rapport sur l'issue *«sans fournir de détail sur les étapes et les détails de l'interception»*.

177. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	Dans tous les cas, les actes de saisie, d'inspection, de surveillance ou d'enregistrement doivent se tenir sous le couvert d'un mandat justifié, pendant une période inférieure à trente jours soumise à renouvellement pour une ou plusieurs autres périodes équivalentes **Loi sur les télécommunications 10/2003** **Article 19** Toutes les entités et entreprises travaillant dans le domaine des télécommunications doit fournir à la NTRA (Autorité nationale de régulation des télécommunications) tout rapport, statistique ou information requise en association avec ses activités à l'exception des questions liées à la Sécurité nationale **Article 64** Les opérateurs de services de télécommunications, les fournisseurs, leurs employés et les utilisateurs de tels services n'utiliseront pas d'équipement de cryptage des services de télécommunications sauf après avoir obtenu un consentement écrit de la NTRA, des Forces Armées et des organismes de Sécurité nationale et cette mesure ne s'applique pas aux équipements de cryptage des diffusions radio et télévisuelles	*Les officiers de police qui procèdent à l'interception des «courriers électroniques, adresses IP et comptes de réseaux sociaux» doivent le faire sans enfreindre la vie privée d'autres individus.* Les motifs de chaque acte d'interception sont écrits dans le Code de procédure pénale ainsi que la condition requise pour l'émission d'un décret par le juge d'instruction. **Analyse des lacunes** **Recommandations:** Il conviendrait d'obliger de manière spécifique les FSC opérant en Égypte à coopérer à la collecte en temps réel des contenus. De même, des garanties devraient être incorporées afin d'assurer que la collecte se fasse selon des modalités légales, raisonnables et proportionnelles. Il faudrait envisager d'étudier l'article 29 de la CITO, l'article 21 de la CB et la section 26 de l'HIPCAR, afin d'en incorporer les termes dans la législation nationale

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	En tenant compte de l'inviolabilité de la vie privée des citoyens protégée par la loi, chaque opérateur et fournisseur doit, à ses propres frais, fournir, au sein des réseaux de télécommunication dont il détient la licence, tous les potentiels techniques, y compris l'équipement, les systèmes, les logiciels et les communication qui permettent aux Forces armées et aux organismes de Sécurité nationale d'exercer leurs pouvoirs dans le cadre de la loi. La fourniture du service doit être synchronisée avec la disponibilité des potentiels techniques requis. Les fournisseurs et opérateurs de service de télécommunication et leurs agents marketing ont le droit de récolter des informations et des données précises concernant les utilisateurs auprès d'individus et de différentes entités dans l'État.	
Article 20 de la CB[178] **Collecte en temps réel des données relatives au trafic** 1. 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:	**Code de Procédure Pénale** **Articles 95, 206 et 206 bis** **Loi sur les télécommunications 10/2003** **Article 19 et 64**	

178. Article 31, paragraphe 3, sous e), de la CUA – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.		Étude juridique Comme ci-dessus, pour l'interception de données de contenu, le Code de procédure pénale et la loi sur les communications pourraient être utilisés pour collecter des données de trafic en temps réel. Il pourrait cependant exister un seuil inférieur pour le recueil des données relatives au trafic en temps réel. Il pourrait exister des situations où un seuil légal plus élevé pour accéder aux contenus pourrait ne pas être compris par un demandeur – mais un seuil plus bas pour accéder au trafic pourrait l'être. Aussi, il devrait exister une distinction entre la collecte en temps réel de contenus stockés et de données de trafic. Il s'avère nécessaire de créer des garanties et des exigences/ procédures pour contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques en Égypte **Analyse des lacunes** **Recommandations:** Il conviendrait de disposer d'un pouvoir spécifique pour collecter les données de trafic en temps réel et d'obliger les FSC opérant en Égypte à coopérer à la collecte en temps réel des données de trafic. De même, des garanties devraient être intégrées afin d'assurer que la collecte soit légale, raisonnable et proportionnelle au vu des circonstances. La terminologie de l'article 28 de la CITO pourrait être envisagée, mais elle ne fait pas allusion à la collecte rapide en temps réel uniquement. L'article 31(3)(e) de l'AUC permet un recueil en temps réel mais des garanties sont requises. Par conséquent, l'article 20 de la CB et la section 25 de l'HIPCAR devraient être utilisés comme guide pour la législation nationale

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de l'HIPCAR - Collecte des données de trafic 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche. 2. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	Loi sur les communicationsn° 10/2003 **Article 64** Les opérateurs de services de télécommunications, les fournisseurs, leurs employés et les utilisateurs de tels services n'utiliseront pas d'équipement de cryptage des services de télécommunications sauf après avoir obtenu un consentement écrit de la NTRA, des Forces Armées et des organismes de Sécurité nationale et cette mesure ne s'applique pas aux équipements de cryptage des diffusions radio et télévisuelles. En tenant compte de l'inviolabilité de la vie privée des citoyens protégée par la loi, chaque opérateur et fournisseur doit, à ses propres frais, fournir, au sein des réseaux de télécommunication dont il détient la licence, tous les potentiels techniques, y compris l'équipement, les systèmes, les logiciels et les communication qui permettent aux Forces armées et aux organismes de Sécurité nationale d'exercer leurs pouvoirs dans le cadre de la loi. La fourniture du service doit être synchronisée avec la disponibilité des potentiels techniques requis. Les fournisseurs et opérateurs de service de télécommunication et leurs agents marketing ont le droit de récolter des informations et des données précises concernant les utilisateurs auprès d'individus et de différentes entités dans l'État.	*Étude juridique* Cet article empêche toute utilisation d'équipements cryptés – tels que les appareils verrouillés par un code pin L'article permet également la fourniture de logiciels pour accéder aux services cryptés. La présence d'une disposition relative à l'exécution n'est pas claire. **Analyse des lacunes** **Recommandation:** Ce pouvoir peut être considéré comme trop large et impossible à appliquer à la lumière du nombre d'appareils et d'applications de messagerie cryptés - un pouvoir viable pour fournir les clés ou mots de passe pour débloquer les appareils au cas par cas est une disposition anglaise[179]

179. En guise d'exemple, voir la section 49 de la loi anglaise régissant les pouvoirs d'enquête 2000 (GB) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations de conservation des données[180] Un tel pouvoir peut permettre aux autorités policières de 1. Tracer et identifier la source d'une communication 2. Identifier la destination d'une communication; 3. Identifier la date, l'heure et la durée d'une communication; et 4. Identifier le type de communication L'Égypte ne dispose pas d'une telle obligation[181]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB[182] **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.	**Aucun équivalent**	**Étude juridique** Sans cadre clairement défini pour les infractions de cybercriminalité, qui sont de nature internationale, toute législation sera restreinte. **Analyse des lacunes** **Recommandation:** La législation nationale garantit que la juridiction est définie en utilisant les termes de l'article 22 de la CB, de la section 19 de l'HIPCAR ou de l'article 30 de la CITO. S'il existe un conflit entre des juridictions, il convient de tenir compte des directives quant à la détermination de la juridiction appropriée pour poursuivre une infraction – consulter les directives Eurojust permettant de décider quelle juridiction doit poursuivre (révisées en 2016)[183]

180. En 2006, l'UE a émis sa directive de conservation des données - les États Membres de l'UE devaient stocker les données de télécommunications électroniques pendant au moins six mois et au plus 24 mois pour enquêter, détecter et poursuivre des crimes graves. En 2014, la Cour de Justice de l'UE a invalidé la directive de conservation des données, arguant qu'elle fournissait des garanties insuffisantes contre les interférences avec les droits à la vie privée et la protection des données. En l'absence d'une direction de conservation des données valide de l'UE, les États Membres peuvent toujours prévoir un protocole de conservation des données – pour les protocoles nationaux, consulter: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

181. Examen global ICMEC page 25

182. Pas d'équivalent dans la CUA

183. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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. **Article 19 de l'HIPCAR – Juridiction** La présente loi s'applique à tout acte ou omission commis: a. sur le territoire de [État prenant les dispositions]; b. sur un bateau ou un avion immatriculé en [État prenant les dispositions]; c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		
Article 43 de la CITO **Autorité spécialisée**[184] 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.	**Aucun équivalent**	Étude juridique Il s'agit d'un mécanisme essentiel pour disposer d'une aptitude efficace à l'enquête de cybercrimes. Le Service des crimes sur ordinateur et réseau, établi par le décret du Ministère de l'intérieur n1 3507/2002 (dans le cadre du Service d'information et de documentation) a la capacité d'intercepter les courriers électroniques, les adresses IP et les comptes de réseaux sociaux (sans enfreindre la vie privée d'autres individus). Le réseau 24/7 est conçu pour répondre immédiatement aux requêtes internationales afin de conserver les données **et** le recueil de preuves **et** toute autre assistance pour enquêter sur la cybercriminalité (par ex. localiser un suspect)

184. Article 35 de la CB et article 25, paragraphe 2, de la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.		**Analyse des lacunes** **Recommandation:** La mise en œuvre ne devrait pas nécessiter de législation et, en fonction des ressources, cette mesure devrait être établie en priorité. Cette mesure peut uniquement nécessiter l'élargissement des attributions du Service des crimes sur ordinateur et réseau déjà mis en place, en nommant un point de contact unique 24/7 (SPOC). Les coordonnées doivent être partagées pour le SPOC nommé au niveau national, au niveau international pour les autorités centrales et INTERPOL. Il convient également de tenir compte de l'élaboration d'un Mémorandum de compréhension avec les agences nationales, afin que le SPOC dispose d'une autorité pour entreprendre les actions requises dans le cadre d'une enquête de cybercriminalité internationale appliquant les traités et lois nationaux. Ce MOU doit comprendre les requêtes entrantes et sortantes et garantir un processus efficace et effectif.
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.		Étude juridique L'article 32 de la CITO garantit qu'il peut être utilisé comme un instrument pour faciliter la MLA[185] et assure une préservation accélérée des données informatiques enregistrées,[186] une préservation accélérée et une divulgation partielle des données de trafic[187] et une divulgation des données enregistrées[188] et des données de trafic [189] aux États qui ont ratifié le CITO.

185. aucune disposition équivalente dans l'AUC
186. Article 29 de la CB et Article 37 de la CITO
187. Article 30 de la CB et Article 38 de la CITO
188. Article 31 de la CB et Article 39 de la CITO
189. Article 33 de la CB et Article 41 de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication. 4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.		**Analyse des lacunes** **Recommandation:** Il est recommandé de légiférer pour les pouvoirs procéduraux dans la CITO au plan national, afin qu'ils puissent être utilisés pour des enquêtes nationales et qu'ils soient en outre réciproques afin que les États n'ayant pas ratifié la CITO puissent les utiliser. La CITO ne prévoit pas d'interception de contenu et de données de trafic en temps réel – cela doit être pris en compte dans l'application des précédents dans la BC et l'HIPCAR.[190] Le principe de réciprocité, cependant, peut s'appliquer pour les dispositions appliquant les articles 95, 206 et 206 bis du Code de procédure pénale et les articles 19 et 64 de la loi sur les communications. Il convient d'étudier le fait de permettre aux autorités juridictionnelles d'autoriser l'application du droit national afin d'enquêter dans l'État dans lequel l'accès à un appareil est connu. L'accessibilité des informations constitue le critère essentiel pour lancer une enquête dans des situations dans lesquelles il n'est pas possible de savoir où les données sont stockées (c'est-à-dire dans le cloud). Elle pourrait comprendre une *«reconnaissance mutuelle»* des décisions de justice émises à l'encontre des fournisseurs de service de communications dans un État donné, qui pourraient être remise aux filiales des FSC situées dans d'autres États, en fonction de l'endroit où les données sont stockées.

190. Articles 33 et 34 de la BC et sections 25 et 26 de l'HIPCAR

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante. **Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle** 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres *arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;* d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative. 7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTER-POL.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis. e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de la CB[191] **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre. 2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.	**Aucun équivalent**	**Étude juridique** Il s'agit d'une procédure importante afin de permettre à un État ayant connaissance d'informations qui aideraient un autre État à empêcher un cybercrime ou à enquêter sur celui-ci. Bien qu'elle soit disponible entre les États ayant ratifié la CITO dans l'article 33 de la CITO, l'Égypte ne dispose pas de base juridique pour le partage de ces informations avec les États non membres de la CITO, à moins qu'une requête officielle ne soit envoyée par le biais des canaux MLA classiques. L'article 18(4)-(5) de la CNUCTO prévoit le partage d'intelligence spontané pour des questions satisfaisant la définition d'un crime grave[192], qui est transnational[193] et implique un groupe du crime organisé[194]. Sans satisfaire cette définition une requête officielle devra être envoyée par le biais des canaux MLA classiques aux États n'ayant pas ratifié la CITO. Sur la base de la rapidité de mouvement de la cybercriminalité, le partage spontané est une manière efficace de coopérer avec d'autres États et, en l'absence de partage, empêche une collaboration internationale efficace avec les États n'ayant pas ratifié la CITO. **Analyse des lacunes** **Recommandation:** Utiliser l'article 18(4)-(5) de la CNUCTO comme base pour le partage spontané d'informations qui rentre dans le cadre de la CNUCTO (sans garanties fournies en matière d'utilisation comme preuve ou de divulgation d'informations sensibles à un tiers (y compris un autre État).[195] Prendre en compte la législation basée sur l'article 33 de la CITO ou l'article 26 de la CB.

191. Il n'existe pas de disposition équivalente dans la CUA.
192. Article 2(b), «*un «crime grave» est un acte constituant une infraction passible d'une peine privative de liberté au moins égale à quatre ans ou d'une peine plus lourde*»
193. Article 3(1) de la CNUCTO
194. Article 2(a) de la CNUCTO «*Un «groupe du crime organisé» signifie groupe structuré de trois personnes ou plus, existant pendant une certaine période et agissant de concert dans le but de commettre un ou plusieurs crimes ou infractions graves établis* conformément à la présente *Convention, afin d'obtenir, directement ou indirectement, un avantage financier ou matériel*».
195. Voir article 33(2) de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 33 de la CITO - Informations spontanées reçues 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou	**Aucun équivalent**	Étude juridique Ce pouvoir procédural permet à un État de garantir le contenu stocké dans un autre État dans des circonstances limitées. L'article 32.b. de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permet l'accès transfrontalier unilatéral sans besoin d'entraide judiciaire en cas d'accord ou quand l'information est publiquement disponible.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. **Article 27 de l'HIPCAR – Logiciel de criminalistique** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes: • le suspect de l'infraction, si possible avec ses nom et adresse; et • une description du système informatique ciblé; et • une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et		Les exemples d'usage de ce pouvoir procédural conformément à l'article 32.b de la CB comprennent : L'adresse électronique d'une personne peut être enregistrée dans un autre pays par un fournisseur de service, ou une personne peut enregistrer sciemment des données dans un autre pays. Ces personnes peuvent récupérer les données et à condition qu'elles en aient l'autorité légitime, elles peuvent volontairement divulguer les données à des officiels d'application de la loi, ou permettre à ces officiels d'accéder aux données[196] Un terroriste présumé est arrêté légalement pendant que sa boîte de réception électronique – contenant éventuellement des preuves d'un crime – est ouverte sur sa tablette, son smartphone ou un autre appareil. Si le suspect consent volontairement à ce que la police accède à son compte et si la police est sûre que les données de la boîte de réception sont situées dans un autre État, la police peut accéder aux données selon l'article 32.b. **Analyse des lacunes** **Recommandation:** Ce pouvoir restreint à récupérer unilatéralement les preuves est inclus dans la législation, ce qui garantit que le consentement de l'utilisateur est obtenu légalement.[197] La terminologie de l'article 32 de la CB et de l'article 40 de la CITO peut être utilisée. L'article 32b a été lourdement critiqué et il peut être envisagé que le consentement de l'État dans lequel les données informatiques stockées sont stockées soit obtenu en plus de celui de l'utilisateur. La section 27 de l'HIPCAR prévoit un logiciel judiciaire et cela peut permettre l'accès à un ordinateur dans un autre État. Il existe un certain nombre de restrictions qui nécessitent que les preuves ne puissent pas être obtenues par d'autres moyens, qu'un ordre judiciaire soit requis, qu'il ne peut s'appliquer qu'à certaines infractions et que sa durée soit limitée (3 mois). Il convient également d'examiner le consentement de l'autre État dans lequel le logiciel judiciaire peut intervenir.

196. Paragraphe 294, page 53 du Rapport explicatif de la CB
197. Il convient d'examiner des situations telles que la non disponibilité d'un utilisateur (par ex. sa mort) et si le consentement peut être obtenu dans un autre État

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner a. le moyen technique utilisé ainsi que la date et l'heure de l'application; b. l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et c. toute information obtenue. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect. 5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions]. 8. Un pays peut décider de ne pas mettre en œuvre l'article27.		

Israël

Israël a déposé son instrument d'adhésion à la Convention de Budapest le 9 mai 2016.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[198] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi informatique de 1995** **Section 4** Une personne qui entre illégalement dans du matériel informatique situé dans un ordinateur est passible d'emprisonnement pendant une durée de trois ans. À cet égard, «*pénétration dans un matériel informatique*» - pénétration au moyen de communication ou de connexion avec un ordinateur, ou en le faisant fonctionner, mais à l'exclusion de la pénétration dans du matériel informatique qui constitue une écoute illicite selon la Loi sur les écoutes illicites, 5729 – 1979. **Section 5** Une personne qui commet un acte interdit selon la section 4 afin de commettre un crime selon une loi quelconque, à l'exclusion de la présente loi, est passible d'emprisonnement pour une durée de cinq ans.	**Étude juridique** La CB mentionne «sans droits» La section 4 de la législation nationale mentionne la pénétration «*illégalement*» dans du «*matériel informatique*» et criminalise uniquement l'accès plutôt que l'obtention de tout «*matériel informatique*» L'activité d'obtention d'informations constituerait une infraction, telle que l'infraction de violation de la vie privée, obtention frauduleuse ou malhonnête d'informations ou vol La loi israélienne requiert uniquement une intention de commettre une infraction grave (c'est-à-dire circonstances aggravantes). La pénétration illégale, contrairement à la section 4, est une infraction distincte. Cela est identique à la CB, qui ne nécessite pas de preuve que l'accès illégal était destiné à commettre une autre infraction.

198. Article 6 de la CITO et article 29, paragraphe 1, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[199] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi sur les écoutes téléphoniques** **Section 2**	Étude juridique La section 2 de la Loi sur les écoutes téléphoniques prévoit cette infraction criminelle. Une infraction d'interception illégale est essentielle pour poursuivre les transmissions non publiques de données informatiques vers, depuis ou au sein d'un système informatique, qui peuvent être interceptées illégalement pour obtenir des informations sur la localisation d'une personne (par ex. pour cibler cette personne).[200]
Article 4 de la CB[201] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.	**Loi informatique de 1995** **Sections 2 et 6** 2. Une personne qui effectue illégalement l'un des actes suivants est passible d'emprisonnement pour une durée de trois ans: 1. … 2. Supprime du matériel informatique, l'altère, le perturbe d'une autre manière ou gêne son utilisation.	Étude juridique La CB mentionne «sans droit» et la législation nationale «illégalement» sur la base de la non autorisation de l›accès. L›infraction nationale mentionne dans la section 2(2) la suppression de *"matériel informatique"* Il n'est pas exigé de démontrer que la suppression a provoqué la perturbation ou les dommages.[202] L'infraction de la section 6 comprendrait la création de botnets qui endommagent, effacent, détériorent, altèrent ou suppriment Si un effacement ou une «*suppression de données*» a eu lieu de la manière spécifiée dans la CB article 4, une infraction de la section 2 serait pertinente.

199. Article 29, paragraphe 2, de la CUA
200. http://www.coe.int/en/web/cybercrime/guidance-notes
201. Article 29, paragraphe 1, sous e) à f), de la CUA
202. Dans l'affaire de l'État d'Israël contre Refaeli Oded, M. Refaeli a été accusé d'avoir effectué une intrusion dans un ordinateur depuis un ordinateur extérieur vers l'ordinateur de son précédent employeur et d'avoir effacé des preuves. Le Tribunal a jugé que l'interprétation correcte et raisonnable de la section 2(2) de la Loi sur les ordinateur est que toute suppression et/ou transformation de matériels informatiques étaient interdites selon la Loi informatique et qu'il n'était pas nécessaire de prouver que la suppression avait provoqué un dommage ou une perturbation quelconque.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	a. Une personne qui conçoit un programme logiciel d'une manière qui lui permet de provoquer des dommages à ou de perturber un ordinateur non spécifique ou du matériel informatique, afin de provoquer illégalement des dommages à ou la perturbation d'un ordinateur ou de matériel informatique, qu'il soit spécifique ou non, b. Une personne qui transfère un programme logiciel à un autre ou qui infiltre l'ordinateur d'un autre avec un programme logiciel apte à provoquer des dommages ou une perturbation comme visés dans la sous-section (a), afin de provoquer illégalement les dommages ou la perturbation susmentionnés, est passible d'emprisonnement pour une durée de cinq ans.	
Article 5 de la CB[203] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.	**Loi informatique de 1995** **Section 2** Une personne qui effectue illégalement l'un des actes suivants est passible d'emprisonnement pour une durée de trois ans: (1) Gène le bon fonctionnement d'un ordinateur ou entrave son utilisation;	**Étude juridique** La Loi informatique mentionne la perturbation du *«fonctionnement d›un ordinateur»* en section 2(1) **Analyse des lacunes** **Recommandation:** Il convient de s'interroger pour savoir si la prévention et la poursuite des attaques contre l'infrastructure critique nécessitent une infraction distincte ou aggravée, par exemple, le fonctionnement d'un système informatique peut être entravé à des fins terroristes (par ex. entraver le système qui stocke des dossiers de bourse peut les rendre inexacts ou entraver le fonctionnement d'une infrastructure critique).[204]

203. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
204. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 6 de la CB[205] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus; ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.	**Loi informatique de 1995** **Section 6** a. Une personne qui conçoit un programme logiciel d'une manière qui lui permet de provoquer des dommages à ou de perturber un ordinateur non spécifique ou du matériel informatique, afin de provoquer illégalement des dommages à ou la perturbation d'un ordinateur ou de matériel informatique, qu'il soit spécifique ou non, ... b. Une personne qui transfère un programme logiciel à un autre ou qui infiltre l'ordinateur d'un autre avec un programme logiciel apte à provoquer des dommages ou une perturbation comme visés dans la sous-section (a), afin de provoquer illégalement les dommages ou la perturbation susmentionnés....	**Étude juridique** La Section 6 criminalise la production et la transmission d'un programme logiciel pour infiltrer, provoquer des dommages ou une perturbation. Le transfert visé en section 6(b) comprendrait la vente de tels programmes logiciels (par exemple des chevaux de Troie) en 6(b) et (c). Israël a déposé une réserve concernant l'obtention pour utilisation, ainsi que l'importation et la possession de distribution de codes d'accès et autres données informatisées utilisées pour commettre des cybercrimes lors de la ratification de la CB. Toute infraction devra également prendre en compte les appareils disposant d'une utilisation légitime qui ont été utilisés à des fins criminelles *(«double usage»)* – la législation est claire, tout programme logiciel utilisé pour *«provoquer illégalement des dommages ou une perturbation d'un ordinateur ou de matériel informatique»* et intègre ainsi de manière appropriée le double usage. *«Infiltren»* est utilisé dan s la section 6(b) et, tandis que cela pourrait signifier accéder illégalement, il convient de le clarifier L'article 6.2 de la CB indique qu'il n'est pas nécessaire d'interpréter l'article comme imposant une responsabilité criminelle lorsque les actions ont été effectuées pour d'autres motifs que la réalisation d'une infraction, comme des inspections de protection autorisées ou par la police. Selon la loi israélienne, une condition pour la formation d'une infraction est que l'action ait été réalisée illégalement, par conséquent, il est clair que les autorités d'application de la loi agissant légalement ne seront pas criminalisées et ne nécessitent donc pas d'exemption **Analyse des lacunes** **Recommandation:** Inclure une définition de *«infiltren»* dans la Loi informatique afin de clarifier sa signification

205. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Loi informatique de 1995** **Section 3** a. Une personne qui effectue l'un des actes suivants est passible d'emprisonnement pour une durée de cinq ans: 1. Transfère à une autre personne ou stocke dans un ordinateur des fausses informations ou réalise une action concernant les informations afin d'entraîner la production de fausses informations ou de fausse production;	**Étude juridique** L'article 7 couvre les données sous forme d'équivalent d'un document public ou privé. L'*«entrée»* non autorisée de données correctes ou incorrectes entraîne une situation qui correspond à la création d›un faux document. Les altérations ultérieures (modifications, variations, changements partiels), les effacements (retrait de données d›un support de données) et la suppression (retenue, dissimulation de données) correspondent en général à la falsification d'un document authentique. L'infraction de la section 3 engloberait la contrefaçon informatique qui résulte en de *«fausses informations»* ou une *«fausse production»*. L›envoi d›un document contrefait ou l›altération de données (telles que celles utilisées pour le hameçonnage) serait suffisant(e) pour une condamnation. Une infraction de contrefaçon dans l'article 7 de la CB nécessite une intention que les données non authentiques soient considérées comme authentiques.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	2. Écrit un programme logiciel, transfère un programme logiciel à une autre personne ou stocke un programme logiciel dans un ordinateur, afin d'entraîner la production de fausses informations ou de fausse production ou exploite un ordinateur pendant l'utilisation du programme logiciel comme susmentionné. b. Dans la présente section, «fausses informations» et «fausse production» - des informations ou une production qui peut induire en erreur conformément aux objectifs de leur utilisation.	La section 3 ne nécessite pas une telle intention – l'intention visée à l'article 7 de la CB était à la discrétion des parties et non une exigence spécifique. La section 6 concernant la production et la transmission d'un programme logiciel pour infiltrer, provoquer des dommages ou une perturbation, pourrait être utilisée pour les personnes écrivant ou envoyant un programme contrefait, mais nécessite la preuve de la perturbation ou des dommages
Article 8 de la CB[206] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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.	**Loi informatique de 1995** **Section 3**	**Étude juridique** L'objectif de l'article 8 de la CB est de criminaliser toute manipulation abusive dans le cadre d'un traitement de données avec pour intention d'effectuer un transfert illégal de propriété. L'infraction de l'article 8 de la CB doit être commise «sans droits» et un bénéfice économique doit être obtenu en résultat. Cela est destiné à empêcher la criminalisation de pratiques commerciales légitimes courantes. Par exemple, les activités effectuées conformément à un contrat valide entre les personnes affectées sont légitimes (par ex. la désactivation d'un site Internet conformément aux termes du contrat).[207]

206. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA
207. Paragraphe 89, page 15 du Rapport explicatif de la CB

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article12 de l'HIPCAR – Fraude informatique Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; • avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		L'infraction de l'article 8 de la CB doit être commise «intentionnellement». L'élément d'intention générale désigne la manipulation ou l'interférence de l'ordinateur provoquant une perte de propriété à un tiers. L'infraction nécessite également une intention frauduleuse ou malhonnête spécifique afin de retirer un bénéfice économique ou autre pour soi ou pour un tiers. Ainsi, par exemple, les pratiques commerciales relatives à la concurrence sur le marché qui peuvent provoquer un préjudice économique à une personne et bénéficier à une autre, mais ne sont pas réalisées avec une intention frauduleuse ou malhonnête, ne sont pas destinées à être intégrées dans l'infraction établie dans cet article. Par exemple, l'utilisation de programmes de recueil d'informations à des fins de comparaison pour un achat sur Internet («bots»), même si elle n'est pas autorisée par un site visité par le «bot» n'est pas destinée à être criminalisée.[208] La section 3 ne nécessite pas une intention malhonnête ou une tromperie. La section 6 pourrait être utilisée pour les personnes qui écrivent ou envoient un programme mais elle nécessite des preuves de la perturbation ou des dommages **Analyse des lacunes** **Recommandation:** Une infraction de fraude informatique spécifique est intégrée dans la Loi informatique de 1995 afin de garantir qu'une telle infraction est commise *«sans droits»* et intentionnellement – selon l'article 8 de la CB ou la section 12 de l'HIPCAR.
Article 9 de la CB[209] **Infractions se rapportant à la pornographie enfantine** **AJOUTER CONTENU ARTICLE**	**Code pénal** **Section 214**	Étude juridique La section 214 du Code pénal concerne les publications d'obscénités L'expression «matériel indécent incluant l'image d'un mineur» est l'expression israélienne pour la «pornographie infantile». - Section 214(b)
Article 10 de la CB[210] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes**	**L'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) Accord**	En tant que membre partie à l'accord ADPIC, Israël garantit qu'il dispose d'une responsabilité criminelle conforme à ses obligations

208. Paragraphe 90, page 15 du Rapport explicatif de la CB
209. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA
210. Pas d'équivalent dans la CUA et l'HIPCAR

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 11 de la CB[211] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.	**Code pénal** **Section 25** **Section 31** **Section 32**	**Étude juridique** Aider et encourager d'autres à commettre des crimes est essentiel afin de poursuivre ceux qui peuvent avoir apporté une assistance ou avoir encouragé la réalisation de cybercrimes. Les sections 31 et 32 du Code pénal incluent l'aide et l'encouragement En outre, la section 25 du Code pénal définit une tentative de commettre une infraction
Article 12 de la CB[212] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:	**Code pénal** **Section 23**	**Étude juridique** La section 23 du Code pénal vise la responsabilité criminelle d'une corporation, ainsi qu'une responsabilité civile éventuelle (violation d'une obligation légale ou négligence).

211. Article 29, paragraphe 2, sous f), de la CUA
212. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale. 2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[213] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.	**Aucun équivalent**	**Étude juridique** Il n'existe pas d'infraction similaire dans la loi israélienne - Veuillez noter qu'Israël n'a pas ratifié le Protocole supplémentaire et qu'il n'existe pas d'exigence quant à la mise en application du présent article **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 3 du Protocole Supplémentaire comme guide pour la législation nationale si nécessaire

213. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 4[214] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Code pénal** **Section 144(b)** **Section 192**	**Étude juridique** Les menaces en général sont interdites conformément à la section 192 du Code pénal et incluent les menaces raciales et non raciales. La section 144f(b) du Code pénal (crime haineux) constitue des circonstances aggravantes, qui doublent la peine maximale définie pour l'infraction à six ans d'emprisonnement.

214. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 5[215] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques. 2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Aucun équivalent**	**Étude juridique** Il n'existe pas d'infraction dans la loi israélienne - Veuillez noter qu'Israël n'a pas ratifié le Protocole supplémentaire et qu'il n'existe pas d'exigence quant à la mise en application du présent article **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 du Protocole Supplémentaire comme guide pour la législation nationale si nécessaire.

215. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 6[216] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.	**Aucun équivalent**	**Étude juridique** La loi israélienne n'inclut pas d'interdiction sur le déni de génocide ou sa justification (tant qu'il n'est pas considéré comme une incitation à la violence) - Veuillez noter qu'Israël n'a pas ratifié le Protocole supplémentaire et qu'il n'existe pas d'exigence quant à la mise en application du présent article **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 du Protocole Supplémentaire comme guide pour la législation nationale si nécessaire.

216. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à étudier		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Section 441** **Loi informatique** **Section 3**	Étude juridique Cette infraction couvre la phase préparatoire d'un crime de malhonnêteté lié à l'identité–. De tels actes peuvent constituer une infraction d'usurpation d'identité (section 441 du Code pénal) et de fausses informations (section 3 de la Loi informatique)

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Procédure Pénale (Pouvoirs** **d'application - Données de communications) 5768 - 2007** **Sections 5 et 11(a)** **Code pénal** **Section 287**	**Étude juridique** Cette infraction sanctionne les violations de données et la divulgation d'informations sensibles qui pourraient affecter les enquêtes criminelles. La section 5 conjointement avec la section 11(a) de la Procédure pénale (Pouvoirs d'application - Données de communications), 5768 - 2007 prévoient la responsabilité criminelle d'un fournisseur d'Internet qui découvre qu'un ordre lui a été délivré et qu'il agit en violation des instructions de l'ordre selon la Loi sur les données de communications. Concernant les autres ordres, la loi israélienne inclut l'infraction de violation d'une instruction juridique (section 287 du Code pénal).
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22[217] commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.	**Code pénal** **Non respect d'une ordonnance de la Cour**	**Étude juridique** Cette infraction concerne les personnes, ayant une connaissance spécifique de preuve tangible, qui refusent d'apporter leur aide. Fréquemment, les autorités policières se fient à de telles personnes pour collecter les preuves lors d'enquêtes de cybercrimes. Une infraction séparée est constituée par le défaut de fourniture de mots de passe ou d'accès à des codes vers des données ou des appareils cryptés (c'est-à-dire «*une clé vers des informations protégées*») – la section 53 de la loi anglaise régissant les pouvoirs d'enquête de 2000 (RIPA) [218] prévoit de caractériser en infraction pénale les personnes qui ne se conforment pas à une section 49 de la RIPA Avis de divulgation de la «*clé*» La violation d'une instruction juridique est une infraction selon le Code pénal israélien ou conformément au Non respect d'une ordonnance de la Cour en Israël. Cela inclut un défaut de se conformer à une instruction de fournir un mot de passe ou un code PIN.

217. Perquisition et saisie, assistance et injonctions de produire
218. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.	**Loi sur les communications (Bezeq et Transmission)** **Section 30**	**Étude juridique** L'infraction contraire à la section 30 de la Loi sur les communications criminalise les personnes qui harcèlent des personnes en ligne.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous.		**Étude juridique** Pour prouver l'infraction néerlandaise, un rendez-vous à des fins sexuelles est requis pour apporter la preuve de l'historique de discussion en ligne à caractère sexuel, une demande de rendez-vous avec preuve de la planification (c'est-à-dire la date et le lieu). Le but de la loi canadienne est d'empêcher la préparation des adultes prédateurs des enfants en ligne. Cette infraction ne nécessite pas la commission de l'infraction sexuelle. Cela signifie que l'accusé n'a pas besoin de s'être réellement présenté au rendez-vous pour rencontrer la victime en personne. L'infraction est commise avant que toute action n'ait lieu pour commettre l'infraction substantielle. **Analyse des lacunes** **Recommandation:** Nous recommandons l'inclusion dans la législation nationale pour criminaliser ce comportement prédateur avant qu'une infraction sexuelle ne soit commise

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Section 172.1** 1. 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[219] **Perquisition et saisie de données informatiques stockées** 1. 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.	**Ordonnance de Procédure Pénale (Arrestation et Recherches) [Nouvelle Version], 5729 – 1969** **Section 23A** **Pénétration de matériel informatique** **Section 32** **Pouvoir de saisie d'objets**	Étude juridique La section 23A permet la «pénétration d'un matériel informatique - selon sa signification dans la section 4 de la loi informatique 5755-1995» La section 1 de la Loi informatique définit la *«pénétration d'un matériel informatique».* La section 32 stipule qu'un policier peut saisir un *«objet»* englobant le «matériel informatique» Nonobstant, la section 32 mentionne un officiel formé, elle ne fait pas référence à la copie, la conservation du contenu des données d'origine, garantissant l'intégrité de toute preuve saisie ou rendant les données inaccessibles pour empêcher toute infraction supplémentaire. Cependant, la copie et la conservation sont réalisées de manière routinière par la Police israélienne et les informations sont conservées.

219. Article 3 de la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe l .a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou obtenir d'une façon similaire les données informatiques consultées selon les paragraphes 1 et 2. Ces mesures incluent les prérogatives suivantes: 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.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.		
Article 16 de la CB[220] **Conservation rapide des données informatiques stockées** 1. 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.	**Code de procédure pénale (données de communication) (2007)** **Article 3 et 4** **Ordonnance de procédure pénale (Arrestation et Recherches) (1969)** **Article 43**	**Étude juridique** Ce pouvoir d'enquête est important pour garantir que les données vulnérables à la suppression ou la perte sont préservées Les Articles 3 et 4 du code de procédure pénale (données de communication) (2007) concernent la préservation des données de communication. L'Article 43 de l'ordonnance de procédure pénale (Arrestation et Recherches) (1969) concerne la préservation de toutes les autres données informatiques.

220. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 17 de la CB[221] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	**Loi sur les Communications** **Article 13(b)(2)** **Code de procédure pénale (données de communication) 2007**	Étude juridique Ce pouvoir procédural est particulièrement important pour s'assurer que les FSC fournissent les adresses IP pouvant localiser l'auteur d'un cybercrime. L'article 13(b)(2) de la loi sur les communications (1982), avec les directives spécifiques de la police israélienne, permet la divulgation partielle des données de trafic avec un contrôle judiciaire conformément aux Articles 3 et 4 du Code de procédure pénale (données de communication) (2007).

221. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[222] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;	**Procédure pénale (Pouvoirs d'application - Données de communications) 5768 - 2007** **Article 3 et 4** **Ordonnance de procédure pénale (Arrestation et Recherches) (1969)** **Article 43**	**Étude juridique** Les Articles 3 et 4 de la procédure pénale (pouvoirs d'application - données de communication) 5768 - 2007 concernent la préservation des données de communication. L'article 43 de l'ordonnance de procédure pénale (Arrestation et Recherches) (1969) concerne la préservation de toutes les autres données informatiques.

222. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.		
Article 21 de la CB[223] **Interception de données relatives au contenu**	**Loi sur les écoutes téléphoniques de 1979**	**Étude juridique[224]** La loi sur les écoutes téléphoniques de 1979 permet le suivi, l'enregistrement ou la copie de conversations de tierces personnes sans le consentement d'aucun des participants soumis à la protection de la vie privée. La loi sur les écoutes téléphoniques de 1979 a été amendée en 1995 pour permettre l'équilibrage des intérêts et des droits, avec le droit à la confidentialité par l'écoute téléphonique autorisée judiciairement. La Loi de 1981 de protection de la vie privée définit les limites légales et illégales de la vie privée. Celles-ci comprennent: une limitation raisonnable de la vie privée par une autorité de sécurité dans l'exercice de ses fonctions (c'est-à-dire des enquêtes de police). Le droit à la vie privée aura priorité et des preuves obtenues illégalement ne seront pas admises comme preuves, sauf cas exceptionnels pour le maintien de la primauté du droit.[225]

223. Pas d'équivalent dans la CUA
224. EuroMed Fiche 2014 pages 82-84
225. HCJ 3815/90 Gilat v. Ministre de la Police et autres; 3816 Yefet et autres v. Ministre de la Police et autres

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Une conversation se définit en droit comme un discours, au téléphone, au téléphone mobile, sur ondes radio, par fax, par télex et au téléimprimeur **et une communication entre des ordinateurs.** La mesure peut servir au besoin pour la découverte, l'enquête ou la prévention d'une infraction dans la catégorie du crime (infractions punissables d'au moins 3 ans d'emprisonnement), ou pour la découverte ou la capture de criminels qui ont commis ces infractions, ou dans une enquête destinée à des fins de confiscation de propriété liée à ces infractions. La Loi sur l'entraide juridique entre États de 1998 permet à un État requérant de demander l'interception si celle-ci est nécessaire en rapport avec une affaire criminelle dans l'État requérant, concernant l'un des éléments suivants: 1. Une infraction qui, selon les lois de l'État requérant, est punissable de plus de 3 ans d'emprisonnement. 2. Une infraction qui, si elle est commise en Israël, aurait fourni des motifs d'autorisation de mise sur écoute téléphonique. 3. À des fins de confiscation Le président du Tribunal de première instance ou son délégué agréé est l'organisme autorisé à permettre les écoutes téléphoniques par un mandat. Une requête de mandat tel que mentionné doit être déposée par un officier de police ayant un grade de commandant (Nitzav Mishneh) et supérieur. La requête doit être déposée en utilisant un formulaire standard et doit mentionner, entre autres, la base factuelle sur laquelle la requête est basée, les raisons de la requête et les détails de l'action requise. La requête doit être entendue ex parte.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Le permis dans le mandat doit être fourni une fois que l'organisme compétent a pris en compte la gravité de la violation de la vie privée et la mesure est nécessaire pour la découverte, l'enquête et la prévention d'une infraction dans la catégorie du crime (infractions punissables d'au moins 3 ans d'emprisonnement), ou pour la découverte ou la capture de criminels qui ont commis ces infractions, ou dans une enquête destinée à des fins de confiscation de propriété liée à ces infractions. Le permis doit spécifier l'identité de la personne, l'identité de la ligne ou de l'installation, la place ou le type de conversations et les méthodes de mise sur écoute. La durée du permis ne dépassera pas trois mois, et elle peut être prolongée périodiquement. Une fois par mois, le Commissaire de police établira un rapport sur les permis émis. Le Commissaire de police a le droit de délivrer un permis urgent pour 48 h en cas d'absence de délai pour obtenir un permis, et ce dernier est nécessaire, pour la prévention d'un crime et pour la découverte de son auteur. Le Commissaire doit rendre compte immédiatement au Procureur général lors de la délivrance du permis, et ce dernier a le droit de le révoquer. En vertu de la loi, les requêtes entrantes d'entraide juridique dans des affaires criminelles peuvent être reçues par la Direction de la Cour, le Directeur du Service des affaires internationales ou le Bureau du Procureur de l'État ou l'inspecteur général de la police israélienne ou le Chef de la Division des renseignements. En pratique, les requêtes sont envoyées au Conseil d'administration des Tribunaux puis transmises par ces derniers à l'Unité d'entraide judiciaire de la Police israélienne qui supervise l'exécution des requêtes par les autorités compétentes.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Dans certains cas, l'Unité d'entraide juridique doit consulter le Département des affaires internationales concernant l'exécution d'une requête. Tandis que les décisions concernant l'exécution des requêtes peuvent être prises par le Service des affaires internationales du Bureau du Procureur de l'État et par l'Unité d'entraide judiciaire, seul le Ministre de la Justice est autorité à refuser une requête entrante. Une requête d'entraide judiciaire doit préciser le type de procédure pour lequel l'assistance est demandée, les faits qui constituent la base pour la suspicion de la commission d'une infraction et le rapport avec l'assistance demandée. Dans une requête d'assistance de ce type, il convient d'examiner, entre autres si elle est conforme aux exigences de la loi israélienne pour l'émission d'un mandat pour des écoutes téléphoniques, de la manière susmentionnée. La Police exécute les mesures demandées dans le cadre de la requête.
Article 20 de la CB[226] **Collecte en temps réel des données relatives au trafic** 1. 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	**Procédure pénale (Pouvoirs d'application - Données de communications) 5768 - 2007** **Article 3(g)** **Loi sur les communications (1982)** **Article 13(b)(2)**	**Étude juridique** L'article 3(g) de la Procédure pénale (Pouvoirs d'application - Données de communications) 5768 - 2007 et l'article 13(2)(b) de la Loi israélienne sur les Communications (1982) permettent le recueil des données de trafic en temps réel.

226. Article 31, paragraphe 3, sous e), de la CUA – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Disclosure of encryption keys		**Étude juridique** Les terroristes et les membres du crime organisé utilisent régulièrement des applications de messagerie cryptées[227] cela peut donc être considéré comme un pouvoir viable pour dévoiler les clés des mots de passe afin de déverrouiller les appareils[228] **Analyse des lacunes** **Recommandation:** Il n'existe pas de pouvoirs de décryptage en Israël – une telle disposition est recommandée pour permettre aux autorités d'application de la loi de contraindre les propriétaires à fournir les codes PIN et les mots de passe afin de déverrouiller les appareils
Data retention obligations		**Étude juridique** Un tel pouvoir peut permettre aux autorités policières de 1. Tracer et identifier la source d'une communication 2. Identifier la destination d'une communication; 3. Identifier la date, l'heure et la durée d'une communication; et 4. Identifier le type de communication Les lois israéliennes sur la protection et la confidentialité des données ne comprennent pas de limitations spécifiques concernant la période pendant laquelle les registres doivent être conservés. Cependant, des exigences spécifiques existent pour certaines sortes de données, comme les données médicales (en particulier dans les hôpitaux) et les données de crédit, qui prévoient que les données relatives doivent être conservées pendant des durées minimales spécifiques. De même, dans le cadre de projet de directives publié par l'Autorité israélienne pour le droit, l'information et les technologies (ILITA) concernant les numéros d'identification, ILITA a interprété le terme 'consentement' d'un individu comme signifiant le consentement d'un individu à ce que les dossiers soient conservés aussi longtemps que nécessaire (et pas plus). Aucune restriction explicite n'a été imposée sur la période pendant laquelle une organisation peut (ou doit) conserver des dossiers.

227. Eleanor Saitta. «Le cryptage peut-il nous sauver?» Nation 300, n° 24 (15 juin 2015): 16-18. Academic Search Premier, EBSCOhost (dernier accès le 29 février 2016).
228. En guise d'exemple, voir la section 49 de la loi anglaise régissant les pouvoirs d'enquête 2000 (GB) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB[229] **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État. 2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.	**Loi pénale de 1977** **Article 7(a)(1)** **Article 7(c)** **Article 15(a)**	**Étude juridique** La législation nationale garantit que la juridiction est définie en utilisant les termes de l'article 22 de la CB (soumis à la réserve par Israël sur le paragraphe 1.d.) S'il existe un conflit entre des juridictions, il convient de tenir compte des directives quant à la détermination de la juridiction appropriée pour poursuivre une infraction – consulter les directives Eurojust permettant de décider quelle juridiction doit poursuivre (révisées en 2016)[230]

229. Pas d'équivalent dans la CUA
230. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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.		
Article 35 de la CB	**En place**	**Étude juridique** Il s'agit d'un mécanisme essentiel pour assurer une capacité d'enquête sur la cybercriminalité internationale efficace et constitue une exigence obligatoire de la ratification de la CB Le National Cyber Center à Lahav 433 (NCC) fonctionne comme la CB le requiert dans le cadre du réseau 24/7.
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.	**Loi sur l'entraide judiciaire internationale 5758-1998** **Sections 2-11** **Section 5(a)(4)** **Section 8(b)**	**Étude juridique** L'Article 25 de la CB garantit qu'il peut être utilisé comme un instrument pour faciliter la MLA pour Israël. La loi sur l'entraide judiciaire internationale 5758-1998 La section 8(b) prévoit que toute requête d'entraide judiciaire d'un État étranger doit être exécutée uniquement si l'acte est autorisé selon le droit israélien. Conformément à la section 5(a)(4) de la Loi sur l'entraide judiciaire internationale 5758-1998, le Ministre israélien de la justice peut refuser une requête d'entraide judiciaire si la requête est basée sur une infraction fiscale. Cependant, les infractions des sections 2 à 11 de la convention sont exclues de l'expression *«infraction fiscale»*, car elle est définie dans la section 1 de la Loi sur l›entraide judiciaire internationale 5758-1998

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication. 4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.		Il convient d'étudier le fait de permettre aux autorités juridictionnelles d'autoriser l'application du droit national afin d'enquêter dans l'État dans lequel l'accès à un appareil est connu. L'accessibilité des informations constitue le critère essentiel pour lancer une enquête dans des situations dans lesquelles il n'est pas possible de savoir où les données sont stockées (c'est-à-dire dans le cloud). Elle pourrait comprendre une «*reconnaissance mutuelle*» des décisions de justice émises à l'encontre des fournisseurs de service de communications dans un État donné, qui pourraient être remise aux filiales des FSC situées dans d'autres États, en fonction de l'endroit où les données sont stockées.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de la CB[231] **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre. 2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.	**Aucun équivalent**	Étude juridique Il s'agit d'une procédure importante afin de permettre à un État ayant connaissance d'informations qui aideraient un autre État à empêcher un cybercrime ou à enquêter sur celui-ci. Israël peut partager ces informations si cela est approprié.

231. Il n'existe pas de disposition équivalente dans la CUA.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b. b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.	**Aucun équivalent**	Étude juridique Ce pouvoir procédural permet à un État de garantir le contenu stocké dans un autre État dans des circonstances limitées. L'article 32.b. de la CB constitue une exception au principe de territorialité et permet l'accès transfrontalier unilatéral sans besoin d'entraide judiciaire en cas d'accord ou quand l'information est publiquement disponible. Les exemples d'usage de ce pouvoir procédural conformément à l'article 32.b de la CB comprennent : L'adresse électronique d'une personne peut être enregistrée dans un autre pays par un fournisseur de service, ou une personne peut enregistrer sciemment des données dans un autre pays. Ces personnes peuvent récupérer les données et à condition qu'elles en aient l'autorité légitime, elles peuvent volontairement divulguer les données à des officiels d'application de la loi, ou permettre à ces officiels d'accéder aux données[232] Un terroriste présumé est arrêté légalement pendant que sa boîte de réception électronique – contenant éventuellement des preuves d'un crime – est ouverte sur sa tablette, son smartphone ou un autre appareil. Si le suspect consent volontairement à ce que la police accède à son compte et si la police est sûre que les données de la boîte de réception sont situées dans un autre État, la police peut accéder aux données selon l'article 32.b. Si les informations sont en source ouverte (comme sur Facebook), il n'existe pas d'interdiction concernant le recueil - toute personne est autorisée à accéder à ces pages, y compris un officier de police. La police israélienne demande également de façon courante le consentement afin d'obtenir des données informatique stockées dans une autre juridiction.

232. Paragraphe 294, page 53 du Rapport explicatif de la CB

Jordanie

La Jordanie a ratifié la CITO et a récemment promulgué la Loi sur la cybercriminalité n° 27 de 2015.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[233] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi sur les cybercrimes N° 27 de 2015** **Article 3** A. Quiconque accède de façon intentionnelle à un réseau d'informations de quelque manière que ce soit sans autorisation ou en violation ou en dépassant son autorisation. **Article 12(a)** a. Quiconque est entré intentionnellement sans permis ou en violation ou en dépassant son autorisation sur Internet ou un système d'informations par quelque moyen que ce soit afin d'obtenir les données ou informations non disponibles pour le public et affecte la sécurité nationale ou les relations étrangères du Royaume, la sécurité publique ou l'économie nationale	Étude juridique Il est fait référence à un accès illégal à un *«réseau d›informations»* qui est défini dans l'article 2 comme «une corrélation entre plusieurs systèmes d›informations pour permettre l›accès à des données et informations, ainsi qu›au système». Un *«Système d›informations»* est défini dans l'article 2 comme «des programmes et outils développés pour établir un ensemble de données ou d›informations par voie électronique ou envoyés, reçus ou traités ou stockés ou gérés ou affichés par un moyen électronique.» L'infraction de l'article 12(a) prend une forme aggravée pour un accès illégal à des ordinateurs associés à une infrastructure critique. **Analyse des lacunes** **Recommandation:** La traduction de la législation n'est pas claire - mais la définition d'un réseau d'informations semble similaire à celle d'un système informatique[234] dans la CB car elle implique le traitement de données. Dans ce cas, le présent article est conforme aux normes internationales.

233. Article 6 de la CITO et article 29, paragraphe 1, de la CUA

234. Voir article 1.a. de la CB: «tout dispositif ou un groupe de dispositifs interconnectés ou associés dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques»ou la section 3(5) de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou associés, y compris par Internet, dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques ou toute autre fonction».

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[235] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.	**Loi sur les cybercrimes N° 27 de 2015** **Article 5** Quiconque capture, interfère ou intercepte intentionnellement ce qui est transmis par le biais d'un réseau d'informations ou de tout système d'informations	**Étude juridique** Cette infraction est essentielle afin de poursuivre les transmissions de données informatiques vers, depuis ou au sein d'un système informatique qui peuvent être interceptées illégalement afin d'obtenir des informations (par ex. wikileaks ou Panama Papers). L'infraction telle que projetée est conforme aux Bonnes pratiques internationales

235. Article 29, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 4 de la CB[236] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.	**Loi sur les cybercrimes N° 27 de 2015** **Article 3(b) et (c)** b. Lorsque l'accès visé dans le paragraphe (a) du présent article est destiné à annuler, effacer, ajouter, anéantir, dévoiler, détruire, obscurcir, amender, modifier, déplacer, copier et désactiver le fonctionnement d'un réseau d'informations c. Quiconque est entré intentionnellement dans un site Internet pour changer ou annuler ou anéantir ou modifier son contenu ou son activité ou usurper l'identité décrite ou usurper l'identité du propriétaire **Article 12(c)** Si l'entrée visée au paragraphe (a) du présent article a été réalisé avec l'intention d'annuler de telles données ou informations, endommager, détruire ou altérer, changer ou déplacer ou copier ou dévoiler	**Étude juridique** L'article 3(b) fait référence à l'infraction de l'article 3(a) et l'accès à un réseau d'informations sans autorisation avec l'intention de perturber les données. Les articles 3(c) en relation avec un site Internet ne mentionnent pas l'interférence des données «sans autorisation» La CB mentionne «sans droit» dans l'Article 4 sur la base de la non autorisation de l'accès. Le Rapport explicatif de la CB a confirmé la dérivation de l'expression *«sans droit»* comme *«une conduite entreprise sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou une conduite autrement non couverte par des défenses, des excuses, des justifications ou des principes pertinents juridiques établis dans le cadre de la loi nationale.»*.[237] La législation nationale n'inclut pas la suppression de données informatiques qui est un élément de hameçonnage fréquemment utilisé pour obtenir un accès illégal par installation d›un enregistreur de frappe afin d›obtenir des informations sensibles.[238] L'article 12(c) concerne une infraction aggravée d'interférence de données affectant une infrastructure critique (paragraphe 12(a) mentionne sans autorisation). **Analyse des lacunes** **Recommandation:** La législation nationale devrait ajouter l'acte de «*suppression*» «*Sans autorisation*» devrait être inclus dans l'article 3(c) pour qu'il soit conformé à l'article 3(b). Actuellement, le projet de loi mentionne une stricte infraction de responsabilité, un accusé pourrait donc être condamné pour une modification quelconque d'un site Internet. La Police judiciaire serait protégé par l'article 13(b) – mais d'autres personnes pouvant aider les enquêtes ou ceux qui modifient de façon légitime les données dans des sites Internet ne seraient pas protégés.

236. Article 29, paragraphe 1, sous e) à f), de la CUA
237. Paragraphe 38, page 8 du Rapport explicatif à la Convention sur la cybercriminalité – N°185 https://rm.coe.int/16800cce5b
238. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 5 de la CB[239] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.	**Loi sur les cybercrimes N° 27 de 2015** **Article 4** Quiconque entre ou utilise intentionnellement des programmes par Internet ou par l'utilisation d'un système d'informations afin d'annuler ou d'effacer, ajouter ou détruire, dévoiler ou anéantir, obscurcir ou amender, modifier ou transférer, copier, capturer ou pour permettre à d'autres de voir les données ou les informations, inhiber ou interférer ou fermer ou perturber le travail d'un système d'informations ou accéder ou changer le site Internet ou annuler ou détruire ou modifier son contenu ou usurper l'identité du propriétaire sans autorisation ou en outrepassant son autorité	Étude juridique L'article 4 prévoit une infraction d'interférence du système. Tandis que l'interférence des données et l'accès illégal disposent d'une infraction aggravée pour affecter l'infrastructure critique, il n'existe pas d'équivalent pour l'interférence du système. **Analyse des lacunes** **Recommandations:** Une autre infraction doit être examinée pour la prévention et la poursuite d'attaques contre l'infrastructure critique qui entravent le fonctionnement d'un système informatique – par exemple entraver le système qui stocke les dossiers de bourse pour les rendre inexacts.[240] Il est fait référence aux «*sites Internet*» ou à un «*système d'informations*», examiner la référence à des «*systèmes informatiques*» ou «*réseaux informatiques*» et «*données*» – afin de se conformer à la CB et la CITO. La législation nationale devrait inclure des références aux «*systèmes informatiques*», «*réseaux informatiques*» et «*données*»
Article 6 de la CB[241] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:	**Aucun équivalent**	**Étude juridique** Cette infraction permettra des poursuites pour la production, la vente, l'obtention pour utilisation, l'importation, la distribution de codes d'accès et d'autres données informatisées utilisés pour commettre des cybercrimes. Il s'agit d'éléments souvent présents dans les poursuites en matière de logiciel malveillant. Toute infraction devra également tenir compte des appareils légitimes utilisés à des fins criminelles *(«double usage»)* – elle devra inclure la terminologie de la CB de *«principalement adapté»*

239. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
240. http://www.coe.int/en/web/cybercrime/guidance-notes
241. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus; ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.		**Analyse des lacunes** **Recommandation:** La législation nationale devrait inclure une infraction en utilisant la terminologie pertinente de la CB, de la CITO ou de l'HIPCAR pour garantir que tout accès est sans autorisation et tout appareil *«principalement» a*dapté à commettre l'infraction Veuillez noter que l'HIPCAR propose l'option de lister les appareils dans un calendrier si cela est opportun – cela pourrait être restrictif et nécessite une mise à jour en fonction des avancées technologiques. La loi nationale doit fournir une excuse raisonnable pour que les autorités policières puissent utiliser les appareils pour des techniques d'enquêtes spéciales – la terminologie de l'article 6.2. de la CB ou la section 10(2) de l'HIPCAR peut être utilisée comme guide.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article. **Article10 de l'HIPCAR – Dispositifs illégaux** 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée. **Article 10 de la CITO** **Infraction de falsification** Utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques.	**Loi sur les cybercrimes N° 27 de 2015** **Article 4** Quiconque entre ou utilise intentionnellement des programmes par Internet ou par l'utilisation d'un système d'informations afin d'annuler ou d'effacer, ajouter ou détruire, dévoiler ou anéantir, obscurcir ou amender, modifier ou transférer, copier, capturer ou pour permettre à d'autres de voir les données ou les informations, inhiber ou interférer ou fermer ou perturber le travail d'un système d'informations ou accéder ou changer le site Internet ou annuler ou détruire ou modifier son contenu ou usurper l'identité du propriétaire sans autorisation ou en outrepassant son autorité	**Étude juridique** Cette infraction désigne uniquement l'usurpation d'identité du propriétaire et ne fait pas référence à une intention malhonnête et est plus pertinente pour une infraction d'interférence du système. L'intégration de l'article 7 de la CB ou la section 11 de l'HIPCAR est conseillée pour assurer une protection contre cette infraction qui pourrait inclure un hameçonnage et un harponnage Par exemple, les données informatiques (telles que les données utilisées dans les passeports électroniques) peuvent être entrées, altérées, effacées ou supprimées, entraînant la prise en compte ou l'utilisation de données non authentiques à des fins juridiques, comme si elles étaient authentiques.[242] La Section 11(2) de l'HIPCAR vise également l'envoi de multiples messages de courrier électronique comme une infraction aggravée. Le langage dans l'article 10 de la CITO ne fait pas référence à toute intention malhonnête et nécessite que des dommages soient causés – le langage dans la CB et l'HIPCAR doit être préféré car il ne nécessite pas que des dommages soient causés. La CB et l'HIPCAR nécessitent uniquement que les données «*données non authentiques*» soient «*prises en compte*» **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 7 ou la section 11 de l'HIPCAR comme guide pour la législation nationale

242. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 11 de l'HIPCAR – Falsification informatique 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 8 de la CB[243] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi sur les cybercrimes N° 27 de 2015** **Article 6** Quiconque obtient intentionnellement et sans autorisation par le biais d'un réseau d'informations ou de tout système d'informations des données ou informations liées à des cartes de crédit ou des données ou informations utilisées pour exécuter des transactions bancaires ou financières électroniques **Article 7** Quiconque commet l'un des actes stipulés dans les articles 3, 4, 5 ou 6 de la présente loi en rapport avec un système d'informations ou un site Internet ou le réseau d'informations concernant le transfert d'argent ou la fourniture de services de paiement ou la compensation ou le règlement de l'un quelconque des services bancaires fournis par des banques et entreprises financières	**Étude juridique** Cette infraction concerne uniquement l'obtention et l'utilisation de données de transaction bancaire financière ou de carte de crédit sans autorisation. Elle ne couvrirait pas tous les types de hameçonnage ou autres types de cyber-fraude, tels que le vol d'identité. Une fraude nécessiterait une déclaration trompeuse ou une intention malhonnête – elle ne repose pas sur l'obtention ni l'utilisation des données. Une fraude informatique désigne un auteur ayant l'intention d'obtenir un bénéfice économique pour lui-même ou un tiers. Il n'est pas toujours nécessaire de prouver ou de démontrer cette perte. **Analyse des lacunes** **Recommandation:** Une infraction de fraude avec intention malhonnête est incluse pour intégrer tous les types d'activité frauduleuse liée aux ordinateurs – utiliser la section 12 de l'HIPCAR ou l'article 8 de la CB

243. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 9 de la CB[244] **Infractions se rapportant à la pornographie enfantine** **Article13 de l'HIPCAR – Pédopornographie ou pornographie infantile**	**Loi sur les cybercrimes N° 27 de 2015** **Article 9** a. Toute personne qui envoie ou dissémine intentionnellement des informations audibles ou visuelles, par le biais de systèmes d'informations ou de réseaux d'informations, contenant quelque matériel que ce soit associé à la pornographie ou l'exploitation sexuelle de personnes n'ayant pas atteint l'âge de dix-huit ans sera punie. b. Toute personne qui utilise intentionnellement un système d'informations ou un réseau d'informations pour créer, préparer, sauvegarder, afficher, imprimer ou publier ou promouvoir des activités ou actes de pornographie dans le but d'influencer les personnes n'ayant pas atteint la majorité ou les personnes en situation de handicap psychologique ou mental ou de les diriger et de les inciter à commettre un crime. c. Quiconque a délibérément utilisé un système d'informations ou réseau d'informations dans le but d'exploiter des personnes n'ayant pas atteint dix-huit ans ou qui souffrent d'un handicap psychologique ou mental, dans le cadre de la prostitution ou de la pornographie	**Étude juridique** Il s'agit d'une infraction essentielle afin de protéger les enfants du danger en criminalisant la distribution, la transmission, la mise à disposition, l'offre, la production et la possession d'images indécentes d'enfants. La législation nationale se concentre sur la distribution ou l'utilisation d'un «système d'informations ou réseau d'informations» pour créer la pornographie. Cette infraction n'inclut pas la possession ou l'offre ou la mise à disposition ou la fourniture à une autre personne. Il n'existe pas de définitions de *«pornographie», «créer», «préparer», «sauvegarder», «afficher», «imprimer», «publier»* ou *«promouvoir des activités ou actes de pornographie»* Le paragraphe c. mentionne spécifiquement l'exploitation sexuelle des enfants – mais il n'est pas spécifique à la production ou la possession d'images indécentes d'enfants **Analyse des lacunes** **Recommandation:** La terminologie de l'article 9 de la CB ou la section 13 de l'HIPCAR est préférable pour protéger les enfants et poursuivre les auteurs

244. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de la CB[245] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome),	1. Livres, brochures et autre matériel écrit. 2. Œuvres à la limite de conférences, discours et sermons. 3. Œuvres théâtrales et comédies musicales et pièces musicales et représentations théâtrales. 4. Œuvres musicales, numérotées ou non ou accompagnées de mots ou non. 5. Œuvres cinématographiques et audiovisuelles. 6. Peintures, sculpture, gravures, architecture, arts appliqués et de décoration. 7. Illustrations, cartes, dessins, esquisses et stéréotypes associés à la géographie et cartes de la surface de la terre. 8. Programmes logiciels qu'ils soient en langage source ou en langage machine C. Les poursuites incluent le titre de l'œuvre seulement si le titre est un terme actuel pour désigner le sujet de l'œuvre.	**Étude juridique** Cette disposition assure la protection de l'innovation dans le 21e siècle des PPVS, entreprises et citoyens. De plus, elle protège la collection d'œuvres littéraires ou artistiques telles que les encyclopédies, anthologies et données recueillies, sous forme lisible par machine ou sous tout autre forme et en termes de sélection et d'agencement du contenu constituant des œuvres d'art créatives. Les collections contenant des extraits choisis de poésie, de prose ou de musique ou autres pour mentionner dans ces collections la source des extraits et leurs auteurs sans préjudice aux droits des auteurs concernant chaque œuvre formant une partie de ces collections

245. Pas d'équivalent dans la CUA et l'HIPCAR

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article. **Article 17 CITO - Infractions relatives à la violation des droits d'auteur et des droits connexes** La violation des droits tels que définis dans la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel et la violation des droits connexes afférents aux droits d'auteur tels que définis par la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 11 de la CB[246] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention. **Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions** 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2du présent article.	**Loi sur les cybercrimes N° 27 de 2015** **Article 14** Toute personne intervenant ou incitant intentionnellement ou conjointement à commettre l'un quelconque des crimes stipulés dans la présente Loi, la peine spécifiée dans les présentes pour les auteurs punis s'applique	Étude juridique Aider et encourager d'autres à commettre des crimes est essentiel afin de poursuivre ceux qui peuvent avoir apporté une assistance ou avoir encouragé la réalisation de cybercrimes. L'article 19 de la CITO contient également la tentative qui n'est pas mentionnée dans l'article 14 **Analyse des lacunes** **Recommandation:** Intégrer l'article 19 de la CITO (où il n'existe aucune référence à la tentative en Jordanie) comme guide pour la législation nationale

246. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 12 de la CB[247] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale. 2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.	**Code de Procédure pénale**	**Étude juridique** Cette disposition constitue un élément essentiel afin que des personnes morales (par ex. des entités professionnelles) agissant pour le compte de personnes physiques disposent d'une responsabilité pénale

247. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[248] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.	**Code pénal**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 3 du Protocole Supplémentaire comme guide pour la législation nationale lorsque des lacunes sont identifiées

248. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.		
Protocole additionnel **Article 4[249] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Article 278** Une peine d'emprisonnement pour une durée ne dépassant pas trois mois ou une amende ne dépassant pas vingt dinars sera prononcée pour: 1. Publication d'un document imprimé, manuscrit, image, dessins ou symbole qui insulterait le sentiment religieux d'autres personnes ou insulterait leur croyances religieuses; 2. Tenue d'un discours sur un lieu public et pouvant être entendu par d'autres personnes avec des mots ou un ton qui insulterait le sentiment religieux ou les croyances d'une autre personne	**Étude juridique** L'article 278 est lié à l'article 15 de la Loi sur les crimes électroniques n° 27 de 2015 qui stipule que toute personne qui commet un crime punissable selon une législation applicable quelconque en utilisant le réseau d'informations ou tout système d'informations ou site Internet ou participe ou initie ou instigue la commission de celui-ci est passible d'une peine stipulée dans la législation en question **Analyse des lacunes** **Recommandation:** L'article 278 ne mentionne que l'insulte religieuse et non l'infraction plus large de menaces xénophobes ou racistes. En outre, aucune référence n'est faite au mens rea de l'intention ou de l'absence de droits – ou d'une conduite qui serait menaçante. Utiliser la terminologie de la CB dans l'article 4 du Protocole Supplémentaire comme guide pour la législation nationale

249. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 5[250] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques. 2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Code pénal**	**Étude juridique** L'article pertinent est lié à l'article 15 de la Loi sur les crimes électroniques n° 27 de 2015 qui stipule que toute personne qui commet un crime punissable selon une législation applicable quelconque en utilisant le réseau d'informations ou tout système d'informations ou site Internet ou participe ou initie ou instigue la commission de celui-ci est passible d'une peine stipulée dans la législation en question **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 du Protocole Supplémentaire comme guide pour la législation nationale lorsque des lacunes sont identifiées

250. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 6[251] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie. 2. Une Partie peut:	**Code pénal**	**Étude juridique** L'article pertinent est lié à l'article 15 de la Loi sur les crimes électroniques n° 27 de 2015 qui stipule que toute personne qui commet un crime punissable selon une législation applicable quelconque en utilisant le réseau d'informations ou tout système d'informations ou site Internet ou participe ou initie ou instigue la commission de celui-ci est passible d'une peine stipulée dans la législation en question **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 du Protocole Supplémentaire comme guide pour la législation nationale lorsque des lacunes sont identifiées

251. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à étudier		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi sur les crimes électroniques** **N° 27 de 2015** **Article 15** toute personne qui commet un crime punissable selon une législation applicable quelconque en utilisant le réseau d'informations ou tout système d'informations ou site Internet ou participe ou interfère ou instigue la commission de celui-ci est passible d'une peine stipulée dans la législation en question.	**Étude juridique** Tandis que l'article 15 criminalise toute infraction substantielle qui utilise un réseau d'informations, système d'informations ou site Internet – aucune infraction n'a été identifiée en Jordanie qui couvre la phase de préparation d'un crime de– malhonnêteté lié à l'identité. **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Étude juridique** Cette infraction sanctionne les violations de données et la divulgation d'informations sensibles qui pourraient affecter les enquêtes criminelles **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22252 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		**Étude juridique** Cette infraction concerne les personnes, ayant une connaissance spécifique de preuve tangible, qui refusent d'apporter leur aide. Fréquemment, les autorités policières se fient à de telles personnes pour collecter les preuves lors d'enquêtes de cybercrimes. Une infraction séparée est constituée par le défaut de fourniture de mots de passe ou d'accès à des codes vers des données ou des appareils cryptés (c'est-à-dire «*une clé vers des informations protégées*») – la section 53 de la loi anglaise régissant les pouvoirs d'enquête de 2000 (RIPA) 253 prévoit de caractériser en infraction pénale les personnes qui ne se conforment pas à une section 49 de la RIPA Avis de divulgation de la «*clé*» **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

252. Perquisition et saisie, assistance et injonctions de produire
253. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		**Étude juridique** Cette infraction criminalise ceux qui harcèlent des personnes en ligne– certaines juridictions peuvent prévoir des infractions de harcèlement non liées à l'informatique – mais cette infraction est recommandée pour les crimes commis en ligne. **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous.		**Étude juridique** Pour prouver l'infraction néerlandaise, un rendez-vous à des fins sexuelles est requis pour apporter la preuve de l'historique de discussion en ligne à caractère sexuel, une demande de rendez-vous avec preuve de la planification (c'est-à-dire la date et le lieu). Le but de la loi canadienne est d'empêcher la préparation des adultes prédateurs des enfants en ligne. Cette infraction ne nécessite pas la commission de l'infraction sexuelle. Cela signifie que l'accusé n'a pas besoin de s'être réellement présenté au rendez-vous pour rencontrer la victime en personne. L'infraction est commise avant que toute action n'ait lieu pour commettre l'infraction substantielle. **Analyse des lacunes** **Recommandation:** Nous recommandons l'inclusion dans la législation nationale pour criminaliser ce comportement prédateur avant qu'une infraction sexuelle ne soit commise

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Section 172.1** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[254] **Perquisition et saisie de données informatiques stockées** 1. 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.	**Loi sur les cybercrimes N° 27 de 2015**	**Étude juridique** Il s'agit du principal pouvoir d'enquête et doit faire référence à obtenir l'accès plutôt qu'à la recherche. Dans le Rapport explicatif de la CB, *«recherche»* signifie chercher, lire, inspecter ou examiner des données. Cela inclut la notion de recherche de données et de recherche (examen) dans des données. Le terme *«accès»* a une signification neutre et reflète plus précisément la terminologie informatique – en outre il est utilisé dans les articles 26 et 27 de la CITO.[255] **Analyse des lacunes** **Recommandation:** Il convient de faire référence particulière à la *saisie* telle que présentée dans l'article 27 de la CITO. Une définition de «saisir» pour garantir l'intégrité et pour des procédures spécifiques est conseillée – voir la section 3(16) de l'HIPCAR

254. Article 3 de la CUA
255. Paragraphe 191, page 33 du Rapport explicatif de la CB

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou obtenir d'une façon similaire les données informatiques consultées selon les paragraphes 1 et 2. Ces mesures incluent les prérogatives suivantes: 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.	**Article 13** A. En prenant en compte les conditions générales prescrites dans la législation en vigueur et en prenant en compte les droits personnels du prévenu, les employés de la Police judiciaire peuvent, après avoir obtenu la permission du Procureur général concerné ou du tribunal compétent, accéder partout où il existe des indications d'une utilisation afin de commettre l'une quelconque des infractions stipulées dans la loi et peuvent également inspecter l'équipement, les outils, programmes, réglementations et moyens dont les preuves suggèrent une utilisation pour commettre l'un quelconque de ces crimes et, dans tous les cas, l'employé qui a effectué l'inspection doit établir le compte-rendu de celle-ci et le soumettre au procureur compétent.	«*Saisir inclut:* • *activer tout système informatique sur site et tout support de stockage de données informatiques;* • *réaliser et conserver une copie de données informatiques, y compris par l'utilisation d'équipement sur site;* • *entretenir l'intégrité des données informatiques stockées pertinentes;* • *rendre inaccessibles ou supprimer les données informatiques sur le système informatique utilisé;* • *garder une impression de sortie des données informatiques; ou* • *saisir ou se procurer de manière similaire un système informatique, en tout ou en partie, ou un dispositif de stockage de données informatiques.*» La section 21 de l'HIPCAR prévoit une législation afin de garantir que de l'aide est apportée par ceux disposant d'une connaissance spécialiste du site des preuves pertinentes – cela peut être utilisé comme guide – voir également la section 17 de l'HIPCAR pour une infraction si l'aide est refusée sans excuse légitime

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article 20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou b. ayant été obtenus par une personne suite à une infraction, le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à:		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les *données informatiques peuvent être stockées sur le territoire du pays.* 2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2. **Article21 de l'HIPCAR – Assistance** Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à:		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; • accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; • obtenir et copier ces données informatiques; • utiliser l'équipement pour faire des copies; et • obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci; b. un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe 1 de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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; d. enlever ou rendre inaccessibles ces données du système informatique consulté.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes 2 et 3 de l'article 26 de la présente Convention.		
Article 16 de la CB[256] **Conservation rapide des données informatiques stockées** 1. 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.		**Étude juridique** Ce pouvoir d'enquête est important pour garantir que les données vulnérables à la suppression ou la perte sont préservées. **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré de conserver les BSI, les métadonnées et le contenu enregistré et transactionnel est essentiel dans le cadre des enquêtes sur la cybercriminalité pour s'assurer que des preuves sont disponibles pour la recherche, l'accès, la saisie et la vérification. La terminologie de l'article 16 de la CB, section 23 de l'HIPCAR ou l'article 23 de la CITO pourrait être utilisée. Il convient également d'ajouter des définitions de *«données informatiques»*,[257] *«informations d›abonnés ou BSI»*, *«données de trafic»*[258] *et «Fournisseur de service de communication»*[259] Il convient de noter que la CB et l'HIPCAR ne fournissent pas de définition de BSI – mais la CITO en fournit une pour informations d'abonnés:[260]

256. Pas d'équivalent dans la CUA
257. Voir article 1.b. de la CB **ou** section 3(6) de l'HIPCAR
258. Voir Article 1.d de la CB: «toutes les données informatiques associées à la communication par le biais d›un système informatique, générées par un système informatique faisant partie intégrante d›une chaîne de communication, indiquant l›origine de la communication, sa destination, sa voie, l›heure la date, la taille, la durée ou le type de service sous-jacent» **ou** la section 3(18) de l'HIPCAR: «Le trafic de données désigne toutes les données informatiques qui: a. sont associées à la communication par le biais d›un système informatique; et b. sont générées par un système informatique faisant partie intégrante d'une chaîne de communication; et c. indiquent l'origine de la communication, sa destination, sa voie, l›heure, la date, la taille, la durée ou le type de service sous-jacent.»
259. Voir Article 1.c. de la CB: «i toute entité publique ou privée qui fournit aux utilisateurs de son service la capacité de communiquer par le biais d'un système informatique et ii toute autre entité qui traite ou stocke des données informatiques pour le compte de tels services de communication ou utilisateurs de tels services»
260. Voir article 2(9) de la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.	**Aucun équivalent**	«*Toute information à disposition du fournisseur de service concernant les abonnés au service, à l'exception des informations par le biais desquelles les éléments suivants peuvent être connus:* a. *le type de service de communication utilisé, les exigences techniques et la période de service.* b. *L'identité de l'abonné, son adresse postale ou géographique ou son numéro de téléphone et les informations de paiement disponibles en vertu du contrat ou de l'arrangement de service* c. *Toute autre information sur le site d'installation de l'équipement de communication en vertu du contrat de service.*» Il convient de tenir compte que la durée de conservation jugée raisonnable dans les circonstances et permettant une demande de prolongation dans des circonstances particulières – la CB et la CITO prévoient 90 jours et l'HIPCAR 7 jours. D'après l'expérience, 90 jours est trop court dans une enquête de cybercriminalité, le chiffre devrait se rapprocher de 180 jours puis être soumis à prolongation.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article23 de l'HIPCAR – Conservation rapide Si un [agent de répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		
Article 17 de la CB[261] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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	**Aucun équivalent**	**Étude juridique** Ce pouvoir procédural est particulièrement important pour s'assurer que les FSC fournissent les adresses IP pouvant localiser l'auteur d'un cybercrime. Le questionnaire confirme que les données peuvent être conservées lors de la réception d'un LOR **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré concernant la divulgation de données de trafic devrait être inclus dans la législation pour permettre des enquêtes efficaces sur les cybercrimes. La terminologie de l'article 17 de la CB, sections 23 et 24 de l'HIPCAR ou l'article 24 de la CITO pourrait être utilisée. Des définitions de *«données de trafic» et «Fournisseur de service de communication» seraient également requises*[262]

261. Pas d'équivalent dans la CUA
262. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 23 de l'HIPCAR – Conservation rapide** Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de l'HIPCAR – Divulgation partielle des données de trafic Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. a. les fournisseurs de services Internet; et/ou b. b. l'itinéraire de la communication. **Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic** Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[263] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir:	**Aucun équivalent**	**Étude juridique** Il existe une disposition cruciale pour une enquête efficace en matière de cybercrime et son absence affectera les poursuites et la coopération internationale. **Analyse des lacunes** **Recommandation:** Ce pouvoir crucial est nécessaire pour garantir que les FSC en Jordanie fournissent les BSI, les données de trafic et les données du contenu stocké. Il convient également d'ajouter des définitions de *«données informatiques», «informations d›abonnés ou BSI», «données de trafic» et «Fournisseur de service de communication».*[264] L'article 25 de la CITO est un modèle qui pourrait être utilisé et utilise différentes définitions incluant *«technologie de l›information»,*[265] *«fournisseur de service»*[266] *et «données»*[267] – nous recommandons d'ajouter des définitions pour *«informations d›abonnés ou BSI», «données de trafic»* car il existe différents types de preuves pouvant être fournies par les FSC. En outre, ce pouvoir obligera les individus et les tiers (tels que les entreprises, les institutions financières et les autres organismes) qui détiennent des données à les produire aux autorités policières. L'article 18 de la CB et la section 22 de l'HIPCAR pourraient constituer un guide avec une application cohérente des définitions

263. Pas d'équivalent dans la CUA
264. Voir les définitions ci-dessus
265. Article 2(1) de la CITO: «*tout matériel ou moyen virtuel ou groupe de moyens interconnectés utilisés pour stocker, trier, disposer, développer et échanger des informations conformément à des commandes et des instructions stockées à l'intérieur. Cela inclut toutes les entrées et sorties associées, au moyens de câbles ou sans fil, dans un système ou un réseau.*»
266. Article 2(2) de la CITO: «toute personne physique ou morale, publique ou privée, qui fournit à des abonnés les services nécessaires pour communiquer par le biais de la technologie de l'information ou pour traiter ou stocker des informations pour le compte du service de communication ou de ses utilisateurs.»
267. Article 2(3) de la CITO: «tout ce qui peut être stocké, traité, généré et transféré par le biais de la technologie de ›information, comme des nombres, lettres, symboles, etc…»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: a. à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou b. à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[268] **Interception de données relatives au contenu** **Article 26 HIPCAR** **Article 29 de la CITO - Interception de données relatives au contenu**	**Loi sur les cybercrimes N° 27 de 2015**	**Étude juridique** Cet article permet à la Police judiciaire d'intercepter les communications avec l'autorisation du Procureur général **Analyse des lacunes** **Recommandations:** *Il* conviendrait obliger les FSC opérant en Jordanie à coopérer à la collecte en temps réel des contenus pour l'ensemble des crimes. De même, des garanties devraient être incorporées afin d'assurer que l'interception et la collecte se fassent selon des modalités légales, raisonnables et proportionnelles. Il faudrait envisager d'étudier l'article 29 de la CITO, l'article 21 de la CB et la section 26 de l'HIPCAR, afin d'en incorporer les termes dans la législation nationale

268. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	Article 13 A. En prenant en compte les conditions générales prescrites dans la législation en vigueur et en prenant en compte les droits personnels du prévenu, les employés de la Police judiciaire peuvent, après avoir obtenu la permission du Procureur général concerné ou du tribunal compétent, accéder partout où il existe des indications d'une utilisation afin de commettre l'une quelconque des infractions stipulées dans la loi et peuvent également inspecter l'équipement, les outils, programmes, réglementations et moyens dont les preuves suggèrent une utilisation pour commettre l'un quelconque de ces crimes et, dans tous les cas, l'employé qui a effectué l'inspection doit établir le compte-rendu de celle-ci et le soumettre au procureur compétent.	

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	B. Sous réserve du paragraphe (a) du présent article, prendre en compte les droits des autres bona fide, à l'exclusion de ceux accordés selon les dispositions de la Loi sur les télécommunications, qui n'ont pas participé à une infraction quelconque selon le présent Acte, les employés de la Police judiciaire peuvent contrôler les appareils, outils, programmes, systèmes et moyens utilisés pour commettre l'un quelconque des crimes stipulés ou couverts par la présente loi et l'argent gagné à la suite de ceux-ci et conserver les informations et les données associées à la commission de ceux-ci. C. Le tribunal compétent peut statuer sur la confiscation des équipements et outils, l'arrêt ou la perturbation du travail de tout système d'informations ou site Internet utilisé pour commettre l'une quelconque des infractions visées ou couvertes par la présente loi, la confiscation de l'argent gagné grâce à ces crimes et la décision de retirer la violation aux frais de l'auteur.	

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 20 de la CB[269] **Collecte en temps réel des données relatives au trafic** 1. 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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.	**Aucun équivalent**	**Étude juridique** Il n'existe pas de pouvoir procédural pour collecter les données de trafic en temps réel. Il pourrait exister un seuil plus bas pour collecter des données de trafic en temps réel, ce qui constitue un outil d'enquête essentiel. Il pourrait exister des situations où un seuil légal plus élevé pour accéder aux contenus pourrait ne pas être compris par un demandeur – mais un seuil plus bas pour accéder au trafic pourrait l'être. Aussi, il devrait exister une distinction entre la collecte en temps réel de contenus stockés et de données de trafic. Il s'avère nécessaire de créer des garanties et des exigences/ procédures pour contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques en Jordanie **Analyse des lacunes** **Recommandations:** Il conviendrait de disposer d'un pouvoir spécifique pour collecter les données de trafic en temps réel et d'obliger les FSC opérant en Jordanie à coopérer à la collecte en temps réel des données de trafic. De même, des garanties devraient être intégrées afin d'assurer que la collecte soit légale, raisonnable et proportionnelle au vu des circonstances. La terminologie de l'article 28 de la CITO pourrait être envisagée, mais elle ne fait pas allusion à la collecte rapide en temps réel uniquement. L'article 20 de la CB et la section 25 de l'HIPCAR devraient être utilisés comme guide pour la législation nationale

269. Article 31, paragraphe 3, sous e), de la CUA – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 25 de l'HIPCAR - Collecte des données de trafic** 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		
		Obligation de divulgation des clés de cryptage Les terroristes et les membres du crime organisé utilisent régulièrement des applications de messagerie cryptées[270] cela peut donc être considéré comme un pouvoir viable pour dévoiler les clés des mots de passe afin de déverrouiller les appareils[271] **Analyse des lacunes** **Recommandation:** Impossible de clarifier l'existence de tels pouvoirs en Jordanie – cela permettra aux autorités d'application de la loi d'obliger les propriétaires à déverrouiller les appareils

270. Eleanor Saitta. «Le cryptage peut-il nous sauver?» Nation 300, n° 24 (15 juin 2015): 16-18. Academic Search Premier, EBSCOhost (dernier accès le 29 février 2016).
271. En guise d'exemple, voir la section 49 de la loi anglaise régissant les pouvoirs d'enquête 2000 (GB) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations de conservation des données[272] Un tel pouvoir peut permettre aux autorités policières de 1. Tracer et identifier la source d'une communication 2. Identifier la destination d'une communication; 3. Identifier la date, l'heure et la durée d'une communication; et 4. Identifier le type de communication La Jordanie ne dispose pas d'une telle obligation[273]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB[274] **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.	**Aucun équivalent**	**Étude juridique** Sans cadre clairement défini pour les infractions de cybercriminalité, qui sont de nature internationale, toute législation sera restreinte. **Analyse des lacunes** **Recommandation:** La législation nationale garantit que la juridiction est définie en utilisant les termes de l'article 22 de la CB, de la section 19 de l'HIPCAR ou de l'article 30 de la CITO. S'il existe un conflit entre des juridictions, il convient de tenir compte des directives quant à la détermination de la juridiction appropriée pour poursuivre une infraction – consulter les directives Eurojust permettant de décider quelle juridiction doit poursuivre (révisées en 2016)[275]

272. En 2006, selon la directive de conservation des données - les États Membres de l'UE devaient stocker les données de télécommunications électroniques pendant au plus 6 mois pour enquêter, détecter et poursuivre des crimes graves. En 2014, la Cour de Justice de l'UE a invalidé la directive de conservation des données, arguant qu'elle fournissait des garanties insuffisantes contre les interférences avec les droits à la vie privée et la protection des données. Pour consulter les protocoles nationaux, voir: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
273. Examen global ICMEC page 29
274. Pas d'équivalent dans la CUA
275. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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. **Article 19 de l'HIPCAR – Juridiction** La présente loi s'applique à tout acte ou omission commis: a. a. sur le territoire de [État prenant les dispositions]; b. b. sur un bateau ou un avion immatriculé en [État prenant les dispositions]; c. c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 43 de la CITO **Autorité spécialisée**[276] 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. 2. a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.	**Aucun équivalent**	Étude juridique Il s'agit d'un mécanisme essentiel pour disposer d'une aptitude efficace à l'enquête de cybercrimes. **Analyse des lacunes** **Recommandation:** La mise en œuvre ne devrait pas nécessiter de législation et, en fonction des ressources, cette mesure devrait être établie en priorité. Les coordonnées doivent être partagées pour le point de contact unique (SPOC) nommé au niveau national, au niveau international pour les autorités centrales et INTERPOL. Il convient également de tenir compte de l'élaboration d'un Mémorandum de compréhension avec les agences nationales, afin que le SPOC dispose d'une autorité pour entreprendre les actions requises dans le cadre d'une enquête de cybercriminalité internationale appliquant les traités et lois nationaux. Ce MOU doit comprendre les requêtes entrantes et sortantes et garantir un processus efficace et effectif.

276. Article 35 de la CB et article 25, paragraphe 2, de la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35. 3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.		**Étude juridique** L'article 32 de la CITO garantit qu'il peut être utilisé comme un instrument pour faciliter la MLA et assure une préservation accélérée des données informatiques enregistrées[277], une préservation accélérée et une divulgation partielle des données de trafic[278] et une divulgation des données enregistrées[279] et des données de trafic [280] aux États qui ont ratifié la CITO. **Analyse des lacunes** **Recommandation:** Il est recommandé de légiférer pour les pouvoirs procéduraux dans la CITO au plan national, afin qu'ils puissent être utilisés pour des enquêtes nationales et qu'ils soient en outre réciproques afin que les États n'ayant pas ratifié la CITO puissent les utiliser. La CITO ne prévoit pas d'interception de contenu et de données de trafic en temps réel – cela doit être pris en compte dans l'application des précédents dans la BC et l'HIPCAR.[281] Il convient d'étudier le fait de permettre aux autorités juridictionnelles d'autoriser l'application du droit national afin d'enquêter dans l'État dans lequel l'accès à un appareil est connu. L'accessibilité des informations constitue le critère essentiel pour lancer une enquête dans des situations dans lesquelles il n'est pas possible de savoir où les données sont stockées (c'est-à-dire dans le cloud). Elle pourrait comprendre une «*reconnaissance mutuelle*» des décisions de justice émises à l'encontre des fournisseurs de service de communications dans un État donné, qui pourraient être remise aux filiales des FSC situées dans d'autres États, en fonction de l'endroit où les données sont stockées.

277. Article 29 de la CB et Article 37 de la CITO
278. Article 30 de la CB et Article 38 de la CITO
279. Article 31 de la CB et Article 39 de la CITO
280. Article 33 de la CB et Article 41 de la CITO
281. Articles 33 et 34 de la BC et sections 25 et 26 de l'HIPCAR

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles; c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires. 6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL. c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		
Article 26 de la CB[282] **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.	**Aucun équivalent**	**Étude juridique** Il s'agit d'une procédure importante afin de permettre à un État ayant connaissance d'informations qui aideraient un autre État à empêcher un cybercrime ou à enquêter sur celui-ci. Bien qu'elle soit disponible entre les États ayant ratifié la CITO dans l'article 33 de la CITO, la Jordanie ne dispose pas de base juridique pour le partage de ces informations avec les États non membres de la CITO, à moins qu'une requête officielle ne soit envoyée par le biais des canaux MLA classiques. L'article 18(4)-(5) de la CNUCTO prévoit le partage d'intelligence spontané pour des questions satisfaisant la définition d'un crime grave[283], qui est transnational[284] et implique un groupe du crime organisé[285]. Sans satisfaire cette définition une requête officielle devra être envoyée par le biais des canaux MLA classiques aux États n'ayant pas ratifié la CITO. Sur la base de la rapidité de mouvement de la cybercriminalité, le partage spontané est une manière efficace de coopérer avec d'autres États et, en l'absence de partage, empêche une collaboration internationale efficace avec les États n'ayant pas ratifié la CITO.

282. Il n'existe pas de disposition équivalente dans la CUA.
283. Article 2(b), «*un «crime grave» est un acte constituant une infraction passible d'une peine privative de liberté au moins égale à quatre ans ou d'une peine plus lourde*»
284. Article 3(1) de la CNUCTO
285. Article 2(a) de la CNUCTO «*Un «groupe du crime organisé» signifie groupe structuré de trois personnes ou plus, existant pendant une certaine période et agissant de concert dans le but de commettre un ou plusieurs crimes ou infractions graves établis* conformément à la présente *Convention, afin d'obtenir, directement ou indirectement, un avantage financier ou matériel*».

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières. **Article 33 de la CITO - Informations spontanées reçues** 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		**Analyse des lacunes** **Recommandation:** Utiliser l'article 18(4)-(5) de la CNUCTO comme base pour le partage spontané d'informations qui rentre dans le cadre de la CNUCTO (sans garanties fournies en matière d'utilisation comme preuve ou de divulgation d'informations sensibles à un tiers (y compris un autre État).[286] Prendre en compte la législation basée sur l'article 33 de la CITO ou l'article 26 de la CB.

286. Voir article 33(2) de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. **Article 27 de l'HIPCAR – Logiciel de criminalistique** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes:	**Aucun équivalent**	**Étude juridique** Ce pouvoir procédural permet à un État de garantir le contenu stocké dans un autre État dans des circonstances limitées. L'article 32.b. de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permet l'accès transfrontalier unilatéral sans besoin d'entraide judiciaire en cas d'accord ou quand l'information est publiquement disponible.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le suspect de l'infraction, si possible avec ses nom et adresse; et b. une description du système informatique ciblé; et c. une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et d. les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner a. le moyen technique utilisé ainsi que la date et l'heure de l'application; b. l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et c. toute information obtenue. d. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser.		Les exemples d'usage de ce pouvoir procédural conformément à l'article 32.b de la CB comprennent : L'adresse électronique d'une personne peut être enregistrée dans un autre pays par un fournisseur de service, ou une personne peut enregistrer sciemment des données dans un autre pays. Ces personnes peuvent récupérer les données et à condition qu'elles en aient l'autorité légitime, elles peuvent volontairement divulguer les données à des officiels d'application de la loi, ou permettre à ces officiels d'accéder aux données[287] Un terroriste présumé est arrêté légalement pendant que sa boîte de réception électronique – contenant éventuellement des preuves d'un crime – est ouverte sur sa tablette, son smartphone ou un autre appareil. Si le suspect consent volontairement à ce que la police accède à son compte et si la police est sûre que les données de la boîte de réception sont situées dans un autre État, la police peut accéder aux données selon l'article 32.b. **Analyse des lacunes** **Recommandation:** Ce pouvoir restreint à récupérer unilatéralement les preuves est inclus dans la législation, ce qui garantit que le consentement de l'utilisateur est obtenu légalement.[288] La terminologie de l'article 32 de la CB et de l'article 40 de la CITO peut être utilisée. L'article 32.b. a été lourdement critiqué et il peut être envisagé que le consentement de l'État dans lequel les données informatiques stockées sont stockées soit obtenu en plus de celui de l'utilisateur. La section 27 de l'HIPCAR prévoit un logiciel judiciaire et cela peut permettre l'accès à un ordinateur dans un autre État. Il existe un certain nombre de restrictions qui nécessitent que les preuves ne puissent pas être obtenues par d'autres moyens, qu'un ordre judiciaire soit requis, qu'il ne peut s'appliquer qu'à certaines infractions et que sa durée soit limitée (3 mois). Il convient également d'examiner le consentement de l'autre État dans lequel le logiciel judiciaire peut intervenir.

287. Paragraphe 294, page 53 du Rapport explicatif de la CB
288. Il convient d'examiner des situations telles que la non disponibilité d'un utilisateur (par ex. sa mort) et si le consentement peut être obtenu dans un autre État

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect. 5. 5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20. 6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions]. 8. Un pays peut décider de ne pas mettre en œuvre l'article27. **Article 40 de la CITO - Accès transfrontière à des données informatiques** Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité.		

Liban

Le Liban a adopté la loi n° 81 relative aux transactions électroniques et aux données personnelles le 10 octobre 2018, entrée en vigueur en janvier 2019. L'équipe EuroMed Justice s'efforce de maintenir les informations mises à jour et correctes. Néanmoins, en dépit de nos efforts, et en raison des limitations temporelles et de ressources du projet en cours, une analyse des nouvelles dispositions législatives de 2018 ne sera possible que dans le cadre de la prochaine phase.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[289] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 6 de la CITO** **Article 4 de l'HIPCAR – Accès illégal** 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Aucun équivalent**	**Étude juridique** Le CITO mentionne «l›accès illégal à, la présence dans ou le contact avec» sans définir ce que ces actes signifient. La CB mentionne «sans droit» dans l'Article 2 sur la base de la non autorisation de l'accès. Le Rapport explicatif de la CB a confirmé la dérivation de l'expression *«sans droit»* comme *«une conduite entreprise sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou une conduite autrement non couverte par des défenses, des excuses, des justifications ou des principes pertinents juridiques établis dans le cadre de la loi nationale.»* Les sections Commentaires[290] sur le modèle de projet de loi HIPCAR fournissent une explication quant à l'exigence de «l›absence de justification ou d›excuse légitime» de la manière suivante, *«L'accès à un système informatique ne peut être poursuivi conformément à la Section 4, que s'il se produit en «l'absence de justification ou d'excuse légitime».* Cela nécessite que le contrevenant agisse sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) et que la conduite ne soit pas couverte autrement par des défenses, excuses, justifications ou principes pertinents juridiques établis. L'accès à un système permettant un accès libre et ouvert au public ou l'accès à un système avec l'autorisation du propriétaire ou d'un autre détenteur de droits n'est en conséquence pas de nature criminelle. Les administrateurs réseau et les entreprises de sécurité qui testent la protection des systèmes informatiques afin d'identifier des lacunes éventuelles dans les mesures de sécurité ne commettent pas un acte criminel.»

289. Article 6 de la CITO et article 29, paragraphe 1, de la CUA
290. Page 30 Section Commentaires du modèle de projet de loi HIPCAR

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête. **Article5 de l'HIPCAR – Présence illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.		La CITO mentionne «l›accès illégal à, la présence dans ou le contact avec» sans définir ce que ces actes signifient – par conséquent, il convient de privilégier la CB et l'HIPCAR. **Analyse des lacunes** **Recommandation:** *La législation nationale peut contenir un langage approprié provenant de l'Article 2 de la CB/sections 4 et 5 de l'HIPCAR afin d'inclure des définitions d'un système informatique*[291] *et l'inclusion des programmes dans la définition des données car certaines données contiennent des programmes et d'autres non. En outre, afin de se conformer aux normes internationales, la législation devrait désigné l'accès «sans droits» plutôt que frauduleusement.* *Il convient également de prendre en compte une infraction distincte consistant à rester dans un système informatique conformément à la section 5 HIPCAR.*

291. Voir article 1.a. de la CB: «tout dispositif ou un groupe de dispositifs interconnectés ou associés dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques» **ou** la section 3(5) de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou associés, y compris par Internet, dont un ou plusieurs exécute(nt), sur la base d›un programme informatique, des traitements de données automatiques ou toute autre fonction».

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[292] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. **Article6 de l'HIPCAR – Interception illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques: • toute transmission non publique vers, de, ou au sein d'un système informatique; ou • des émissions électromagnétiques provenant d'un système informatique, • commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Aucun équivalent**	**Étude juridique** Cette infraction est essentielle afin de poursuivre les transmissions de données informatiques vers, depuis ou au sein d'un système informatique qui peuvent être interceptées illégalement afin d'obtenir des informations (par ex. wikileaks ou Panama Papers). **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 3, l'HIPCAR section 6 comme guide pour la législation nationale - la terminologie de l'article 7 de la CITO est appropriée – bien qu'il n'existe pas de définition de *«données des technologies de l'information»*

292. Article 29, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut imposer que l'infraction soit commise avec une intention malhonnête ou en rapport avec un système informatique connecté à un autre système informatique ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique. **Article 7 de la CITO** **Interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques.		
Article 4 de la CB[293] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux. **Article 7 de l'HIPCAR – Atteinte à l'intégrité des données** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants:	**Aucun équivalent**	Étude juridique De la même manière que ci-dessus, pour l'accès illégal, il n'est pas fait référence dans la CITO à «*sans droits*» et cela n'inclut pas la suppression des données informatiques, qui constitue un élément d'hameçonnage afin d'obtenir un accès illégal en installant un enregistreur de frappe pour obtenir des informations sensibles.[294] **Analyse des lacunes** **Recommandation:** L'absence de certains éléments clés associés à cette infraction dans la CITO peut être corrigée en utilisant la terminologie de l'article 4 de la CB ou de la section 7 de l'HIPCAR.

293. Article 29, paragraphe 1, sous e) à f), de la CUA
294. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes; • obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Article 8 de la CITO** **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 5 de la CB[295] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. **Article9 de l'HIPCAR – Atteinte à l'intégrité du système** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: a. entrave ou porte atteinte au fonctionnement d'un système informatique; ou b. entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Aucun équivalent**	**Étude juridique** Cette infraction empêcherait les logiciels malveillants qui interfèrent avec le fonctionnement d'un ordinateur – par exemple des vers informatiques - un sous-groupe des logiciels malveillants (comme les virus informatiques). Il existe des programmes informatiques à réplication automatique qui entravent le réseau en initiant de multiples processus de transfert de données. Ils peuvent influencer les systèmes informatiques en entravant le bon fonctionnement du système informatique, en utilisant des ressources du système pour se répliquer sur Internet ou en générant du trafic réseau qui peut rendre certains services (notamment des sites Internet) indisponibles. **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 ou la section 9 de l'HIPCAR comme guide pour la législation nationale. Il convient également de s'interroger pour savoir si la prévention et la poursuite des attaques contre l'infrastructure critique nécessitent une infraction distincte ou aggravée (Section 9(2) de l'HIPCAR) par exemple, le fonctionnement d'un système informatique peut être entravé à des fins terroristes (par ex. entraver le système qui stocke des dossiers de bourse peut les rendre inexacts ou entraver le fonctionnement d'une infrastructure critique).[296]

295. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
296. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		
Article 6 de la CB[297] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Aucun équivalent**	**Étude juridique** Comme ci-dessus, concernant l'accès illégal, aucune référence n'est faite à «sans droits» Cette infraction permettra les poursuites pour la production, la vente, l'obtention pour utilisation, l'importation, la distribution de codes d'accès et autres données informatisées pour commettre des cybercrimes - par exemple l'accès à des systèmes informatiques pour faciliter une attaque terroriste en perturbant le réseau électrique d'un pays. Toute infraction devra également tenir compte des appareils légitimes utilisés à des fins criminelles *(«double usage»)* – elle devra inclure la terminologie de la CB de *«principalement adapté»* **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 ou la section 10 de l'HIPCA comme guide pour la législation nationale.

297. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		Veuillez noter que l'HIPCAR propose l'option de lister les appareils dans un calendrier si cela est opportun – cela pourrait être restrictif et nécessite une mise à jour en fonction des avancées technologiques. La loi nationale doit fournir une excuse raisonnable pour que les autorités policières puissent utiliser les appareils pour des techniques d'enquêtes spéciales – voir la terminologie de l'article 6.2. de la CB ou la section 10(2) de l'HIPCAR pour guide.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de l'HIPCAR – Dispositifs illégaux 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Aucun équivalent**	**Étude juridique** Toute infraction ou contrefaçon est poursuivie comme une infraction substantielle uniquement – l'objectif de l'article 7 de la CB est de combler les lacunes du droit pénal liées à la contrefaçon traditionnelle, qui nécessite une lisibilité visuelle des communiqués ou déclarations au sein d'un document et qui ne s'applique pas aux données stockées par des moyens électroniques. La contrefaçon informatique implique la création ou l'altération sans autorisation de données stockées de manière à leur faire acquérir une valeur probante différente dans le cadre de transactions légales, qui repose sur l'authenticité des informations contenues dans les données, peut faire l'objet d'une tromperie. L'intérêt juridique protégé est la sécurité et la fiabilité des données électroniques qui peuvent avoir des conséquences pour les relations juridiques.[298]

298. Paragraphe 81, page 14 du Rapport explicatif de la CB

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de la CITO **Infraction de falsification** Utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques. **Article11 de l'HIPCAR – Falsification informatique** 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		L'intégration de l'article 7 de la CB ou la section 11 de l'HIPCAR est conseillée pour assurer une protection contre cette infraction qui pourrait inclure un hameçonnage et un harponnage Par exemple, les données informatiques (telles que les données utilisées dans les passeports électroniques) peuvent être entrées, altérées, effacées ou supprimées, entraînant la prise en compte ou l'utilisation de données non authentiques à des fins juridiques, comme si elles étaient authentiques.[299] La Section 11(2) de l'HIPCAR vise également l'envoi de multiples messages de courrier électronique comme une infraction aggravée. Le langage dans l'article 10 de la CITO ne fait pas référence à toute intention malhonnête et nécessite que des dommages soient causés – le langage dans la CB et l'HIPCAR doit être préféré car il ne nécessite pas que des dommages soient causés. La CB et l'HIPCAR nécessitent uniquement que les données «données non authentiques» soient «prises en compte» **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 7 ou la section 11 de l'HIPCAR comme guide pour la législation nationale

299. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 8 de la CB[300] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Aucun équivalent**	**Étude juridique** Toute infraction ou fraude est poursuivie comme une infraction substantielle. La fraude informatique consiste principalement en des manipulations d'entrées, où des données incorrectes sont fournies dans l'ordinateur ou des manipulations de programmes et d'autres interférences dans le cadre du traitement des données. L'objectif de l'article 8 est de criminaliser toute manipulation abusive dans le cadre d'un traitement de données avec pour intention d'effectuer un transfert illégal de propriété.[301] La terminologie de l'article 11 de la CITO est vague, sans référence à toute intention malhonnête et nécessite une forme de *«dommages» (CITO)* sans définir ce que ces termes couvrent **Recommandation:** La terminologie dans la CB ou l'HIPCAR pour cette infraction est un bon guide pour la législation nationale

300. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA
301. Paragraphe 86, pages 14 et 15 du Rapport explicatif de la CB

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 9 de la CB[302] **Infractions se rapportant à la pornographie enfantine** **AJOUTER CONTENU ARTICLE** **Article13 de l'HIPCAR – Pédopornographie ou pornographie infantile** **AJOUTER CONTENU ARTICLE**	**Aucun équivalent**	**Étude juridique** Il s'agit d'une infraction essentielle afin de protéger les enfants du danger en criminalisant la distribution, la transmission, la mise à disposition, l'offre, la production et la possession d'images indécentes d'enfants. **Analyse des lacunes** **Recommandation:** sLa terminologie de l'article 9 de la CB ou la section 13 de l'HIPCAR constitue un guide pour la législation nationale pour protéger les enfants et poursuivre les auteurs
Article 10 de la CB[303] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**Aucun équivalent**	**Étude juridique** Les autorités d'application de la loi utilisent les infractions en matière de droits d'auteur numériques dans le monde entier comme conduite criminelle supplémentaire pour enquêter sur et poursuivre différentes formes de cybercriminalité (y compris les crimes tels que le hameçonnage, la fraude électronique, la contrefaçon électronique, les sites Internet frauduleux et le vol de données/ violations de données). L'une des infractions sous-jacentes dans de nombreux cas est la violation des droits d'auteur numériques. La cyber-attaque Sony[304] ne constitue qu'un exemple récent dans lequel les infractions et pouvoirs associés à la cybercriminalité, le vol de données/espionnage industriel et la violation des droits d'auteur viennent se compléter. L'absence de toute disposition concernant la propriété intellectuelle constitue un échec dans la protection de l'innovation du 21e siècle concernant les PPVS, entreprises et citoyens. Elle peut bien sûr être protégée dans d'autres législations que la présente analyse n'a pas examinées **Analyse des lacunes** **Recommandation:** S'assurer de l'existence de protections contre la violation des droits d'auteur en conformité avec les obligations internationales.

302. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA
303. Pas d'équivalent dans la CUA et l'HIPCAR
304. https://en.wikipedia.org/wiki/Sony_Pictures_hack

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 17 CITO - Infractions relatives à la violation des droits d'auteur et des droits connexes La violation des droits tels que définis dans la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel et la violation des droits connexes afférents aux droits d'auteur tels que définis par la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel.		
Article 11 de la CB[305] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.	**Aucun équivalent**	**Étude juridique** Aider et encourager d'autres à commettre des crimes est essentiel afin de poursuivre ceux qui peuvent avoir apporté une assistance ou avoir encouragé la réalisation de cybercrimes. L'article 19 de la CITO inclut également la tentative **Analyse des lacunes** **Recommandation:** Utiliser l'article 11 de la CB et la section 19 de la CITO comme guide pour la législation nationale

305. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2du présent article.		
Article 12 de la CB[306] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale.	**Aucun équivalent**	**Étude juridique** Cette disposition constitue un élément essentiel afin que des personnes morales (par ex. des entités professionnelles) agissant pour le compte de personnes physiques disposent d'une responsabilité pénale **Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 12 comme guide pour la législation nationale

306. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[307] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 3 du Protocole Supplémentaire comme guide pour la législation nationale

307. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.		
Protocole additionnel **Article 4[308] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 4 du Protocole Supplémentaire comme guide pour la législation nationale

308. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 5[309] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques. 2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 du Protocole Supplémentaire comme guide pour la législation nationale

309. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 6[310] - Négation, minimisation grossière, approbation ou justification du génocide oudes crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie. 2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments;	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 6 du Protocole Supplémentaire comme guide pour la législation nationale

310. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à étudier		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Étude juridique** Cette infraction couvre la phase préparatoire d'un crime de malhonnêteté lié à l'identité– **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Étude juridique** Cette infraction sanctionne les violations de données et la divulgation d'informations sensibles qui pourraient affecter les enquêtes criminelles **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22[311] commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		**Étude juridique** Cette infraction concerne les personnes, ayant une connaissance spécifique de preuve tangible, qui refusent d'apporter leur aide. Fréquemment, les autorités policières se fient à de telles personnes pour collecter les preuves lors d'enquêtes de cybercrimes. Une infraction séparée est constituée par le défaut de fourniture de mots de passe ou d'accès à des codes vers des données ou des appareils cryptés (c'est-à-dire «*une clé vers des informations protégées*») – la section 53 de la loi anglaise régissant les pouvoirs d'enquête de 2000 (RIPA) [312] prévoit de caractériser en infraction pénale les personnes qui ne se conforment pas à une section 49 de la RIPA Avis de divulgation de la «*clé*» **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		**Étude juridique** Cette infraction criminalise ceux qui harcèlent des personnes en ligne– certaines juridictions peuvent prévoir des infractions de harcèlement non liées à l'informatique – mais cette infraction est recommandée pour les crimes commis en ligne. **Analyse des lacunes** **Recommandation:** Nous recommandons de l'inclure dans la législation nationale.

311. Perquisition et saisie, assistance et injonctions de produire
312. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous. **Code criminel canadien** **Section 172.1** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280;		**Étude juridique** Pour prouver l'infraction néerlandaise, un rendez-vous à des fins sexuelles est requis pour apporter la preuve de l'historique de discussion en ligne à caractère sexuel, une demande de rendez-vous avec preuve de la planification (c'est-à-dire la date et le lieu). Le but de la loi canadienne est d'empêcher la préparation des adultes prédateurs des enfants en ligne. Cette infraction ne nécessite pas la commission de l'infraction sexuelle. Cela signifie que l'accusé n'a pas besoin de s'être réellement présenté au rendez-vous pour rencontrer la victime en personne. L'infraction est commise avant que toute action n'ait lieu pour commettre l'infraction substantielle. **Analyse des lacunes** **Recommandation:** Nous recommandons l'inclusion dans la législation nationale pour criminaliser ce comportement prédateur avant qu'une infraction sexuelle ne soit commise

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours. Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[313] **Perquisition et saisie de données informatiques stockées** 1. 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. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.		

313. Article 3 de la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou obtenir d'une façon similaire les données informatiques consultées selon les paragraphes 1 et 2. Ces mesures incluent les prérogatives suivantes: 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. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.	**Aucun équivalent**	**Étude juridique** Il s'agit du principal pouvoir d'enquête et doit faire référence à obtenir l'accès plutôt qu'à la recherche. Dans le Rapport explicatif de la CB, «recherche» signifie chercher, lire, inspecter ou examiner des données. Cela inclut la notion de recherche de données et de recherche (examen) dans des données. Le terme «*accès*» a une signification neutre et reflète plus précisément la terminologie informatique – en outre il est utilisé dans les articles 26 et 27 de la CITO.[314] **Analyse des lacunes** **Recommandation:** La législation nationale pourrait inclure la terminologie pertinente de la CB et l'HIPCAR afin d'inclure les définitions d'un *système informatique*[315] et *de données informatiques*[316] Il convient d'ajouter une définition de «saisir» pour garantir l'intégrité et pour des procédures spécifiques - section 3(16) de l'HIPCAR «*Saisir inclut:* • *activer tout système informatique sur site et tout support de stockage de données informatiques;* • *réaliser et conserver une copie de données informatiques, y compris par l'utilisation d'équipement sur site;* • *entretenir l'intégrité des données informatiques stockées pertinentes;* • *rendre inaccessibles ou supprimer les données informatiques sur le système informatique utilisé;* • *garder une impression de sortie des données informatiques; ou* • *saisir ou se procurer de manière similaire un système informatique, en tout ou en partie, ou un dispositif de stockage de données informatiques.*»

314. Paragraphe 191, page 33 du Rapport explicatif de la CB

315. Voir article 1.a. de la CB: «tout dispositif ou un groupe de dispositifs interconnectés ou associés dont un ou plusieurs exécute(nt), sur la base d'un programme informatique, des traitements de données automatiques» **ou** la section 3(5) de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou associés, y compris par Internet, dont un ou plusieurs exécute(nt), sur la base d'un programme informatique, des traitements de données automatiques ou toute autre fonction».

316. Voir article 1.b. de la CB: «toute représentation de faits, informations ou notions sous une forme adaptée pour leur traitement dans le cadre d'un système informatisé, y compris un programme permettant à un système informatique de réaliser une fonction» **ou** la section 3(6) de l'HIPCAR: «Les *données informatiques signifient toute représentation de faits, notions, informations (qu'il s'agisse de textes, sons ou images), instructions ou code lisibles par machine, sous une forme adaptée pour leur traitement dans le cadre d'un système informatisé, y compris un programme permettant à un système informatique de réa*liser une fonction.»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article 20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou b. ayant été obtenus par une personne suite à une infraction, le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à: i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays.		La section 21 de l'HIPCAR prévoit une législation afin de garantir que de l'aide est apportée par ceux disposant d'une connaissance spécialiste du site des preuves pertinentes – cela peut être utilisé comme guide – voir également la section 17 de l'HIPCAR pour une infraction si l'aide est refusée sans excuse légitime

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2. **Article 21 de l'HIPCAR – Assistance** Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à: • fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; • accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• obtenir et copier ces données informatiques; • utiliser l'équipement pour faire des copies; et • obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci; b. un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques. 2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1 (a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 27 de la CITO - Saisie de données stockées 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe 1 de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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; d. enlever ou rendre inaccessibles ces données du système informatique consulté. 2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes 2 et 3 de l'article 26 de la présente Convention.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 16 de la CB[317] **Conservation rapide des données informatiques stockées** 1. 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. 2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.		**Étude juridique** Ce pouvoir d'enquête est important pour garantir que les données vulnérables à la suppression ou la perte sont préservées. Bien qu'aucune disposition n'a été prévue pour la conservation – le questionnaire confirme que toute requête de conservation doit être envoyée au Bureau du Procureur général auprès de la Cour de cassation. **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré de conserver les BSI, les métadonnées et le contenu enregistré et transactionnel est essentiel dans le cadre des enquêtes sur la cybercriminalité pour s'assurer que des preuves sont disponibles pour la recherche, l'accès, la saisie et la vérification. La terminologie de l'article 16 de la CB, section 23 de l'HIPCAR ou l'article 23 de la CITO pourrait être utilisée. Il convient également d'ajouter des définitions de *«données informatiques»*,[318] *«informations d›abonnés ou BSI»*, *«données de trafic»*[319] et *«Fournisseur de service de communication»*[320] Il convient de noter que la CB et l'HIPCAR ne fournissent pas de définition de BSI – mais la CITO en fournit une pour informations d'abonnés:[321]

317. Pas d'équivalent dans la CUA
318. Voir article 1.b. de la CB **ou** section 3(6) de l'HIPCAR
319. Voir Article 1.d de la CB: «toutes les données informatiques associées à la communication par le biais d›un système informatique, générées par un système informatique faisant partie intégrante d›une chaîne de communication, indiquant l›origine de la communication, sa destination, sa voie, l›heure la date, la taille, la durée ou le type de service sous-jacent» **ou** la section 3(18) de l'HIPCAR: «Le trafic de données *désigne toutes les données informatiques qui: a. sont associées à la communication par le biais d'un système informatique; et b. sont générées par un système informatique faisant partie intégrante d'une chaîne de communication; et c. indiquent l'origine de la communication, sa destination, sa voie, l'heure, la date, la taille, la durée ou le type de service sous-jacent.»*
320. Voir article 1.c. de la CB: «i toute entité publique ou privée qui fournit aux utilisateurs de son service la capacité de communiquer par le biais d'un système informatique et ii toute autre entité qui traite ou stocke des données informatiques pour le compte de tels services de communication ou utilisateurs de tels services»
321. Voir article 2(9) de la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article23 de l'HIPCAR – Conservation rapide** Si un [agent de répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.	**Aucun équivalent**	«*Toute information à disposition du fournisseur de service concernant les abonnés au service, à l'exception des informations par le biais desquelles les éléments suivants peuvent être connus:* a. *le type de service de communication utilisé, les exigences techniques et la période de service.* b. *L'identité de l'abonné, son adresse postale ou géographique ou son numéro de téléphone et les informations de paiement disponibles en vertu du contrat ou de l'arrangement de service* c. *Toute autre information sur le site d'installation de l'équipement de communication en vertu du contrat de service.*» Il convient de tenir compte que la durée de conservation jugée raisonnable dans les circonstances et permettant une demande de prolongation dans des circonstances particulières – la CB et la CITO prévoient 90 jours et l'HIPCAR 7 jours. D'après l'expérience, 90 jours est trop court dans une enquête de cybercriminalité, le chiffre devrait se rapprocher de 180 jours puis être soumis à prolongation.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification. 2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 17 de la CB[322] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	**Aucun équivalent**	**Étude juridique** Ce pouvoir procédural est particulièrement important pour s'assurer que les FSC fournissent les adresses IP pouvant localiser l'auteur d'un cybercrime. **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré concernant la divulgation de données de trafic devrait être inclus dans la législation pour permettre des enquêtes efficaces sur les cybercrimes. La terminologie de l'article 17 de la CB, sections 23 et 24 de l'HIPCAR ou l'article 24 de la CITO pourrait être utilisée. Des définitions de «données de trafic» et «Fournisseur de service de communication» seraient également requises[323]

322. Pas d'équivalent dans la CUA
323. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 23 de l'HIPCAR – Conservation rapide Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 24 de l'HIPCAR – Divulgation partielle des données de trafic** Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. les fournisseurs de services Internet; et/ou b. l'itinéraire de la communication.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		
Article 18 de la CB[324] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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	**Aucun équivalent**	**Étude juridique** Il existe une disposition cruciale pour une enquête efficace en matière de cybercrime et son absence affectera les poursuites et la coopération internationale.

324. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;		**Analyse des lacunes** **Recommandation:** Ce pouvoir crucial est nécessaire pour garantir que les FSC au Liban fournissent les BSI, les données de trafic et les données du contenu stocké. Il convient également d'ajouter des définitions de «données informatiques», «informations d›abonnés ou BSI», «données de trafic» et «*Fournisseur de service de communication*».[325] L'article 25 de la CITO est un modèle qui pourrait être utilisé et utilise différentes définitions incluant «technologie de l›information»,[326] «*fournisseur de service*»[327] et «*données*»[328] – nous recommandons d'ajouter des définitions pour «*informations d›abonnés ou BSI*», «*données de trafic*» car il existe différents types de preuves pouvant être fournies par les FSC. En outre, ce pouvoir obligera les individus et les tiers (tels que les entreprises, les institutions financières et les autres organismes) qui détiennent des données à les produire aux autorités policières. L'article 18 de la CB et la section 22 de l'HIPCAR pourraient constituer un guide avec une application cohérente des définition

325. Voir les définitions ci-dessus
326. Article 2(1) de la CITO: «*tout matériel ou moyen virtuel ou groupe de moyens interconnectés utilisés pour stocker, trier, disposer, développer et échanger des informations conformément à des commandes et des instructions stockées à l'intérieur. Cela inclut toutes les entrées et sorties associées, au moyens de câbles ou sans fil, dans un système ou un réseau.*»
327. Article 2(2) de la CITO: «toute personne physique ou morale, publique ou privée, qui fournit à des abonnés les services nécessaires pour communiquer par le biais de la technologie de l'information ou pour traiter ou stocker des informations pour le compte du service de communication ou de ses utilisateurs.»
328. Article 2(3) de la CITO: «tout ce qui peut être stocké, traité, généré et transféré par le biais de la technologie de l›information, comme des nombres, lettres, symboles, etc…»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: a. à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou b. à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service. **Article 25 CITO - Injonction de produire les informations** Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[329] **Interception de données relatives au contenu** **Article 26 de l'HIPCAR** **Article 29 de la CITO - Interception de données relatives au contenu**	**Loi 140/99, amendée par la Loi 158/99.** **Articles 2, 3 et 9**	**Étude juridique** Loi 140/99 telle qu'amendée par la Loi 158/99 permet l'interception, l'écoute et la surveillance de tous les moyens de télécommunication y compris les e-mails. L'interception ne peut avoir lieu qu'à la suite d'une décision judiciaire ou administrative, comme l'indiquent les Articles 2 et 3 de la Loi 140/99 pendant une durée maximale de deux mois - renouvelable. L'article 2 permet l'interception dans des cas d'extrême urgence, pour des infractions qui sont sanctionnées par une durée d'emprisonnement d'au moins un an. L'article 9 permet au Ministre de la défense nationale et au Ministre de l'intérieur d'ordonner l'interception, après accord du Premier ministre, de recueillir des informations pour les infractions terroristes et de crime organisé. Ce pouvoir est essentiel pour la législation nationale – et des garanties et une exigence/procédure devraient exister pour contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques au Liban. **Analyse des lacunes** **Recommandations:** Il conviendrait obliger les FSC opérant au Liban (au-delà des simples courriers électroniques, par ex. les applications de messagerie) à coopérer à la collecte en temps réel des contenus. De même, des garanties devraient être incorporées afin d'assurer que la collecte se fasse selon des modalités légales, raisonnables et proportionnelles. Il faudrait envisager d'étudier l'article 29 de la CITO, l'article 21 de la CB et la section 26 de l'HIPCAR, afin d'en incorporer les termes dans la législation nationale

329. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 20 de la CB[330] **Collecte en temps réel des données relatives au trafic** 1. 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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.	**Aucun équivalent**	**Étude juridique** Il n'existe pas de pouvoir procédural pour collecter les données de trafic en temps réel. Il pourrait exister un seuil plus bas pour collecter des données de trafic en temps réel, ce qui constitue un outil d'enquête essentiel. Il pourrait exister des situations où un seuil légal plus élevé pour accéder aux contenus pourrait ne pas être compris par un demandeur – mais un seuil plus bas pour accéder au trafic pourrait l'être. Aussi, il devrait exister une distinction entre la collecte en temps réel de contenus stockés et de données de trafic. Il s'avère nécessaire de créer des garanties et des exigences/ procédures pour contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques au Liban **Analyse des lacunes** **Recommandations:** Il conviendrait de disposer d'un pouvoir spécifique pour collecter les données de trafic en temps réel et d'obliger les FSC opérant au Liban à coopérer à la collecte en temps réel des données de trafic. De même, des garanties devraient être intégrées afin d'assurer que la collecte soit légale, raisonnable et proportionnelle au vu des circonstances. La terminologie de l'article 28 de la CITO pourrait être envisagée, mais elle ne fait pas allusion à la collecte rapide en temps réel uniquement. L'article 20 de la CB et la section 25 de l'HIPCAR devraient être utilisés comme guide pour la législation nationale

330. Article 31, paragraphe 3, sous e), de la CUA – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 25 de l'HIPCAR - Collecte des données de trafic** 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		
		Obligation de divulgation des clés de cryptage Les terroristes et les membres du crime organisé utilisent régulièrement des applications de messagerie cryptées331 cela peut donc être considéré comme un pouvoir viable pour dévoiler les clés des mots de passe afin de déverrouiller les appareils[332] **Analyse des lacunes** **Recommandation:** Impossible de clarifier l'existence de tels pouvoirs au Liban – mais un tel pouvoir permettra aux autorités d'application de la loi d'obliger les propriétaires à déverrouiller les appareils

331. Eleanor Saitta. «Le cryptage peut-il nous sauver?» Nation 300, n° 24 (15 juin 2015): 16-18. Academic Search Premier, EBSCOhost (dernier accès le 29 février 2016).
332. En guise d'exemple, voir la section 49 de la loi anglaise régissant les pouvoirs d'enquête 2000 (GB) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations de conservation des données[333] Un tel pouvoir peut permettre aux autorités policières de 1. Tracer et identifier la source d'une communication 2. Identifier la destination d'une communication; 3. Identifier la date, l'heure et la durée d'une communication; et 4. Identifier le type de communication Le Liban dispose d'une telle obligation[334]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB[335] **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.	**Aucun équivalent**	**Étude juridique** Sans cadre clairement défini pour les infractions de cybercriminalité, qui sont de nature internationale, toute législation sera restreinte. **Analyse des lacunes** **Recommandation:** La législation nationale garantit que la juridiction est définie en utilisant les termes de l'article 22 de la CB, de la section 19 de l'HIPCAR ou de l'article 30 de la CITO. S'il existe un conflit entre des juridictions, il convient de tenir compte des directives quant à la détermination de la juridiction appropriée pour poursuivre une infraction – consulter les directives Eurojust permettant de décider quelle juridiction doit poursuivre (révisées en 2016)[336]

333. En 2006, l'UE a émis sa directive de conservation des données - les États Membres de l'UE devaient stocker les données de télécommunications électroniques pendant au moins six mois et au plus 24 mois pour enquêter, détecter et poursuivre des crimes graves. En 2014, la Cour de Justice de l'UE a invalidé la directive de conservation des données, arguant qu'elle fournissait des garanties insuffisantes contre les interférences avec les droits à la vie privée et la protection des données. En l'absence d'une direction de conservation des données valide de l'UE, les États Membres peuvent toujours prévoir un protocole de conservation des données – pour les protocoles nationaux, consulter: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
334. Examen global ICMEC page 30
335. Pas d'équivalent dans la CUA
336. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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. **Article 19 de l'HIPCAR – Juridiction** La présente loi s'applique à tout acte ou omission commis: a. sur le territoire de [État prenant les dispositions]; b. sur un bateau ou un avion immatriculé en [État prenant les dispositions]; c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		
Article 35 de la BC	**Aucun équivalent**	**Étude juridique** Il s'agit d'un mécanisme essentiel pour disposer d'une aptitude efficace à l'enquête de cybercrimes. **Analyse des lacunes** **Recommandation:** La mise en œuvre ne devrait pas nécessiter de législation et, en fonction des ressources, cette mesure devrait être établie en priorité. Les coordonnées doivent être partagées pour le point de contact unique (SPOC) nommé au niveau national, au niveau international pour les autorités centrales et INTERPOL. Il convient également de tenir compte de l'élaboration d'un Mémorandum de compréhension avec les agences nationales, afin que le SPOC dispose d'une autorité pour entreprendre les actions requises dans le cadre d'une enquête de cybercriminalité internationale appliquant les traités et lois nationaux. Ce MOU doit comprendre les requêtes entrantes et sortantes et garantir un processus efficace et effectif.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35. 3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.	**Aucun équivalent**	**Étude juridique** Le Liban ne fait pas partie de la CB ou de la CITO. Le Liban ne fait pas partie d'une convention internationale dédiée à la cybercriminalité, cet état de fait perturbe les enquêtes internationales car les pouvoirs procéduraux n'auront aucune base juridique. En dehors de tout traité bilatéral – le Liban est signataire de la CNUCTO[337] et l'article 18 de la CNUCTO constitue la base pour la MLA et le principe de mutualité/réciprocité.[338] Cela signifie que sans législation nationale, des requêtes de conservation accélérée de données informatiques stockées, de conversation accélérée et de divulgation partielle des données de trafic et de divulgation des données stockées et des données de trafic ne peuvent pas être déposée, ce qui constitue une limite à la coopération internationale que le Liban peut apporter aux États requérants. **Analyse des lacunes** **Recommandation:** La loi nationale est requise pour la conversation accélérée des données informatiques stockées, la conservation accélérée et la divulgation partielle des données de trafic et des ordres de production. La CB, l'HIPCAR et la CITO peuvent être utilisés comme précédents pour la conservation accélérée des données informatiques stockées,[339] la conservation accélérée et la divulgation partielle des données de trafic[340] la divulgation des données stockées[341] et le recueil accéléré des données de trafic[342] - il convient également d'étudier une disposition d'interception en temps réel des données de trafic et du contenu[343]. En outre, un cadre de coopération lors d'enquêtes sur des faits de cybercriminalité doit être fourni par des conventions multilatérales, comme l'article 27 de la CB et l'article 32 de la CITO.[344]

337. Ratification du 5 octobre 2005
338. L'article 18 de la CNUCTO pourrait constituer la base pour la MLA si la définition du crime organisé transnational est satisfaite et l'Accord de coopération judiciaire de Riyad pourrait constituer la base pour les États l'ayant ratifié
339. Article 29 de la CB, section 23 de l'HIPCAR et Article 37 de la CITO
340. Article 30 de la CB, sections 23 et 24 de l'HIPCAR et Article 38 de la CITO
341. Article 31 de la CB et Article 39 de la CITO
342. Article 41 de la CITO
343. Articles 33 et 34 de la BC et sections 25 et 26 de l'HIPCAR
344. Il n'existe pas de dispositions équivalentes sur la procédure pour la MLA dans l'AUC

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.		Il convient d'étudier le fait de permettre aux autorités juridictionnelles d'autoriser l'application du droit national afin d'enquêter dans l'État dans lequel l'accès à un appareil est connu. L'accessibilité des informations constitue le critère essentiel pour lancer une enquête dans des situations dans lesquelles il n'est pas possible de savoir où les données sont stockées (c'est-à-dire dans le cloud). Elle pourrait comprendre une «reconnaissance mutuelle» des décisions de justice émises à l'encontre des fournisseurs de service de communications dans un État donné, qui pourraient être remise aux filiales des FSC situées dans d'autres États, en fonction de l'endroit où les données sont stockées.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles; c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires. 6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL. c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		
Article 26 de la CB[345] **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.	**Aucun équivalent**	**Étude juridique** Il s'agit d'une procédure importante afin de permettre à un État ayant connaissance d'informations qui aideraient un autre État à empêcher un cybercrime ou à enquêter sur celui-ci. Bien qu'elle soit disponible entre les États ayant ratifié la CITO dans l'article 33 de la CITO, le Liban ne dispose pas de base juridique pour le partage de ces informations avec les États non membres de la CITO, à moins qu'une requête officielle ne soit envoyée par le biais des canaux MLA classiques. L'article 18(4)-(5) de la CNUCTO prévoit le partage d'intelligence spontané pour des questions satisfaisant la définition d'un crime grave[346], qui est transnational[347] et implique un groupe du crime organisé[348]. Sans satisfaire cette définition une requête officielle devra être envoyée par le biais des canaux MLA classiques aux États n'ayant pas ratifié la CITO. Sur la base de la rapidité de mouvement de la cybercriminalité, le partage spontané est une manière efficace de coopérer avec d'autres États et, en l'absence de partage, empêche une collaboration internationale efficace avec les États n'ayant pas ratifié la CITO.

345. Il n'existe pas de disposition équivalente dans la CUA.
346. Article 2(b), «*un «crime grave» est un acte constituant une infraction passible d'une peine privative de liberté au moins égale à quatre ans ou d'une peine plus lourde*»
347. Article 3(1) de la CNUCTO
348. Article 2(a) de la CNUCTO «*Un «groupe du crime organisé» signifie groupe structuré de trois personnes ou plus, existant pendant une certaine période et agissant de concert dans le but de commettre un ou plusieurs crimes ou infractions graves établis* conformément à la présente *Convention, afin d'obtenir, directement ou indirectement, un avantage financier ou matériel*».

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières. **Article 33 de la CITO - Informations spontanées reçues** 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		**Analyse des lacunes** **Recommandation:** Utiliser l'article 18(4)-(5) de la CNUCTO comme base pour le partage spontané d'informations qui rentre dans le cadre de la CNUCTO (sans garanties fournies en matière d'utilisation comme preuve ou de divulgation d'informations sensibles à un tiers (y compris un autre État).[349] Prendre en compte la législation basée sur l'article 33 de la CITO ou l'article 26 de la CB.

349. Voir article 33(2) de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.	**Aucun équivalent**	**Étude juridique** Ce pouvoir procédural permet à un État de garantir le contenu stocké dans un autre État dans des circonstances limitées. L'article 32.b. de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permet l'accès transfrontalier unilatéral sans besoin d'entraide judiciaire en cas d'accord ou quand l'information est publiquement disponible. Les exemples d'usage de ce pouvoir procédural conformément à l'article 32.b de la CB comprennent : L'adresse électronique d'une personne peut être enregistrée dans un autre pays par un fournisseur de service, ou une personne peut enregistrer sciemment des données dans un autre pays. Ces personnes peuvent récupérer les données et à condition qu'elles en aient l'autorité légitime, elles peuvent volontairement divulguer les données à des officiels d'application de la loi, ou permettre à ces officiels d'accéder aux données[350] Un terroriste présumé est arrêté légalement pendant que sa boîte de réception électronique – contenant éventuellement des preuves d'un crime – est ouverte sur sa tablette, son smartphone ou un autre appareil. Si le suspect consent volontairement à ce que la police accède à son compte et si la police est sûre que les données de la boîte de réception sont situées dans un autre État, la police peut accéder aux données selon l'article 32.b.

350. Paragraphe 294, page 53 du Rapport explicatif de la CB

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 27 de l'HIPCAR – Logiciel de criminalistique 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes: • le suspect de l'infraction, si possible avec ses nom et adresse; et • une description du système informatique ciblé; et • une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et • les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner		**Analyse des lacunes** **Recommandation:** Ce pouvoir restreint à récupérer unilatéralement les preuves est inclus dans la législation, ce qui garantit que le consentement de l'utilisateur est obtenu légalement.[351] La terminologie de l'article 32 de la CB et de l'article 40 de la CITO peut être utilisée. L'article 32.b. a été lourdement critiqué et il peut être envisagé que le consentement de l'État dans lequel les données informatiques stockées sont stockées soit obtenu en plus de celui de l'utilisateur. La section 27 de l'HIPCAR prévoit un logiciel judiciaire et cela peut permettre l'accès à un ordinateur dans un autre État. Il existe un certain nombre de restrictions qui nécessitent que les preuves ne puissent pas être obtenues par d'autres moyens, qu'un ordre judiciaire soit requis, qu'il ne peut s'appliquer qu'à certaines infractions et que sa durée soit limitée (3 mois). Il convient également d'examiner le consentement de l'autre État dans lequel le logiciel judiciaire peut intervenir.

351. Il convient d'examiner des situations telles que la non disponibilité d'un utilisateur (par ex. sa mort) et si le consentement peut être obtenu dans un autre État

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le moyen technique utilisé ainsi que la date et l'heure de l'application; b. l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et c. toute information obtenue. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect. 5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20. 6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions]. 8. Un pays peut décider de ne pas mettre en œuvre l'article27.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 40 de la CITO - Accès transfrontière à des données informatiques Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité.		

Maroc

Invité à adhérer à la CB

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[352] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 6 de la CITO – Infraction d'accès illégal** 1. L'accès ou le maintien illégal et tout contact avec tout ou partie d'un système informatique. 2. La peine est aggravée lorsqu'il résulte de cet accès, maintien, liaison ou continuation de ce contact: a. La suppression, la modification, la déformation, le transfert, la reproduction ou la destruction des données sauvegardées, des appareils et des systèmes électroniques et des réseaux de communication, et de porter préjudice aux utilisateurs et bénéficiaires. b. L'obtention de renseignements gouvernementaux confidentiels.	**Code pénal** **Article 607-3** Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données (...). Est passible de la même peine toute personne qui se maintient dans tout ou partie d'un système de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit. La peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système de traitement automatisé de données, soit une altération du fonctionnement de ce système. **Article 607-4** Sans préjudice de dispositions pénales plus sévères, est puni de six mois à deux ans d'emprisonnement et de 10000 à 100000 dirhams d'amende quiconque commet les actes prévus à l'article précédent contre tout ou partie d'un système de traitement automatisé de données supposé contenir des informations relatives à la sûreté intérieure ou extérieure de l'État ou des secrets concernant l'économie nationale.	**Analyse juridique** La disposition nationale utilise le terme *«frauduleusement»*, ce qui semble suggérer que l'auteur a accédé aux données de façon malhonnête (alors que la CB utilise l'expression *«sans droit»* en cas d'accès non autorisé). La CB évoque *«l'intention malhonnête»* mais il s'agit du mens rea (intention criminelle) qui vise à obtenir les données plutôt que l'accès illégal en lui-même. Actuellement, cette infraction nationale peut être perpétrée uniquement si l'auteur fait preuve d'une intention malhonnête. En l'absence de définition du terme «frauduleusement», on ne sait pas si cela exige un acte manifeste ou si chaque accès illégal est considéré comme frauduleux. Une définition du terme *«frauduleux»* s'avère donc nécessaire. La CITO, quant à elle, fait référence à «l'accès ou le maintien illégal et tout contact avec», sans définir ce que ces actes signifient. Le recours à la CB et à l'HIPCAR devrait donc être privilégié. L'infraction fait également référence à un *«système de traitement automatisé de données»*, sans définir ce dernier. On ne sait pas si elle concerne un «système informatique» (à savoir 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 (article 1 de la CB) ou des «données informatiques» (à savoir toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme permettant à un système informatique d'exécuter une fonction (article 1 de la CB)).

352. Article 29, paragraphe 1, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 4 de l'HIPCAR – Accès illégal 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête. **Article 5 de l'HIPCAR – Présence illégale** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		La forme aggravée du délit prévue à l'article 607-4 pourrait être plus large, afin d'englober tous les intérêts nationaux de l'État, la santé par exemple. **Analyse des écarts** **Recommandation:** La législation nationale pourrait intégrer la terminologie pertinente de la CB et de l'HIPCAR, afin d'inclure la définition de l'expression système informatique[353] et l'inclusion des programmes dans la définition des données, dans la mesure où certaines données incluent des programmes et d'autres non. En outre, pour faire preuve de cohérence par rapport à la CB et à l'HIPCAR, il conviendrait d'évoquer l'accès *«sans droit»* plutôt que *«frauduleusement»*. Le délit aggravé prévu à l'article 607-4 pourrait être plus large, afin de tenir compte des accès illégaux aux données d'infrastructure critiques, plutôt que de faire uniquement référence à la sécurité nationale et à l'économie (voir l'article 4, paragraphe 2, de l'HIPCAR).

353. Voir l'article 1, sous a), de la CB: «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 » **ou** l'article 3, paragraphe 5, de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions».

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.		
Article 3 de la CB[354] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 7 de la CITO** **Infractions d'interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques.	**Pas d'équivalent**	**Analyse juridique** Cette infraction est essentielle pour poursuivre en justice des transmissions non publiques de données informatisées en direction ou en provenance d'un système informatique et qui pourraient avoir été interceptées de façon illégale afin d'obtenir des informations concernant la localisation d'une personne (pour cibler cette dernière par exemple).[355] Le vol d'identifiants implique souvent l'utilisation de keyloggers ou d'autres types de programmes malveillants, en vue de l'interception illégale de transmissions non publiques de données informatisées en direction ou en provenance d'un système informatique comportant des informations sensibles, telles que des données relatives à l'identité. Cette infraction s'avère essentielle pour poursuivre en justice les transmissions de données informatisées en provenance ou en direction d'un système informatique qui pourraient avoir été interceptées de manière illégale pour obtenir des informations (par exemple, Wikileaks ou Panama Papers). La terminologie utilisée à l'article 7 de la CITO (interception illégale) ne comporte pas de définition des *«données des technologies de l'information»*. **Analyse des écarts** **Recommandation:** L'article 7 de la CITO (avec une définition des «données des technologies de l'information»), l'article 3 de la CB ou l'article 6 de l'HIPCAR pourrait être utilisé comme guide pour la législation nationale.

354. Article 29, paragraphe 2, de la CUA
355. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 6 de l'HIPCAR – Interception illégale 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques: • toute transmission non publique vers, de, ou au sein d'un système informatique; ou • des émissions électromagnétiques provenant d'un système informatique, • commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut imposer que l'infraction soit commise avec une intention malhonnête ou en rapport avec un système informatique connecté à un autre système informatique ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique.		
Article 4 de la CB[356] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.		

356. Article 29, paragraphe 1, sous e) à sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 7 de l'HIPCAR – Atteinte à l'intégrité des données 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants: • endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes; • obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, • commet une infraction passible, en cas de condamnation, d'une peine de prison • maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Article 8 de la CITO** **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.	**Code pénal** **Article 607-6** Le fait d'introduire frauduleusement des données dans un système de traitement automatisé des données ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient, leur mode de traitement ou de transmission (...).	**Analyse juridique** L'utilisation du terme «frauduleusement» n'est pas cohérente (rentre en conflit) avec la règle posée par l'article 4, paragraphe 1, de la CB, c'est-à-dire «(...) le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques» qui n'exige pas la preuve de l'existence d'une fraude. Cela signifie, essentiellement, que la conduite constitutive d'un délit d'atteinte à l'intégrité des données au sens de l'article 4, paragraphe 1, de la CB, ne serait pas criminalisée en vertu de l'article 607-6 du Code pénal national. Ledit article n'englobe pas la suppression de données informatisées. **Analyse des écarts** **Recommandation:** Utiliser l'article 4 de la CB ou l'article 7 de l'HIPCAR comme guide pour la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 5 de la CB[357] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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. **Article 9 de l'HIPCAR – Atteinte à l'intégrité du système** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: • entrave ou porte atteinte au fonctionnement d'un système informatique; ou • entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Article 607-5** Le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé de données (...).	**Analyse juridique** Cette infraction contribuerait à lutter contre les logiciels malveillants qui perturbent le fonctionnement d'un ordinateur (des vers informatiques par exemple) ou les sous-groupes de logiciels malveillants (comme les virus informatiques). Il s'agit de programmes informatiques auto-répliquants qui nuisent au réseau en lançant de multiples processus de transfert de données. Ils peuvent affecter les systèmes informatiques en entravant leur bon fonctionnement, en utilisant des ressources du système pour se reproduire sur Internet ou en générant du trafic sur le réseau susceptible d'interrompre la disponibilité de certains services (tels que des sites Internet). L'article 607-5 du Code pénal ne fait pas référence au *«fait d'entraver ou de fausser intentionnellement» «sans droit».* En outre, l'article 607-5 ne fait pas référence au fait d'entraver ou de fausser intentionnellement *«par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques».* La mention de ces actes permettrait de garantir que l'infraction décrit la signification de l'entrave ou de la distorsion intentionnelle. **Analyse des écarts** **Recommandation:** Utiliser la terminologie employée par la CB, dans son article 5, en ajoutant l'expression *««entrave grave intentionnelle» et «sans droit» et les actes constitués par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques».*

357. Article 29, paragraphe 1, sous d), de la CUA, sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		Examiner également la question de savoir si la prévention et la poursuite en justice des attaques à l'encontre des infrastructures critiques nécessitent l'instauration d'une autre infraction séparée ou aggravée, comme lorsque le fonctionnement d'un système informatique est entravé à des fins terroristes (l'entrave à un système stockant des registres boursiers pourrait les rendre inexacts, ou entraver le fonctionnement d'une infrastructure critique).[358] Voir le précédent à l'article 9, paragraphe 2, de l'HIPCAR.
Article 6 de la CB[359] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Code pénal** **Article 607-10** Est puni d'un emprisonnement de deux à cinq ans et d'une amende de 50000 à 2000.000 de dirhams le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données, conçus ou spécialement adaptés pour commettre les infractions prévues au présent chapitre.	**Analyse juridique** Cette infraction permettra de poursuivre en justice la production, la vente ou l'acquisition à des fins d'utilisation, ainsi que l'importation ou la distribution de codes d'accès et d'autres données informatiques utilisées pour perpétrer des délits. C'est ainsi, par exemple, que l'on peut accéder à un système informatique pour faciliter une attaque terroriste, en perturbant le réseau de distribution électrique d'un pays. De la même façon que pour l'Accès illégal, la disposition n'utilise pas l'expression «sans droit» (l'intention de commettre l'infraction serait cohérente avec les modifications suggérées concernant les délits susvisés et du fait que l'intention est déjà stipulée à l'article 607-5). L'article 607-10 du Code pénal ne criminalise pas spécifiquement les actes de *«vente, l'obtention pour utilisation, l'importation ou la diffusion» (bien qu'il s'agisse d'une disposition «fourre-tout»).*

358. http://www.coe.int/en/web/cybercrime/guidance-notes
359. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5, et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		Il n'existe pas de référence à un mot de passe, à un code d'accès ou à des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre une infraction liée à la cybercriminalité. Une telle inclusion permettrait de décrire la conduite criminelle avec précision. L'article 6, paragraphe 2, de la CB prévoit une excuse raisonnable si l'acte intentionnel vise l'«essai autorisé ou de protection d'un système informatique». L'adoption d'une disposition analogue permettrait aux autorités chargées de l'application de la loi de ne pas avoir à répondre de la commission de cette infraction (voir également l'article 10, paragraphe 2, de l'HIPCAR). Il convient de noter que l'HIPCAR prévoit la possibilité de répertorier les dispositifs dans une annexe, si nécessaire. Une telle disposition pourrait s'avérer restrictive et exiger des mises à jour au fur et à mesure des progrès technologiques. **Analyse des écarts** **Recommandation:** Utiliser la terminologie employée par l'HIPCAR dans son article 10, ou par la CB dans son article 6, en ajoutant «sans droit» et une intention de commettre le délit. Il conviendrait également d'envisager de préciser l'utilisation de mots de passe et de codes d'accès. L'article devrait prévoir une excuse raisonnable, afin que les autorités chargées de l'application de la loi puissent utiliser des dispositifs à des fins de techniques d'enquête particulières (la terminologie de l'article 6, paragraphe 2, pourrait être utilisée comme guide).

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de l'HIPCAR – Dispositifs illégaux 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.	**Code pénal** **Article 607-7** Sans préjudice de dispositions pénales plus sévères, le faux ou la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui (...).	**Analyse juridique** De la même façon que pour l'Accès illégal, la disposition n'utilise pas l'expression «sans droit» (l'intention de commettre l'infraction serait cohérente avec les modifications suggérées concernant les délits susvisés et du fait que l'intention est déjà stipulée à l'article 607-5). Il n'existe pas de définition de l'expression *«documents informatisés»*. L'article 607-7 du Code pénal exige l'existence d'un préjudice, alors que l'approche adoptée dans le cadre de l'article 7 de la CB consiste à tenir compte de l'intention, sans autorisation, d'introduire, altérer, effacer ou supprimer de données informatiques, engendrant des données non authentiques. Il n'est pas nécessaire que le préjudice ou la perte soit causé(e) à un tiers. Cette exigence additionnelle de l'article 607-7 du Code pénal peut restreindre le nombre de poursuites en justice réussies, car dans certains cas, aucun préjudice n'a été causé par l'intention manifeste. C'est ainsi, par exemple, que dans le cadre d'une escroquerie de harponnage, une fausse déclaration avec une URL non authentique est distribuée, mais l'utilisateur ne donne pas suite, de sorte qu'il n'existe aucun préjudice.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 11 de l'HIPCAR – Falsification informatique 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux. **Article 10 de la CITO** **Infraction de falsification** L'utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques.		**Analyse des écarts** **Recommandation:** Il conviendrait de prévoir une définition de l'expression *«documents informatisés» et d'envisager son remplacement par «données informatiques»*, tel que défini à l'article 1, sous b), de la CB. Il conviendrait d'inclure l'expression «sans droit» et l'intention de commettre l'infraction (et examiner s'il s'agit d'une intention malhonnête). Examiner si le préjudice doit constituer un élément du délit (il serait préférable de ne pas utiliser le terme préjudice car la falsification est commise dès que des données non authentiques ont été créées et prises en compte. Cela signifie que si un faux lien ou document est envoyé dans le cadre d'une escroquerie de harponnage, le délit est constitué dès que le destinataire le prend en compte (c'est-à-dire dès qu'il ouvre le courriel contenant le lien ou la pièce jointe), plutôt que de devoir démontrer qu'il a subi un préjudice.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 29, paragraphe 2, sous b), de la CUA (...) 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. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.		
Article 8 de la CB[360] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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.	**Code pénal** **Article 607-6** Le fait d'introduire frauduleusement des données dans un système de traitement automatisé des données ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient, leur mode de traitement ou de transmission, est puni d'un an à trois ans d'emprisonnement et de 10000 à 200000 dirhams d'amende ou de l'une de ces deux peines seulement. **Dahir n°1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel**	**Analyse juridique** Alors que le terme «frauduleusement» dans ce contexte ne fournit pas assez de protection, l'absence d'actus reus constitué par la commission de cette conduite sans autorisation fait défaut et pourrait créer de l'incertitude. Il n'existe pas de définition du terme *«données» ou «système de traitement automatisé de données»*, ce qui peut créer de l'incertitude. Les articles 54 et 61 peuvent ériger en infraction pénale la diffusion de données personnelles. Ces articles n'érigeraient pas en infraction pénale la violation de données personnelles par négligence, comme en cas de perte ou d'envoi par inadvertance à une adresse incorrecte. Bien que l'article 61 ne fasse pas référence à la négligence, les données divulguées devraient être utilisées à des fins frauduleuses pour que l'infraction puisse être établie.

360. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 12 de l'HIPCAR – Fraude informatique Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: a. introduction, altération, effacement ou suppression des données informatiques; b. atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Article 54** Est puni d'un emprisonnement de trois mois à un an et d'une amende de 20000 à 200000 DH ou de l'une de ces deux peines seulement quiconque, en violation des a), b) et c) de l'article 3 de la présente loi [Critères relatifs aux données], collecte des données à caractère personnel par un moyen frauduleux, déloyal ou illicite, met en œuvre un traitement à des fins autres que celles déclarées ou autorisées ou soumet les données précitées à un traitement ultérieur incompatible avec les finalités déclarées ou autorisées. **Article 61** Est puni d'un emprisonnement de six mois à un an et d'une amende de 20000 à 300000 DH ou de l'une de ces deux peines seulement, tout responsable de traitement, tout sous-traitant et toute personne qui, en raison de ses fonctions, est chargé (e) de traiter des données à caractère personnel et qui, même par négligence, cause ou facilite l'usage abusif ou frauduleux des données traitées ou reçues ou les communique à des tiers non habilités. Le tribunal pourra, en outre, prononcer la saisie du matériel ayant servi à commettre l'infraction ainsi que l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction.	**Analyse des écarts** **Recommandation:** Il conviendrait d'insérer les définitions de *«données»* et de *«système automatisé de traitement de données»* et d'ajouter *«sans droit»* dans l'article 607-6. La terminologie utilisée par la CB ou par l'HIPCAR concernant cette infraction constitue un bon guide pour la législation nationale.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 9 de la CB[361] **Infractions se rapportant à la pornographie enfantine** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit: a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique; b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique; d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique; e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. 2. Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle: a. un mineur se livrant à un comportement sexuellement explicite; b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;	**Code pénal** **Article 503-2** Quiconque provoque, incite ou facilite l'exploitation d'enfants de moins de dix-huit ans dans la pornographie par toute représentation, par quelque moyen que ce soit, d'un acte sexuel réel, simulé ou perçu ou toute représentation des organes sexuels d'un enfant à des fins de nature sexuelle. La même peine est applicable à quiconque produit, diffuse, publie, importe, exporte, expose, vend ou détient des matières pornographiques similaires. Ces actes sont punis même si leurs éléments sont commis en dehors du Royaume.	**Analyse juridique** Il s'agit d'une infraction essentielle pour la protection de l'enfance, qui érige en infraction pénale la diffusion, la transmission, la mise à disposition, la proposition, la production et la possession d'images indécentes représentant des enfants. L'article 503-2 ne fait pas spécifiquement référence au fait que les actes de «*production, diffusion, publication, importation, exportation, exposition ou vente*»» interviennent par le biais d'un système ou d'un réseau informatique, ou encore d'un moyen de stockage. Alors que la protection est fournie dans le cadre de la référence au caractère extraterritorial, le fait d'indiquer l'utilisation d'un système informatique apporterait plus de précision sur les actes commis au sein du Royaume mais aussi à l'extérieur. L'article 9, paragraphe 1, fait aussi référence aux actes suivants qui ne sont pas mentionnés à l'article 503-2: «l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique». **Analyse des écarts** **Recommandation:** Il conviendrait d'étendre les actes couverts par l'article 503-2, pour y inclure «l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique» (voir l'article 9, paragraphe 1, sous b), de la CB). L'article 503-2 fait spécifiquement référence aux actes commis par le biais d'un système informatique, d'un réseau ou d'un dispositif de stockage (voir l'article 13 de l'HIPCAR).

361. Article 12 de la CITO et article 29, paragraphe 3, sous a) à sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. 3. Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. 4. Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c. **Article 13 de l'HIPCAR – Pédopornographie ou pornographie infantile** 1. Une personne qui, de manière intentionnelle et sans motif ou justification légitime: a. produit de la pornographie mettant en scène des enfants à des fins de diffusion par l'intermédiaire d'un système informatique; b. offre ou met à disposition, via un système informatique, des contenus pédopornographiques; c. diffuse ou transmet via un système informatique des contenus pédopornographiques; d. se procure et/ou obtient des contenus pédopornographiques pour elle même ou pour un tiers, via un système informatique; e. possède des contenus pédopornographiques sur un système informatique ou un moyen de stockage des données informatiques; ou f. obtient, en connaissance de cause, l'accès, via les technologies de l'information et de la communication, à des contenus pédopornographiques,		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si la personne établit que les contenus pornographiques servent uniquement à des fins de répression, cela constitue une décharge face à une accusation formulée au titre des paragraphes (1)(b) à (1)f). 3. Un pays peut ne pas criminaliser le comportement décrit à l'article 13(1)(d)-(f).		
Article 10 de la CB[362] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes**	**Dahir n° 1-00-20 du 9 kaada 1420 (15 février 2000) portant promulgation de la loi n° 2-00 relative aux droits d'auteur et droits voisins** **Article 64**	Rédaction satisfaisante
Article 11 de la CB[363] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.	**Pas d'équivalent**	**Analyse juridique** La prise en compte des actes de tentative et de complicité d'autrui en vue de la commission d'infractions s'avère essentielle pour poursuivre en justice ceux qui auraient pu aider ou auraient encouragé la perpétration d'actes relevant de la cybercriminalité. L'article 19 de la CITO prévoit aussi la tentative. **Analyse des écarts** **Recommandation:** Utiliser l'article 11 de la CB et l'article 19 de la CITO (sans référence à la tentative) comme guide pour la législation nationale.

362. Article 17 de la CITO sans équivalent dans la CUA
363. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention. **Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions** 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.		
Article 12 de la CB[364] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé:	**Pas d'équivalent**	**Analyse juridique** Cette disposition s'avère essentielle pour que la responsabilité pénale des personnes morales (par exemple, les sociétés commerciales) puisse être engagée. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 12 de la CB comme guide pour la législation nationale.

364. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale. 2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[365] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.	**Pas d'équivalent**	**Analyse juridique** L'article 3, paragraphe 1, sous e), de la CUA inclut la création et le téléchargement d'éléments racistes et xénophobes par le biais d'un système informatique, plutôt que leur simple diffusion ou mise à disposition (mais sans inclure l'intention ou «sans droit»). La terminologie utilisée par la CB devrait être privilégiée. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 3 de la CB et du Protocole additionnel comme guide pour la législation nationale.

365. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 4[366] – Menace avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 4 de la CB et du Protocole additionnel comme guide pour la législation nationale.
Protocole additionnel **Article 5[367] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.		

366. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO
367. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 5 de la CB et du Protocole additionnel comme guide pour la législation nationale.
Protocole additionnel **Article 6[368] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 6 de la CB et du Protocole additionnel comme guide pour la législation nationale.

368. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à revoir		
Infractions liées à l'identité **Article 14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction englobe la phase de préparation d'un délit de tromperie lié à l'identité. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article 16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: a. le fait qu'une injonction ait été émise; b. toute action réalisée aux termes de l'injonction; ou c. toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne les violations des données et la divulgation d'informations sensibles susceptibles d'avoir des répercussions sur les enquêtes pénales. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.
Refus d'autoriser l'assistance **Article 17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22369 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		**Analyse juridique** Cette infraction concerne les personnes qui ont connaissance d'éléments de preuve pertinents et refusent de coopérer. Souvent, les autorités chargées de l'application de la loi dépendent de ces personnes pour obtenir des éléments de preuve dans le cadre des enquêtes en matière de cybercriminalité. Le refus de fournir des mots de passe ou des codes d'accès à des dispositifs ou des données crypté(e)s (à savoir «des informations protégées par des clés de chiffrement») constitue une infraction séparée (l'article 53 de la loi britannique qui régit les pouvoirs d'enquête intitulée UK Regulation of Investigatory Powers Act 2000 (RIPA) [370] prévoit un délit pénal pour les personnes qui ne se conforment pas à l'article 49 de la RIPA Notice to disclose the *«key» (Injonction de divulgation de la «clé»)).* **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.

369. Perquisition et saisie, assistance et injonctions de produire
370. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article 18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne pénalement ceux qui harcèlent autrui en ligne (certains pays prévoient des sanctions pour les infractions liées au harcèlement non informatique) et cette sanction est recommandée concernant les délits commis en ligne. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Toute personne qui, au moyen d'un système de traitement automatisé des données ou en faisant usage d'un service de communications, propose une rencontre à une personne dont on sait ou, doit raisonnablement soupçonner qu'elle n'a pas encore atteint l'âge de seize ans, dans l'intention de commettre des actes contraires aux bonnes mœurs avec cette personne ou de confectionner une image de comportement sexuel dans lequel la personne est impliquée si elle entreprend un acte quelconque visant la réalisation de cette rencontre, est punie d'une peine d'emprisonnement de deux ans ou plus ou d'une amende de quatrième catégorie.		**Analyse juridique** Pour que l'infraction néerlandaise soit établie, une rencontre à des fins sexuelles est exigée, avec l'existence d'éléments de preuve d'échanges en ligne avec une intention sexuelle. Il doit également être prouvé qu'une rencontre a été prévue (à savoir, la date et le lieu). La disposition canadienne vise à éviter le leurre d'enfants par des adultes prédateurs en ligne. Cette infraction n'exige pas la perpétration d'une agression sexuelle. Cela implique que l'accusé ne doit pas nécessairement avoir rencontré la victime en personne. L'infraction est commise avant que toute mesure n'ait été adoptée en vue de perpétrer le délit en tant que tel. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée en vue de criminaliser cette conduite préparatoire avant que l'infraction sexuelle soit commise.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Article 172.1 - Leurre** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212.(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de quatorze ans, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de 90jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[371] **Perquisition et saisie de données informatiques stockées** 1. 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.	**Pas d'équivalent**	**Analyse juridique** Il s'agit du pouvoir d'enquête le plus essentiel, et il devrait faire référence à l'accès plutôt qu'à la perquisition. Dans le Rapport explicatif de la CB, le terme *«Perquisitionner»* signifie *«chercher, lire, inspecter ou examiner des données»*. Il inclut aussi les notions de recherche et d'examen des données. Le terme *«accéder»*, quant à lui, a un sens neutre et il est plus fidèle à la terminologie informatique (également utilisée aux articles 26 et 27 de la CITO).[372]

371. Article 3 de la CUA
372. Paragraphe 191, page 33 du Rapport explicatif de la CB

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes: a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;		**Analyse des écarts** **Recommandation:** La législation nationale pourrait intégrer la terminologie pertinente de la CB et de l'HIPCAR, afin d'inclure les définitions des expressions *système informatique*[373] et *données informatiques,*[374] et faire référence de manière uniforme au terme *accès*. Le terme «saisir» devrait être défini, de façon à garantir l'intégrité et pour les procédures spécifiques (article 3, paragraphe 16, de l'HIPCAR). ««Saisir» signifie: b. *activer tout système informatique et moyen de stockage des données informatiques sur site;* c. *faire et conserver une copie des données informatiques, en utilisant notamment l'équipement sur site;* d. *maintenir l'intégrité de ces données informatiques stockées;* e. *rendre inaccessible ou retirer les données informatiques du système informatique accédé;* f. *sortir sur imprimante les données informatiques; ou* g. *saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques».* L'article 21 de l'HIPCAR prévoit la législation nécessaire pour s'assurer que l'assistance est apportée par ceux qui disposent de connaissances spécialisées concernant le lieu où se trouvent les éléments de preuve pertinents (il pourrait donc être utilisé comme guide). Consulter également l'article 17 de l'HIPCAR pour les infractions dans le cadre desquelles l'assistance a été refusée sans excuse légitime.

373. Voir l'article 1, sous a), de la CB: «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 » **ou** l'article 3, paragraphe 5, de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions».

374. Voir l'article 1, sous b), de la CB: «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» ou l'article 3, paragraphe 6, de l'HIPCAR: ««Données informatiques» désigne toute représentation de faits, de concepts, d'informations (textes, sons ou images), de codes ou d'instructions lisibles par une machine, dans un format permettant d'être traité par un système informatique, notamment un programme pouvant faire exécuter une fonction à un système informatique».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article 20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: a. pouvant être considérés comme importants pour servir de preuve à une infraction; ou		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. ayant été obtenus par une personne suite à une infraction, le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à: i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays. 2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu des paragraphes 1 ou 2.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 21 de l'HIPCAR – Assistance Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à: a. fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; b. accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; c. obtenir et copier ces données informatiques; d. utiliser l'équipement pour faire des copies; et e. obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci; un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe (1-a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe (1-) de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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; d. enlever ou rendre inaccessibles ces données du système informatique consulté.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes (2 et 3) de l'article 26 de la présente Convention.		
Article 16 de la CB[375] **Conservation rapide de données informatiques stockées** 1. 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.	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir de procédure est important pour garantir la préservation des données vulnérables par rapport à la suppression ou la perte. **Analyse des écarts** **Recommandation:** Ce pouvoir rapide d'obtention de DBA, de métadonnées et de contenus transactionnels et stockés s'avère essentiel dans le cadre des enquêtes relevant de la cybercriminalité, afin de s'assurer de la disponibilité des éléments de preuve à des fins de perquisition, d'accès, de saisie et d'analyse. La terminologie utilisée à l'article 16 de la CB, à l'article 23 de l'HIPCAR et à l'article 23 de la CITO pourrait être utilisée. Il sera alors également nécessaire de définir les expressions *«données informatiques»*, [376]*«données relatives aux abonnés ou DBA»*, *«données de trafic»*[377] et *«Fournisseur de services de communications»*[378]. Il convient de noter que la CB et l'HIPCAR ne donnent pas de définition des DBA, contrairement à la CITO: [379]

375. Pas d'équivalent dans la CUA
376. Voir l'article 1, sous b), de la CB **ou** l'article 3, paragraphe 6, de l'HIPCAR
377. Voir l'article 1, sous d), de la CB: ««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» **ou** l'article 3, paragraphe 18, de l'HIPCAR: «Données relatives au trafic» désigne les données informatiques: a. ayant trait à une communication passant par un système informatique; et b. générées par un système informatique en tant qu'éléments de la chaîne de communication; et c. indiquant l'origine, la destination, l'itinéraire, l'heure, la taille et la durée de la communication ou le type de services sous-jacents».
378. Voir l'article 1, sous c), de la CB: «*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».
379. Voir l'article 2, paragraphe 9, de la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles14 et 15.		«Toutes informations existantes chez le fournisseur de services relatives aux utilisateurs de services à l'exception des informations à travers lesquelles on peut connaître: a. *le type de services de communications utilisés, les conditions techniques et la période desdits services;* b. *l'identité de l'utilisateur, son adresse postale ou géographique ou son téléphone, les renseignements de paiement disponibles sur la base d'un contrat ou d'un arrangement de services;* c. *Toutes autres informations sur le site de montage des équipements de communication sur la base d'un contrat de services*». Il conviendrait de prévoir une durée de conservation raisonnable selon les circonstances et permettre l'extension de la demande dans certaines circonstances exigeantes (la CB et la CITO prévoient 90jours et l'HIPCAR 7jours). L'expérience montre que le délai de 90jours est trop court en matière de cyber-enquêtes et qu'il devrait être plus près des 180 jours avec une possibilité d'extension.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 23 de l'HIPCAR – Conservation rapide Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1-, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		
Article 17 de la CB[380] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir procédural s'avère particulièrement important pour garantir que les FSC mettent à disposition des adresses IP pouvant permettre de localiser l'auteur d'un cybercrime. **Analyse des écarts** **Recommandation:** Le pouvoir de conservation rapide et la divulgation des données de trafic devraient être inclus dans la législation, afin de contribuer à l'efficacité des enquêtes en matière de cybercriminalité. La terminologie de l'article 17 de la CB, des articles 23 et 24 de l'HIPCAR et de l'article 24 de la CITO pourrait être utilisée à de tels effets. La définition des expressions *«données de trafic» et «Fournisseur de services de communications»* sera également nécessaire.[381]

380. Pas d'équivalent dans la CUA
381. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 23 de l'HIPCAR – Conservation rapide** Si un agent de [répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de l'HIPCAR – Divulgation partielle des données de trafic Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. les fournisseurs de services Internet; et/ou b. l'itinéraire de la communication. **Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic** Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[382] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir:	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une disposition essentielle pour la réalisation d'enquêtes efficaces en matière de cybercriminalité, et son absence aura un impact sur les poursuites devant les tribunaux et la coopération internationale. **Analyse des écarts** **Recommandation:** Ce pouvoir essentiel s'avère nécessaire pour s'assurer que les FSC opérant au Maroc fournissent les DBA, les données de trafic et les informations sur les contenus stockés. La définition des expressions *«données informatiques», «données relatives aux abonnés ou DBA», «données de trafic»* et *«Fournisseur de services de communication»* sera également nécessaire.[383] L'article 25 de la CITO est un modèle à utiliser et qui contient différentes définitions, notamment pour les expressions *«système informatique»,*[384] *«fournisseur de services»*[385] *et «données»*[386]*.* Il serait souhaitable de pouvoir également définir les expressions *«données relatives aux abonnés ou DBA» et «données de trafic»,* car différents types de preuves pourront être produits par les FSC. En outre, ce pouvoir exigera des personnes et de toutes les autres entités (sociétés commerciales, institutions financières et autres organisations) qui détiennent des données de les remettre aux autorités chargées de l'application de la loi. L'article 18 de la CB et l'article 22 de l'HIPCAR pourraient constituer des guides pour une application uniforme des définitions.

382. Pas d'équivalent dans la CUA
383. Voir les définitions ci-dessus
384. Article 2, paragraphe 1, de la CITO: «*tout moyen matériel ou moral, ou ensemble de dispositifs interconnectés ou non, utilisés pour stocker des informations, les classer, les organiser, les restituer, les traiter, les développer et les échanger suivant des commandes et des instructions qui y sont stockées et ceci comprend toutes les entrées et sorties câblées à elles ou non par un système ou un réseau*».
385. Article 2, paragraphe 2, de la CITO: «*toute personne physique ou morale, publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ou qui procède au traitement ou au stockage des informations pour le service de communication ou ses utilisateurs*».
386. Article 2, paragraphe 3, de la CITO: «*tout ce qui peut être stocké, traité, émis et transmis au moyen d'un système informatique, tels que les chiffres, les lettres, les symboles* et autres».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: a. à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou b. à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[387] **Interception de données relatives au contenu** 1. 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	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir est déjà prévu dans la législation nationale et des garanties et des exigences/ procédures permettant de contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques au Maroc s'avèrent nécessaires. **Analyse des écarts** **Recommandations:** Il conviendrait d'obliger les FSC opérant au Maroc à coopérer à la collecte en temps réel des données de trafic. De même, des garanties devraient être intégrées afin d'assurer que la collecte soit légale, raisonnable et proportionnée au vu des circonstances. Il conviendrait de revoir l'article 29 de la CITO, l'article 21 de la CB et l'article 26 de l'HIPCAR, afin d'en incorporer les termes dans la législation nationale.

387. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de l'HIPCAR – Interception des données relatives au contenu 1. 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que le contenu d'une communication électronique est raisonnablement nécessaire aux besoins d'une enquête criminelle, il [peut] [doit]: a. ordonner à un fournisseur de services Internet dont les services sont disponibles en [État prenant les dispositions], en utilisant des moyens techniques, de collecter ou d'enregistrer ou de permettre aux autorités compétentes ou de les assister à collecter ou enregistrer les données de contenu associées à des communications spécifiées transmises par l'intermédiaire d'un système informatique; ou b. autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer lesdites données, à l'aide de moyens techniques. 2. Un pays peut décider de ne pas mettre en œuvre l'article 26. **Article 29 de la CITO - Interception de données relatives au contenu** 1. Chaque État partie s'engage à adopter les mesures législatives nécessaires concernant un éventail d'infractions prévues par son droit interne, pour permettre aux autorités compétentes:		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. de collecter ou d'enregistrer par l'application de moyens techniques existant sur le territoire de l'État partie, ou b. de prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer en temps réel les données relatives au contenu des communications spécifiques sur son territoire, transmises au moyen d'un système informatique. 2. Lorsque l'État partie, en raison de son système juridique interne, ne peut adopter les mesures énoncées au paragraphe (1- a), il peut adopter d'autres mesures qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel de données relatives au contenu des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque État partie adopte les mesures nécessaires pour obliger un fournisseur de services à garder le secret de toute information lors de l'exécution des pouvoirs prévus au présent article.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 20 de la CB[388] **Collecte en temps réel des données relatives au trafic** 1. 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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.	**Pas d'équivalent**	**Analyse juridique** Il n'existe pas de pouvoir de procédure permettant seulement de collecter des données de trafic en temps réel. Un seuil plus bas pourrait permettre de collecter les données de trafic en temps réel, ce qui constituerait un outil d'enquête essentiel. Dans certaines situations, le seuil légal supérieur permettant de sécuriser les contenus n'est pas établi par le demandeur, mais un seuil plus bas permettant de sécuriser le trafic pourrait l'être. Une distinction devrait donc être faite entre collecte en temps réel des contenus stockés et collecte des données de trafic. Des garanties et des exigences/procédures permettant de contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques au Maroc s'avèrent nécessaires. **Analyse des écarts** **Recommandations:** Il conviendrait d'instaurer un pouvoir spécifique permettant la collecte de données de trafic en temps réel et de contraindre les FSC opérant au Maroc à coopérer à la collecte en temps réel des contenus. De même, des garanties devraient être incorporées afin d'assurer que la collecte est légale, raisonnable et proportionnée au vu des circonstances. La terminologie utilisée à l'article 28 de la CITO pourrait être envisagée, mais elle ne fait pas référence à la collecte rapide en temps réel. L'article 20 de la CB et l'article 25 de l'HIPCAR devraient être utilisés comme guide pour la législation nationale.

388. Article 31, paragraphe 3, sous e), de la CUA – Notons que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 25 de l'HIPCAR - Collecte des données de trafic** 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		
		Obligation de divulgation et clés de chiffrement Dans la mesure où les terroristes et les criminels organisés utilisent systématiquement des applications de messagerie cryptée,[389] on pourrait envisager un pouvoir viable permettant d'ordonner la remise des clés pour les mots de passe afin de déverrouiller les dispositifs.[390] **Analyse des écarts** **Recommandation:** Nous ne sommes pas parvenus à déterminer si de tels pouvoirs existaient au Maroc (mais ces pouvoirs permettraient aux autorités chargées de l'application de la loi de contraindre les propriétaires à déverrouiller les dispositifs).

389. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, n°24 (15juin2015): 16-18. Academic Search Premier, EBSCOhost (consulté le 29 février 2016).
390. Pour obtenir un exemple, se reporter à l'article 49 de la loi britannique qui régit les pouvoirs d'enquête intitulée Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations en matière de conservation des données[391] Ledit pouvoir pourrait permettre aux autorités chargées de l'application de la loi de: 1. retracer et identifier la source d'une communication; 2. identifier la destination d'une communication; 3. identifier la date, l'heure et la durée d'une communication, et 4. identifier le type de communication. Le Maroc ne prévoit pas une telle obligation[392]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB **Compétence** 1. 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.	**Pas d'équivalent**	**Analyse juridique** En l'absence de champ d'application clairement défini en matière de cyber-crimes, de nature internationale, toute législation sera restreinte. **Analyse des écarts** **Recommandation:** La législation nationale doit garantir que la compétence est définie selon les termes utilisés à l'article 22 de la CB, à l'article 19 de l'HIPCAR ou à l'article 30 de la CITO. En cas de conflit de compétence, il conviendrait de tenir compte des lignes directrices relatives à la détermination de la juridiction compétente pour juger une infraction (voir le document intitulé Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (révisé en 2016)).[393]

391. En 2006, l'UE a publié une directive relative à la conservation des données (les États membres de l'UE devaient stocker les données afférentes aux télécommunications électroniques pendant au moins six mois et tout au plus 24mois, à des fins de recherche, de détection et de poursuite des infractions graves). En 2014, la Cour de justice de l'UE a annulé la directive relative à la conservation des données, estimant qu'elle ne prévoyait pas suffisamment de garanties contre les ingérences dans les droits à la vie privée et à la protection des données. En l'absence de directive valable de l'UE portant sur la conservation des données, les États membres peuvent toujours mettre en place un régime applicable à la conservation des données. Les régimes nationaux sont disponibles à l'adresse suivante: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
392. Examen de la législation type à l'échelle mondiale de l'ICMEC page 33
393. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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. **Article 19 de l'HIPCAR – Juridiction** La présente loi s'applique à tout acte ou omission commis: a. sur le territoire de [État prenant les dispositions]; b. sur un bateau ou un avion immatriculé en [État prenant les dispositions]; c. par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays; ou		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		
Article 35 de la CB[394] **Réseau 24/7** 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'un mécanisme essentiel pour disposer de capacités d'enquête efficaces en matière de cybercriminalité. **Analyse des écarts** **Recommandation:** Cette mesure ne devrait pas exiger l'adoption de législation de mise en œuvre, et sous réserve des ressources, elle devrait être établie en tant que priorité. Les coordonnées de contact devraient être partagées concernant le point de contact unique désigné (SPOC), dans le pays, avec les autorités centrales à l'international et INTERPOL. Il conviendrait d'envisager la rédaction d'un protocole d'entente avec les agences nationales, de façon à ce que le SPOC dispose de l'autorité nécessaire pour entreprendre les actions requises dans le cadre d'une enquête internationale sur la cybercriminalité, en application du droit national et des traités. Le protocole d'entente devrait porter aussi bien sur les demandes entrantes que sur les demandes sortantes, et assurer un processus efficient et efficace.

394. Article 43 de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.		
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.		**Analyse juridique** L'article 25 de la CB permet son utilisation en tant qu'instrument pour faciliter l'entraide. Le Maroc n'a pas encore ratifié la CB ni la CITO, et cette situation ne manquera pas d'entraver les enquêtes internationales, dans la mesure où les pouvoirs de procédure seront dépourvus de base légale. Outre plusieurs traités bilatéraux, le Maroc est signataire de la CNUCTO,[395] de sorte que l'article 18 de la CNUCTO constitue la base de l'entraide et de la mutualité/réciprocité.[396] Cela signifie qu'en l'absence de législation nationale, il est impossible de formuler des requêtes de conservation rapide des données informatiques stockées, de conservation et divulgation partielle rapides des données relatives au trafic, et de divulgation des données stockées et des données de trafic, ce qui restreint la coopération internationale que le Maroc peut apporter aux États requérants.

395. Ratifiée le 19 septembre 2002
396. L'article 18 de la CNUCTO pourrait constituer la base de l'entraide judiciaire si la définition de la criminalité transnationale organisée est retenue. Il en est de même concernant l'Accord de Riyad sur la coopération judiciaire pour les États l'ayant ratifié).).

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication. 4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.		**Analyse des écarts** **Recommandation:** L'adoption d'une législation nationale s'avère nécessaire en matière de conservation rapide des données informatiques stockées et de conservation et divulgation partielle rapides des données relatives au trafic, mais aussi concernant les injonctions de produire. La CB pourrait être utilisée en tant que précédent en ce qui concerne la conservation rapide des données stockées,[397] la conservation et divulgation partielle rapides des données relatives au trafic[398] et la divulgation des données stockées[399] et des données de trafic[400].

397. Article 29 de la CB
398. Article 30 de la CB
399. Article 31 de la CB
400. Article 33 de la CB

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante. **Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle** 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article; d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative. 7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis. e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de la CB **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre. 2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une procédure importante qui permet à un État d'avoir accès à des informations qui aideront un autre État à empêcher la cybercriminalité et à enquêter en la matière. Même si elles sont disponibles entre les États ayant ratifié la CITO (article 33 de la CITO), le Maroc ne dispose pas de base juridique permettant le partage d'informations avec les États non signataires de la CITO, sauf si une requête officielle est adressée par le biais des canaux d'entraide habituels. L'article 18, paragraphes 4 et 5, de la CNUCTO, prévoit le partage spontané d'informations dans le cadre des affaires répondant à la définition d'infractions graves, transnationales[401] et impliquant un groupe criminel organisé[402]. Sans répondre à cette définition. Une requête officielle devra être envoyée aux États non signataires de la CITO, en empruntant les canaux de l'entraide habituels. Étant donné l'évolution rapide de la cybercriminalité, il s'agit d'un moyen efficace de coopérer avec d'autres États, et son absence empêche toute collaboration internationale efficace avec les États non signataires de la CITO. **Analyse des écarts** **Recommandation:** Utiliser l'article 18, paragraphes 4 et 5 de la CNUCTO, comme base pour le partage spontané d'informations relevant du champ d'application de cette dernière (avec des garanties concernant l'utilisation des éléments de preuve ou la divulgation d'informations sensibles à des tiers (notamment un autre État)).[403] Envisager l'adoption d'une législation fondée sur l'article 33 de la CITO ou l'article 26 de la CB.

401. Article 3, paragraphe 1, de la CNUCTO
402. Au sens de l'article 2, sous a), de la CNUCTO, l'expression «groupe criminel organisé» désigne «un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves ou infractions établies conformément à la présente Convention, pour en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel».
403. Voir l'article 33, paragraphe 2, de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 33 de la CITO - Informations spontanées reçues 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou		**Analyse juridique** Ce pouvoir de procédure permet à un État d'obtenir des contenus stockés dans un autre État dans des circonstances limitées. L'article 32, sous b), de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permettent un accès transfrontalier unilatéral sans besoin d'entraide, s'il existe un consentement ou si les informations sont accessibles au public.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. **Article 27 de l'HIPCAR – Logiciel de criminalistique** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes: • le suspect de l'infraction, si possible avec ses nom et adresse; et • une description du système informatique ciblé; et • une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et	**Pas d'équivalent**	Exemples de recours à ce pouvoir de procédure dans le cadre de l'article 32, sous b), de la CB: le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données.[404] Un individu suspecté de terrorisme est arrêté dans les règles alors que son courrier électronique (révélant probablement des preuves d'un délit) est ouvert sur sa tablette, son smartphone ou un autre dispositif. Si le suspect consent volontairement à ce que la police accède à son compte, et si cette dernière est certaine que les données de la boîte de messagerie se trouvent dans un autre État, elle peut accéder à ces dernières dans le cadre de l'article 32, sous b). **Analyse des écarts** **Recommandation:** Prévoir ce pouvoir restreint de collecte unilatérale d'éléments de preuve dans la législation avec des garanties visant à assurer que les contenus seront légalement obtenus auprès de l'utilisateur.[405] La terminologie utilisée peut être celle de l'article 32 de la CB et de l'article 40 de la CITO. L'article 32, sous b), a été vivement critiqué et on pourrait envisager de demander le consentement de l'État dans lequel les données informatiques sont localisées en plus de celui de l'utilisateur. L'article 27 de l'HIPCAR prévoit des logiciels de criminalistique, lesquels pourraient permettre d'accéder à un ordinateur situé dans un autre État. Plusieurs restrictions empêchent l'obtention des éléments de preuve par d'autres moyens. Une décision judiciaire est requise et ne peut s'appliquer qu'à certaines infractions, pendant une durée restreinte (3mois). L'obtention du consentement de l'autre État doit être envisagée lorsque des logiciels criminalistiques sont susceptibles de faire intrusion.

404. Paragraphe 294, page 53 du Rapport explicatif de la CB

405. Il conviendrait également d'envisager les situations telles que l'absence de disponibilité de l'utilisateur (en cas de décès par exemple) et la possibilité d'obtenir le consentement dans un autre État.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner • le moyen technique utilisé ainsi que la date et l'heure de l'application; • l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et • toute information obtenue. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect. 5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions]. 8. Un pays peut décider de ne pas mettre en œuvre l'article27. **Article 40 de la CITO - Accès transfrontière à des données informatiques** Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité.		

Palestine

La Palestine a ratifié la CITO, et le 9 juillet 2017, la loi n°16 de 2017 sur les délits électroniques a été promulguée.[406]

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[407] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 6 de la CITO**	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 4(1)**	**Étude juridique** L'article 4(1) est conforme à l'article 6 de la CITO qui mentionne *«l›accès illégal à, la présence dans ou le contact avec»* sans définir ce que ces actes signifient. La CB mentionne *«sans droit»* dans l'Article 2 sur la base de la non autorisation de l'accès. Le Rapport explicatif de la CB a confirmé la dérivation de l'expression *«sans droit»* comme *«une conduite entreprise sans autorité (qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou une conduite autrement non couverte par des défenses, des excuses, des justifications ou des principes pertinents juridiques établis dans le cadre de la loi nationale.»* L'article 4(1) de la loi nationale inclut également une infraction de présence poursuivie illégale. La législation nationale n'inclut pas les programmes dans la définition de *«données»* **Analyse des lacunes** **Recommandation:** La législation nationale pourrait intégrer l'inclusion des programmes dans la définition des données car certaines données contiennent des programmes et d'autres non. En outre, la législation nationale pourrait prévoir une définition d'«accès illégal» afin de garantir qu›il s›agit uniquement d›une infraction sans justification ou excuse raisonnable. C›est la raison pour laquelle la CB inclut «*sans droits*» et garantit, par exemple, que les officiels d'application de la loi peuvent accéder à un système informatique lorsque cela est justifié dans le cadre d'une enquête.

406. Le texte est disponible uniquement en arabe.
407. Article 6 de la CITO et article 29, paragraphe 1, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 3 de la CB[408] **Interception illégale** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 7 de la CITO** **Interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 7**	**Étude juridique** Cette infraction est essentielle afin de poursuivre les transmissions de données informatiques vers, depuis ou au sein d'un système informatique qui peuvent être interceptées illégalement afin d'obtenir des informations (par ex. wikileaks ou Panama Papers). **Analyse des lacunes** **Recommandation:** Il convient de comprendre que la terminologie de l'article 7 de la CITO a été utilisée – la CITO ne contient pas de définition de *«données de technologie de l»information»* et celle-ci doit être intégrée de la manière appropriée pour faire la distinction avec les données. La législation nationale pourrait prévoir une définition de données ou données informatiques uniquement - L'article 3 de la CB désigne l'interception de *«données informatiques»* qui est définie dans l'article 1.b de la CB comme *«toutes les données informatiques associées à la communication par le biais d'un système informatique, générées par un système informatique faisant partie intégrante d'une chaîne de communication, indiquant l'origine de la communication, sa destination, sa voie, l'heure, la date, la taille, la durée ou le type de service sous-jacent.»*
Article 4 de la CB[409] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 4(3)**	**Étude juridique** Si la même terminologie est utilisée pour la législation nationale, comme stipulé dans la CITO, aucune référence n'est faite à *«sans droits».* En outre, la CITO n'inclut pas la suppression de données informatiques qui est un élément de hameçonnage pour obtenir un accès illégal par installation d'un enregistreur de frappe afin d'obtenir des informations sensibles.[410]

408. Article 29, paragraphe 2, de la CUA
409. Article 29, paragraphe 1, sous e) à f), de la CUA
410. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux. **Article7 de l'HIPCAR – Atteinte à l'intégrité des données** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants: • endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes; • obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse des lacunes** **Recommandation:** L'absence de certains éléments clés associés à cette infraction dans la CITO peut être corrigée en utilisant la terminologie de l'article 4 de la CB ou de la section 7 de l'HIPCAR. L'utilisation de «*sans droits*» (voir ci-dessus concernant l'accès illégal) garantirait que les officiels d'application de la loi, par exemple, pourront interagir avec les données, si cela est approprié et justifié dans le cadre d'enquêtes.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 8 de la CITO **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.		
Article 5 de la CB[411] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. **Article9 de l'HIPCAR – Atteinte à l'intégrité du système** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: • entrave ou porte atteinte au fonctionnement d'un système informatique; ou • entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 4(3)**	**Étude juridique** La CITO ne contient pas d'infraction d'interférence avec le système, il est difficile de savoir quelle terminologie a été utilisée pour la législation nationale. L'article 11 de la CITO mentionne *«l'interférence avec le fonctionnement des systèmes d'exploitation et systèmes de communications ou la tentative de perturber ou modifier ceux-ci»*. De même, *«la perturbation d'instrument électroniques, programmes et sites»*. Bien que cela ait été fait avec pour objectif de commettre une *«fraude»*. Cette infraction empêcherait les logiciels malveillants qui perturbent le fonctionnement d'un ordinateur par des pirates informatiques sans avoir l'objectif de commettre une fraude. **Analyse des lacunes** **Recommandation:** La terminologie de la CB dans l'article 5 ou la section 9 de l'HIPCAR constitue un précédent utile. De même, il convient d'examiner si la prévention et la poursuite des attaques contre l'infrastructure critique doit constituer une infraction séparée ou aggravée (voir la section 9(2) de l'HIPCAR). Cette infraction aggravée serait pertinente lorsque les terroristes entravent le fonctionnement de systèmes informatiques hospitaliers par le biais d'une attaque par déni de service.[412]

411. Article 29, paragraphe 1, sous d), de la CUA sans équivalent dans la CITO
412. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		
Article 6 de la CB[413] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 26**	**Étude juridique** Comme ci-dessus, concernant l'accès illégal, aucune référence n'est faite à «sans droits» dans l'article 9 de la CITO Cette infraction permettra les poursuites pour la production, la vente, l'obtention pour utilisation, l'importation, la distribution de codes d'accès et autres données informatisées pour commettre des cybercrimes - par exemple l'accès à des systèmes informatiques pour faciliter une attaque terroriste en perturbant le réseau électrique d'un pays. **Analyse des lacunes** **Recommandation:** Si la terminologie de l'article 9 dans la CITO est utilisée, il est toujours difficile de savoir si les appareils disposant d'une utilisation légitime étant utilisé à des fins criminelles *(«double usage»)* sont interdits – cela pourrait être réglé en incluant la terminologie de la CB de *«principalement adapté»* La loi nationale doit fournir une excuse raisonnable pour que les autorités policières puissent utiliser les appareils pour des techniques d'enquêtes spéciales – voir la terminologie de l'article 6.2. de la CB ou la section 10(2) de l'HIPCAR pour guide

413. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée. 2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 9 de la CITO **Article10 de l'HIPCAR – Dispositifs illégaux** 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, avec l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.		**Étude juridique** La terminologie de l'article 10 dans la CITO ne fait pas référence à toute intention malhonnête et nécessite que des dommages soient provoqués **Analyse des lacunes** **Recommandation:** La terminologie de l'article CB et l'HIPCAR ne nécessite pas que des dommages soient provoqués. La CB et l'HIPCAR nécessitent uniquement que les données *«données non authentiques» soient «prises en compte»* L'article 7 de la CB ou la section 11 de l'HIPCAR, par conséquent, protègent contre la contrefaçon informatique, qui pourrait inclure le hameçonnage et le harponnage lorsqu'un utilisateur les subit sans qu'aucun dommage ne soit provoqué.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article11 de l'HIPCAR – Falsification informatique 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux. **Article 10 de la CITO** **Infraction de falsification** Utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 11**	Par exemple, les données informatiques (telles que les données utilisées dans les passeports électroniques) peuvent être entrées, altérées, effacées ou supprimées, entraînant la prise en compte de données non authentiques comme si elles étaient authentiques[414] sans qu'aucun dommage ne soit provoqué. Selon CITO, cela ne constituerait pas une infraction. Il convient également d'examiner la Section 11(2) de l'HIPCAR (non inclue dans la CITO) qui vise l'envoi de multiples messages de courrier électronique comme une infraction aggravée.

414. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 8 de la CB[415] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article 11 de la CITO** **Article12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; • avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 14**	**Étude juridique** La terminologie de l'article 11 de la CITO est vague, sans référence à toute intention malhonnête et nécessite une forme de *«dommages» sans définir ce que ces termes couvrent* **Analyse des lacunes** **Recommandation:** La CITO nécessite uniquement une intention - la terminologie de la CB ou de l'HIPCAR prévoit l'exigence d'une intention malhonnête.

415. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 9 de la CB[416] **Infractions se rapportant à la pornographie enfantine** **AJOUTER CONTENU ARTICLE** **Article 12 de la CITO** **Article13 de l'HIPCAR – Pédopornographie ou pornographie infantile** **AJOUTER CONTENU ARTICLE**	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 16**	**Étude juridique** Il s'agit d'une infraction essentielle afin de protéger les enfants du danger en criminalisant la distribution, la transmission, la mise à disposition, l'offre, la production et la possession d'images indécentes d'enfants. **Analyse des lacunes** **Recommandation:** Si la terminologie de l'article 12 de la CITO est utilisée, il n'existe pas de définition d'enfant ou de mineur – cela devrait être similaire avec la législation nationale existante. L'article 9.3 de la CB ne fournit pas de définition de *«mineur»* En outre, il n'existe pas de définition d'«outrage public à la pudeur» L›article 9.2 prévoit une définition de *«pornographie infantile»* L'infraction de la CITO est commise par le biais de la *«technologie de l'information»* définie dans l›article 2(1) de la CITO comme *«tout matériel ou moyen virtuel ou groupe de moyens interconnectés utilisés pour stocker, trier, disposer, récupérer, traiter, développer et échanger des informations conformément à des commandes et des instructions stockées à l'intérieur. Cela inclut toutes les entrées et sorties associées, au moyens de câbles ou sans fil, dans un système ou un réseau.»* Comme il est fait référence à «interconnectés», cela ne comprend pas les supports de stockage de la manière interdite dans l›article 9.1.e de la CB La CITO ne couvre pas les infractions consistant en *«offre» «mise à disposition» ou «fourniture à un tiers» d'images* pornographiques d'enfants de la manière interdite dans l'article 9.1. de la CB et section 13 de l'HIPCAR

416. Article 12 de la CITO et article 29, paragraphe 3, sous a à d), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 10 de la CB[417] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 8**	**Étude juridique** Les autorités d'application de la loi utilisent les infractions en matière de droits d'auteur numériques dans le monde entier comme conduite criminelle supplémentaire pour enquêter sur et poursuivre différentes formes de cybercriminalité (y compris les crimes tels que le hameçonnage, la fraude électronique, la contrefaçon électronique, les sites Internet frauduleux et le vol de données/ violations de données). L'une des infractions sous-jacentes dans de nombreux cas est la violation des droits d'auteur numériques. La cyber-attaque Sony[418] ne constitue qu'un exemple récent dans lequel les infractions et pouvoirs associés à la cybercriminalité, le vol de données/ espionnage industriel et la violation des droits d'auteur viennent se compléter. L'absence de toute disposition concernant la propriété intellectuelle constitue un échec dans la protection de l'innovation du 21e siècle concernant les PPVS, entreprises et citoyens. Elle peut bien sûr être protégée dans d'autres législations que la présente analyse n'a pas examinées **Analyse des lacunes** **Recommandation:** S'assurer de l'existence de protections contre la violation des droits d'auteur en conformité avec les obligations internationales.

417. Pas d'équivalent dans la CUA et l'HIPCAR
418. https://en.wikipedia.org/wiki/Sony_Pictures_hack

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 17 CITO - Infractions relatives à la violation des droits d'auteur et des droits connexes La violation des droits tels que définis dans la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel et la violation des droits connexes afférents aux droits d'auteur tels que définis par la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel.		
Article 11 de la CB[419] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 52**	**Étude juridique** La CITO ne prévoit pas d'article pour criminaliser ceux coupables d'aide et de complicité à des cybercrimes. Bien que l'article 19 de la CITO n'inclut pas la tentative **Analyse des lacunes** **Recommandation:** L'article 19 de la CITO mentionne uniquement la tentative et la législation nationale devrait utiliser l'article 11 de la CB comme précédent pour garantir que les personnes ayant fourni leur assistance ou encouragé la réalisation de cybercrimes puissent être poursuivies.

419. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2du présent article.		
Article 12 de la CB[420] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 52**	**Étude juridique** Cette disposition constitue un élément essentiel afin que des personnes morales (par ex. des entités professionnelles) agissant pour le compte de personnes physiques disposent d'une responsabilité pénale **Analyse des lacunes** **Recommandation:** L'article 20 de la CITO ne prévoit pas de disposition selon laquelle une entreprise peut être tenue responsable lorsqu'elle n'a pas exercé une supervision ou un contrôle suffisant et qu'une personne physique concernée a commis une infraction criminelle en agissant sous son autorité – voir article 12.2. de la CB

420. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction. **Article 20 de la CITO**		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[421] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 24**	**Étude juridique** Si l'article 3 du Protocole supplémentaire a été utilisé, cela constitue un précédent approprié

421. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Protocole additionnel **Article 4[422] – Menace avec une motivation raciste et xénophobe** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 24**	**Étude juridique** Si l'article 4 du Protocole supplémentaire a été utilisé, cela constitue un précédent approprié
Protocole additionnel **Article 5[423] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.		

422. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO
423. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.	**Aucun équivalent**	**Analyse des lacunes** **Recommandation:** Utiliser la terminologie de la CB dans l'article 5 du Protocole Supplémentaire comme guide pour la législation nationale
Protocole additionnel **Article 6[424] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 25**	**Étude juridique** Si l'article 6 du Protocole supplémentaire a été utilisé, cela constitue un précédent approprié

424. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à étudier		
Infractions liées à l'identité **Article14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 10**	Étude juridique Cette infraction couvre la phase préparatoire d'un crime de malhonnêteté lié à l'identité– **Analyse des lacunes** **Recommandation:** Si la section 14 de l'HIPCAR a été incluse, cela constitue un précédent approprié

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Divulgation des détails d'une enquête **Article16 de l'HIPCAR** Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 48**	**Étude juridique** Cette infraction sanctionne les violations de données et la divulgation d'informations sensibles qui pourraient affecter les enquêtes criminelles **Analyse des lacunes** **Recommandation:** Si la section 16 de l'HIPCAR a été incluse, cela constitue un précédent approprié
Refus d'autoriser l'assistance **Article17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22425 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 41**	**Analyse des lacunes** **Recommandation:** Si la section 17 de l'HIPCAR a été incluse, cela constitue un précédent approprié Une infraction séparée est recommandée pour le défaut de fourniture de mots de passe ou d'accès à des codes vers des données ou des appareils cryptés (c'est-à-dire *«une clé vers des informations protégées»*) – la section 53 de la loi anglaise régissant les pouvoirs d'enquête de 2000 (RIPA) [426] *prévoit de caractériser en infraction pénale les personnes qui ne se conforment pas à une section 49 de la RIPA Avis de divulgation de la «clé»*

425. Perquisition et saisie, assistance et injonctions de produire
426. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 15**	Étude juridique Cette infraction criminalise ceux qui harcèlent des personnes en ligne– certaines juridictions peuvent prévoir des infractions de harcèlement non liées à l'informatique – mais cette infraction est recommandée pour les crimes commis en ligne. **Analyse des lacunes** **Recommandation:** Si la section 18 de l'HIPCAR a été incluse, cela constitue un précédent approprié
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Celui qui propose d'organiser un rendez-vous, par le biais d'un système automatisé ou en ayant recours à un service de communication, à une personne concernant laquelle il sait, ou devrait penser raisonnablement, qu'elle n'a pas atteint l'âge de seize ans, dans l'intention de commettre des actes indécents avec ladite personne ou de créer une image d'un acte sexuel impliquant ladite personne, sera puni d'une peine d'emprisonnement d'une durée maximale de deux ans ou d'une amende de la quatrième classe, s'il entreprend une quelconque action visant la matérialisation dudit rendez-vous.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Articles 16(3), (4) et 56**	**Étude juridique** Pour prouver l'infraction néerlandaise, un rendez-vous à des fins sexuelles est requis pour apporter la preuve de l'historique de discussion en ligne à caractère sexuel, une demande de rendez-vous avec preuve de la planification (c'est-à-dire la date et le lieu). Le but de la loi canadienne est d'empêcher la préparation des adultes prédateurs des enfants en ligne. Cette infraction ne nécessite pas la commission de l'infraction sexuelle. Cela signifie que l'accusé n'a pas besoin de s'être réellement présenté au rendez-vous pour rencontrer la victime en personne. L'infraction est commise avant que toute action n'ait lieu pour commettre l'infraction substantielle. **Analyse des lacunes** **Recommandation:** Si la législation nationale empêche le fait d'amadouer, sans qu'un rendez-vous n'ait nécessairement lieu, cela est approprié.

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Code criminel canadien **Section 172.1** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170, 171 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dix ans maximum, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huitmois, la peine minimale étant de quatre-vingt-dix jours.		

Infractions		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de la CITO - Perquisition de données stockées 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci; b. un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques.	**Décret-Loi N° 20 de 2015 sur la Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme** **Article 33** Pouvoirs du Procureur général: Le Procureur général peut, sur la base d'une décision du tribunal compétent....Accéder aux réseaux et systèmes informatiques et aux principaux ordinateurs **Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 33**	**Étude juridique** Il s'agit du principal pouvoir d'enquête et doit faire référence à obtenir l'accès plutôt qu'à la recherche. Dans le Rapport explicatif de la CB, «recherche» signifie chercher, lire, inspecter ou examiner des données. Cela inclut la notion de recherche de données et de recherche (examen) dans des données. Le terme *«accès»* a une signification neutre et reflète plus précisément la terminologie informatique – il est également inclus dans les articles 26 et 27 de la CITO.[427] L'article 33 du décret législatif N° 20 de 2015 concerne l'accès, mais est seulement disponible pour le blanchiment d'argent et le financement du terrorisme. L'article 33 de la loi N° 16 de 2017 sera plus étendu et s'applique aux infractions de cybercriminalité qu'il criminalise.

427. Paragraphe 191, page 33 du Rapport explicatif de la CB

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1(a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe 1 de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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; d. enlever ou rendre inaccessibles ces données du système informatique consulté.	**Article 34 :** 1. Le ministère public doit disposer d'un accès aux appareils, outils, moyens, données, informations électroniques, données de trafic, données liées au trafic des communications ou leurs utilisateurs ou informations de contenu liés à un crime électronique. 2. Le Ministère public a le droit d'autoriser et de préserver strictement le système d'informations, en totalité ou en partie ou tout moyen de technologie de l'information qui pourraient aider à découvrir la vérité. 3. Si la saisie du système d'informations n'est pas nécessaire ou ne peut pas être mise en place, les données ou informations liées au crime et les données considérées comme ayant été lues et comprises seront copiées sur l'un des moyens de technologie de l'information. 4. S'il est impossible de réaliser la saisie ou de détenir efficacement le système, afin de conserver les preuves du crime, tous les moyens appropriés doivent être utilisés pour empêcher l'accès au système ou aux données stockées dans le système d'informations. 5. Les précautions nécessaires doivent être mises en place pour maintenir l'intégrité de la saisie effectuée, y compris les moyens techniques pour protéger son contenu.	L'Article 34(1) confirme l'accès aux ordinateurs et aux données concernant les crimes dans la loi N° 16. L'article 34(3) permet de copier les données pertinentes si elles ne sont pas saisies. L'article 34(4) empêche l'accès si les données ne peuvent pas être saisies et l'article 34(5) requiert que l'intégrité des données saisies soit maintenue. Ces dispositions sont conformes à la CITO

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes 2 et 3 de l'article 26 de la présente Convention.	6. Un rapport consigné doit être conservé en présence de l'accusé ou de ceux dont il est reconnu qu'ils ont effectué la saisie. La saisie conservée doit être gardée en conformité avec l'affaire dans une enveloppe ou une enveloppe scellée, avec un papier mentionnant la date et l'heure de la réservation et le numéro des dossiers et de l'affaire.	
Article 16 de la CB[428] **Conservation rapide des données informatiques stockées** 1. 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.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 34**	**Étude juridique** Ce pouvoir d'enquête est important pour garantir que les données vulnérables à la suppression ou la perte sont préservées **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré de conserver les BSI, les données de trafic et le contenu enregistré et des transactions est essentiel dans le cadre des enquêtes sur la cybercriminalité pour s'assurer que des preuves sont disponibles pour la recherche, l'accès, la saisie et la vérification. La législation nationale nécessitera des définitions suffisantes des termes *«informations d›abonnés ou BSI»*,[429] *«données de trafic»*[430] *et «Fournisseur de service de communication»*[431] pour garantir leur conservation.

428. Pas d'équivalent dans la CUA

429. Voir la définition dans le Glossaire ci-dessous ou l'article 2(9) de la CITO: «Toute information dont le fournisseur de service a connaissance concernant les abonnés au service, à l'exception des informations grâce auxquelles les éléments suivants peuvent être connus: a. le type de service de communication utilisé, les exigences techniques et la période de service. b. l'identité de l'abonné, son adresse postale ou géographique ou son numéro de téléphone et les informations de paiement disponibles conformément au contrat de service ou à l'agencement. c. tout autre information sur le site d'installation de l'équipement de communication conformément au contrat de service.»

430. Voir Article 1.d de la CB: «toute les données informatiques associées à la communication par le biais d›un système informatique, générées par un système informatique faisant partie intégrante d›une chaîne de communication, indiquant l›origine de la communication, sa destination, sa voie, l›heure, la date, la taille, la durée ou le type de service sous-jacent» **ou** la section 3(18) de l'HIPCAR: «Le trafic de données *désigne toutes les données informatiques qui: a. sont associées à la communication par le biais d'un système informatique; et b. sont générées par un système informatique faisant partie intégrante d'une chaîne de communication; et c. indiquent l'origine de la communication, sa destination, sa voie, l'heure, la date, la taille, la durée ou le type de service sous-jacent.»*

431. Voir article 1.c. de la CB: «i toute entité publique ou privée qui fournit aux utilisateurs de son service la capacité de communiquer par le biais d›un système informatique et ii toute autre entité qui traite ou stocke des données informatiques pour le compte de tels services de communication ou utilisateurs de tels services» **ou** l'article 2(2) de la CITO: «toute personne physique ou morale, publique ou privée, qui fournit à des abonnés les services nécessaires pour communiquer par le biais de la technologie de l'information ou pour traiter ou stocker des informations pour le compte du service de communication ou de ses utilisateurs.»

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15.		Il convient de tenir compte que la durée de conservation jugée raisonnable dans les circonstances et permettant une demande de prolongation dans des circonstances particulières – la CB et la CITO prévoient 90 jours et l'HIPCAR 7 jours. D'après l'expérience, 90 jours est trop court dans une enquête de cybercriminalité, le chiffre devrait se rapprocher de 180 jours puis être soumis à prolongation.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article23 de l'HIPCAR – Conservation rapide Si un [agent de répression] [police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle veille à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		
Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 34**	**Étude juridique** Ce pouvoir procédural est particulièrement important pour s'assurer que les FSC fournissent les adresses IP pouvant localiser l'auteur d'un cybercrime La CITO ne dispose pas d'une définition des *«informations de suivi»* – cela serait différent des données de trafic car ces dernières incluraient l'origine de la communication, sa destination, sa voie, l'heure, la date, la taille, la durée ou le type de service sous-jacent (voir l'article 1.d. de la CB ou section 3(18) de l'HIPCAR) **Analyse des lacunes** **Recommandation:** Ce pouvoir accéléré, ainsi que la divulgation des données de trafic, devraient inclure des définitions des «données de trafic» et du *«Fournisseur de service de communication»*[432]

432. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 32** **Ordre de production**	**Étude juridique** Il existe une disposition cruciale pour une enquête efficace en matière de cybercrime et son absence affectera les poursuites et la coopération internationale. **Analyse des lacunes** **Recommandation:** Ce pouvoir crucial est nécessaire pour garantir que les FSC de la PA fournissent les BSI, les données de trafic et les données du contenu stocké. Il convient également d'ajouter des définitions des *«informations d'abonnés ou BSI», «données de trafic» et «Fournisseur de service de communication».*[433] L'article 25 de la CITO utilise des définitions incluant *«technologie de l'information»,*[434] *«fournisseur de service»*[435] *et «données»*[436] – nous recommandons d'ajouter des définitions pour *«informations d'abonnés ou BSI» et «données de trafic» car il* existe différents types de preuves pouvant être fournies par les FSC. En outre, ce pouvoir obligera les individus et les tiers (tels que les entreprises, les institutions financières et les autres organismes) qui détiennent des données à les produire aux autorités policières.
Article 29 de la CITO - Interception de données relatives au contenu	**Décret-Loi N° 20 de 2015 sur la Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme** **Article 33** Le Procurer général peut, sur décision du tribunal compétent, 1. Contrôler les comptes bancaires et autres comptes similaires.	**Étude juridique** Ce pouvoir est essentiel pour la législation nationale contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel en Palestine). L'article 33 du décret législatif N° 20 de 2015 concerne seulement les enquêtes sur le blanchiment d'argent et le financement du terrorisme. L'article 35 de la loi N° 16 de 2017 sera plus étendu et s'applique aux infractions de cybercriminalité qu'il criminalise.

433. idem
434. Article 2(1) de la CITO: «*tout matériel ou moyen virtuel ou groupe de moyens interconnectés utilisés pour stocker, trier, disposer, développer et échanger des informations conformément à des commandes et des instructions stockées à l'intérieur. Cela inclut toutes les entrées et sorties associées, au moyens de câbles ou sans fil, dans un système ou un réseau.*»
435. Article 2(2) de la CITO: «toute personne physique ou morale, publique ou privée, qui fournit à des abonnés les services nécessaires pour communiquer par le biais de la technologie de l'information ou pour traiter ou stocker des informations pour le compte du service de communication ou de ses utilisateurs.»
436. Article 2(3) de la CITO: «tout ce qui peut être stocké, traité, généré et transféré par le biais de la technologie de l'information, comme des nombres, lettres, symboles, etc…» - L'article 1.b. de la CB prévoit également un programme susceptible d'amener un système informatique à effectuer une function.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
	2. Accéder aux réseaux et systèmes informatiques et aux ordinateurs principaux 3. Soumis à la surveillance ou au suivi des communications. 4. Enregistrer ou décrire par le biais de moyens audiovisuels des actes, comportement ou conversations. 5. Intercepter et conserver les correspondances. **Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 35(2)** Le Ministère public peut ordonner le recueil et la fourniture immédiats de toute données, y compris le trafic, informations électroniques, données de trafic ou informations de contenu jugés nécessaires dans le cadre de l'enquête, en utilisant les moyens techniques appropriés et, lorsque cela est approprié, en utilisant les fournisseurs de service en fonction du type de service qu'ils fournissent.	
Article 28 de la CITO	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 35(2)** Le Ministère public peut ordonner le recueil et la fourniture immédiats de toute donnée, **y compris le trafic, informations électroniques, données de trafic** ou informations de contenu jugés nécessaires dans le cadre de l'enquête, en utilisant les moyens techniques appropriés et, lorsque cela est approprié, en utilisant les fournisseurs de service en fonction du type de service qu'ils fournissent.	**Étude juridique** L'article 35(2) possède le même seuil pour les informations de contenu - à savoir le recueil des données de trafic si nécessaire pour l'enquête. **Analyse des lacunes** **Recommandations:** Il convient d'étudier l'inclusion d'un seuil différent. Il pourrait exister des situations où un seuil légal plus élevé pour accéder aux contenus pourrait ne pas être compris par un demandeur – mais un seuil plus bas pour accéder au trafic peut l'être. Aussi, il pourrait exister une distinction entre la collecte en temps réel de contenus stockés et de données de trafic.

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations de conservation des données[437] Un tel pouvoir peut permettre aux autorités policières de 1. Tracer et identifier la source d'une communication 2. Identifier la destination d'une communication; 3. Identifier la date, l'heure et la durée d'une communication; et 4. Identifier le type de communication Impossible d'identifier si la Palestine a une telle obligation[438]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 30 CITO - Compétence 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État;	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 2**	**Étude juridique** L'article garantira un cadre clairement défini pour les infractions de cybercriminalité, qui sont de nature internationale. **Analyse des lacunes** **Recommandation:** La législation nationale garantit que la juridiction est définie. S'il existe un conflit entre des juridictions, il convient de tenir compte des directives quant à la détermination de la juridiction appropriée pour poursuivre une infraction – consulter les directives Eurojust permettant de décider quelle juridiction doit poursuivre (révisées en 2016)[439]

437. En 2006, l'UE a émis sa directive de conservation des données - les États Membres de l'UE devaient stocker les données de télécommunications électroniques pendant au moins six mois et au plus 24 mois pour enquêter, détecter et poursuivre des crimes graves. En 2014, la Cour de Justice de l'UE a invalidé la directive de conservation des données, arguant qu'elle fournissait des garanties insuffisantes contre les interférences avec les droits à la vie privée et la protection des données. En l'absence d'une direction de conservation des données valide de l'UE, les États Membres peuvent toujours prévoir un protocole de conservation des données – pour les protocoles nationaux, consulter: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention
438. Examen global ICMEC page 30
439. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition. 3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 43 de la CITO **Autorité spécialisée**[440] 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. 2. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. 3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.	**Aucun équivalent**	Étude juridique Il s'agit d'un mécanisme essentiel pour disposer d'une aptitude efficace à l'enquête de cybercrimes. **Analyse des lacunes** **Recommandation:** La mise en œuvre ne devrait pas nécessiter de législation et, en fonction des ressources, cette mesure devrait être établie en priorité. Les coordonnées doivent être partagées pour le point de contact unique (SPOC) nommé au niveau national, au niveau international pour les autorités centrales et INTERPOL. Il convient également de tenir compte de l'élaboration d'un Mémorandum de compréhension avec les agences nationales, afin que le SPOC dispose d'une autorité pour entreprendre les actions requises dans le cadre d'une enquête de cybercriminalité internationale appliquant les traités et lois nationaux. Ce MOU doit comprendre les requêtes entrantes et sortantes et garantir un processus efficace et effectif.

440. Article 35 de la CB et article 25, paragraphe 2, de la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et l'État requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles; c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Articles 43 et 44**	**Étude juridique** Les articles 32 et 34 de la CITO garantissent qu'il peut être utilisé comme un instrument pour faciliter la MLA et la loi nationale prévoit maintenant la préservation accélérée des données informatiques enregistrées, la préservation accélérée et la divulgation partielle des données de trafic, la divulgation des données enregistrées et données de trafic, l'interception de données de contenu, la collecte en temps réel de données de trafic, les ordres de production et les recherches et la saisie vers les États parties de la CITO. De la même manière, selon le principe de réciprocité, la Palestine peut exécuter des requêtes des États signataires de la CB et d'autres ayant les mêmes mesures procédurales.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires. 6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
7. L'État partie requérant peut demander à l'État partie requis de garder confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL. c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		
Article 33 de la CITO - Informations spontanées reçues 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 43**	**Étude juridique** Il s'agit d'une procédure importante afin de permettre à un État ayant connaissance d'informations qui aideraient un autre État à empêcher un cybercrime ou à enquêter sur celui-ci. La Palestine ne dispose pas d'une base de législation nationale pour partager de telles informations **Analyse des lacunes** **Recommandation:** Il convient d'examiner la présence de garanties sur l'utilisation des informations fournies spontanément dans les preuves ou la divulgation d'informations sensibles à un tiers (y compris un autre État).[441]

441. Voir article 33(2) de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 40 de la CITO - Accès transfrontière à des données informatiques Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité. **Article 27 de l'HIPCAR – Logiciel de criminalistique** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes:	**Loi N° 16 de 2017 sur les Crimes Électroniques** **Article 40**	**Étude juridique** Ce pouvoir procédural permet à un État de garantir le contenu stocké dans un autre État dans des circonstances limitées. L'article 40 de la CITO est une exception au principe de territorialité et permet l'accès transfrontalier unilatéral sans besoin d'entraide judiciaire en cas d'accord de l'utilisateur ou quand l'information est publiquement disponible. Les exemples d'usage de ce pouvoir procédural comprennent : L'adresse électronique d'une personne peut être enregistrée dans un autre pays par un fournisseur de service, ou une personne peut enregistrer sciemment des données dans un autre État. Ces personnes peuvent récupérer les données et à condition qu'elles en aient l'autorité légitime, elles peuvent volontairement divulguer les données à des officiels d'application de la loi, ou permettre à ces officiels d'accéder aux données[442] Ou Un terroriste présumé est arrêté légalement pendant que sa boîte de réception électronique – contenant éventuellement des preuves d'un crime – est ouverte sur sa tablette, son smartphone ou un autre appareil. Si le suspect consent volontairement à ce que la police accède à son compte et si la police est sûre que les données de la boîte de réception sont situées dans un autre État, la police peut accéder aux données.

442. Paragraphe 294, page 52 du Rapport explicatif de la CB

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
• le suspect de l'infraction, si possible avec ses nom et adresse; et • une description du système informatique ciblé; et • une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; et • les raisons justifiant la nécessité de l'utilisation. 2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner a. le moyen technique utilisé ainsi que la date et l'heure de l'application; b. l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et c. toute information obtenue. Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès non autorisé. 3. La durée de l'autorisation mentionnée à l'article 27, paragraphe 1 est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect.		**Analyse des lacunes** **Recommandation:** Ce pouvoir restreint à récupérer unilatéralement les preuves est désormais inclus dans la législation, ce qui garantit que le consentement de l'utilisateur est obtenu légalement.[443] L'article 40 ne prévoit pas le consentement de l'État requérant. La section 27 de l'HIPCAR prévoit un certain nombre de restrictions qui nécessitent que les preuves ne puissent pas être obtenues par d'autres moyens, qu'un ordre judiciaire soit requis, qu'il ne peut s'appliquer qu'à certaines infractions et que sa durée soit limitée (3 mois). Il convient également d'examiner le consentement de l'autre État dans lequel le logiciel judiciaire peut intervenir.

443. Il convient d'examiner des situations telles que la non disponibilité d'un utilisateur (par ex. sa mort) et si le consentement peut être obtenu dans un autre État

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20. 6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions]. 8. Un pays peut décider de ne pas mettre en œuvre l'article27.		

Tunisie

Il convient de noter que même si la Tunisie ne dispose pas encore de législation en matière de cybercriminalité, une loi est en cours de préparation. La Tunisie a adhéré à la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son Protocole additionnel n°181 sur les autorités de contrôle et les flux transfrontières de données.[444] Ces conventions ratifiées occupent la deuxième position dans la pyramide des textes juridiques applicables en Tunisie, juste après la Constitution et avant les lois et les décrets.

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 2 de la CB – Accès illégal[445] Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique. **Article 6 de la CITO – Infraction d'accès illégal** 1. L'accès ou le maintien illégal et tout contact avec tout ou partie d'un système informatique. 2. La peine est aggravée lorsqu'il résulte de cet accès, maintien, liaison ou continuation de ce contact:	**Code pénal** **Article 199 bis** (...) quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données.	**Analyse juridique** La disposition nationale utilise le terme *«frauduleusement»*, ce qui semble suggérer que l'auteur a accédé aux données de façon malhonnête (alors que la CB utilise l'expression «sans droit» en cas d'accès non autorisé). La CB évoque *«l'intention malhonnête»*, mais cela porte sur l'obtention de données plutôt que sur l'acte illégal en lui-même. Actuellement, cette infraction nationale peut être perpétrée uniquement si l'auteur fait preuve d'une intention malhonnête. En l'absence de définition du terme *«frauduleusement»*, on ne sait pas si cela exige un acte manifeste ou si chaque accès illégal est considéré comme frauduleux. Une définition du terme *«frauduleux»* s'avère donc nécessaire. L'infraction fait également référence à un *«système de traitement automatisé de données»*, sans définir ce dernier. On ne sait pas si elle concerne un *«système informatique»* (à savoir 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 (article 1 de la CB) ou des *«données informatiques»* (à savoir toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme permettant à un système informatique d'exécuter une fonction (article 1 de la CB)).

444. Loi organique n°2017-42 du 30 mai 2017 portant approbation de l'adhésion de la République Tunisienne à la convention n°108 du conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de son protocole additionnel n°181 concernant les autorités de contrôle et les flux transfrontières de données

445. Article 29, paragraphe 1, de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
a. La suppression, la modification, la déformation, le transfert, la reproduction ou la destruction des données sauvegardées, des appareils et des systèmes électroniques et des réseaux de communication, et de porter préjudice aux utilisateurs et bénéficiaires. b. L'obtention de renseignements gouvernementaux confidentiels. **Article 4 de l'HIPCAR – Accès illégal** 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, accède intentionnellement à l'ensemble ou à une partie d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le simple accès non autorisé si d'autres recours efficaces existent. En outre, un pays peut imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.		L'article 6 de la CITO fait référence à «l'accès ou le maintien illégal et tout contact avec», sans définir ce que ces actes signifient. Le recours à la CB et à l'HIPCAR devrait donc être privilégié. **Recommandation:** La législation nationale pourrait intégrer la terminologie pertinente de la CB et/ou de l'HIPCAR, afin d'inclure la définition de l'expression système informatique et l'inclusion des programmes dans la définition des données, dans la mesure où certaines données incluent des programmes et d'autres non. En outre, pour faire preuve de cohérence par rapport à la CB/l'HIPCAR, il conviendrait d'évoquer l'accès *«sans droit» plutôt que «frauduleusement».* Il conviendrait d'envisager la création d'un délit aggravé si l'accès illégal concerne le système informatique ou les données d'une infrastructure critique.

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 5 de l'HIPCAR – Présence illégale 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, reste intentionnellement connectée à l'ensemble ou une partie d'un système informatique, ou qui continue d'utiliser un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser la connexion non autorisée si d'autres recours efficaces existent. Un pays peut également imposer que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques ou dans toute autre intention malhonnête.		
Article 3 de la CB[446] - Interception illégale Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.	**Pas d'équivalent**	

446. Article 29, paragraphe 2, de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 6 de l'HIPCAR – Interception illégale 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, intercepte intentionnellement, par des moyens techniques: • toute transmission non publique vers, de, ou au sein d'un système informatique; ou • des émissions électromagnétiques provenant d'un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut imposer que l'infraction soit commise avec une intention malhonnête ou en rapport avec un système informatique connecté à un autre système informatique ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique. **Article 7 de la CITO** **Infractions d'interception illégale** L'interception intentionnelle et sans droit, par tous moyens techniques, de données et l'interruption de la transmission ou la réception de données informatiques		**Analyse juridique** Cette infraction est essentielle pour poursuivre en justice des transmissions non publiques de données informatisées en direction ou en provenance d'un système informatique et qui pourraient avoir été interceptées de façon illégale afin d'obtenir des informations concernant la localisation d'une personne (pour cibler cette dernière par exemple).[447] La Tunisie a adhéré à la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son Protocole additionnel n°181 sur les autorités de contrôle et les flux transfrontières de données.[448] Cette législation protégera les personnes physiques vis-à-vis des abus susceptibles d'accompagner la collecte et le traitement des données personnelles, tel que le prévoit la Convention. Même si ce n'est pas explicite, cela comprend les données obtenues dans le cadre d'une interception illégale. En outre, la Convention prévoit des garanties concernant la collecte et le traitement de données personnelles, et interdit le traitement de données *«sensibles»* concernant la race, les opinions politiques, la santé, la religion, l'orientation sexuelle, le casier judiciaire, etc., si des garanties légales appropriées n'ont pas été mises en place. La Convention consacre également le droit d'une personne physique de savoir que des informations la concernant sont stockées et, si nécessaire, d'en exiger la correction. Il est possible d'appliquer des restrictions aux droits prévus dans la Convention, mais uniquement lorsque des intérêts supérieurs (par exemple, la sécurité de l'État, la défense, etc.) sont en jeu. Cela signifie qu'en cas d'interception légale,[449] les données seront collectées et traitées licitement. La Convention imposes également certaines restrictions aux flux transfrontières de données personnelles vers des États dont la législation ne confère pas de protection équivalente.[450]

447. http://www.coe.int/en/web/cybercrime/guidance-notes
448. ibid
449. Loi organique n°2015-26 du 7 août 2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent (article 54) ou loi organique n°2016-61 du 3 août 2016 relative à la prévention et à la lutte contre la traite des personnes (article 32)
450. Résumé de la Convention n°108 consultable à l'adresse suivante: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
		Analyse des écarts **Recommandation:** Utiliser la terminologie de l'article 3 de la CB et de l'article 6 de l'HIPCAR comme guide (la terminologie de l'article 7 de la CITO convient également même s'il n'existe pas de définition des «*données informatiques*»).
Article 4 de la CB[451] **Atteinte à l'intégrité des données** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux. **Article 7 de l'HIPCAR – Atteinte à l'intégrité des données** 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, réalise intentionnellement l'un des actes suivants: • endommagement ou détérioration de données informatiques; • suppression de données informatiques; • altération des données informatiques; • rend les données informatiques dénuées de sens, inutiles ou inopérantes;	**Code pénal** **Article 199 bis**: La peine est élevée à deux ans d'emprisonnement et l'amende à deux mille dinars lorsqu'il en résulte, même sans intention, une altération ou la destruction du fonctionnement des données existantes dans le système indiqué. Est puni d'un emprisonnement de cinq ans et d'une amende de cinq mille dinars, quiconque aura frauduleusement introduit des données dans un système de traitement automatisé de nature à altérer les données que contient le programme ou son mode de traitement ou de transmission. La peine est portée au double lorsque l'acte susvisé est commis par une personne à l'occasion de l'exercice de son activité professionnelle.	**Analyse juridique** L'utilisation du terme «*frauduleusement*» n'est pas cohérente (rentre en conflit) avec la règle posée par l'article 4, paragraphe 1, de la CB, c'est-à-dire «*(...) le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques*» qui n'exige pas la preuve de l'existence d'une fraude. Cela signifie que la conduite constitutive d'un délit d'atteinte à l'intégrité des données au sens de l'article 4, paragraphe 1, de la CB, ne serait pas criminalisée en vertu de l'article 199 bis du Code pénal tunisien. Ledit article n'englobe pas la suppression de données informatisées. **Analyse des écarts** **Recommandation:** Utiliser l'article 4 de la CB ou l'article 7 de l'HIPCAR comme guide pour modifier/remplacer la législation nationale.

451. Article 29, paragraphe 1, sous e) à sous f), de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
• obstruction, interruption ou interférence avec l'utilisation légale des données informatiques; • obstruction, interruption ou interférence avec toute personne dans l'utilisation légale de données informatiques; ou • refus de l'accès aux données informatiques à toute personne ayant le droit d'y accéder, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Article 8 de la CITO** **Atteinte à l'intégrité de données** 1. Le fait de supprimer, d'effacer, d'entraver, de modifier ou de retenir intentionnellement et sans droit des données informatiques. 2. Une partie peut exiger que l'incrimination des actes prévus à l'alinéa 1er du présent article entraîne de sérieux dommages.		
Article 5 de la CB[452] **Atteinte à l'intégrité du système** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, 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.		**Analyse juridique** Cette infraction contribuerait à lutter contre les logiciels malveillants qui perturbent le fonctionnement d'un ordinateur (des vers informatiques par exemple) ou les sous-groupes de logiciels malveillants (comme les virus informatiques). Il s'agit de programmes informatiques auto-répliquants qui nuisent au réseau en lançant de multiples processus de transfert de données. Ils peuvent affecter les systèmes informatiques en entravant leur bon fonctionnement, en utilisant des ressources du système pour se reproduire sur Internet ou en générant du trafic sur le réseau susceptible d'interrompre la disponibilité de certains services (tels que des sites Internet).

452. Article 29, paragraphe 1, sous d), de la CUA, sans équivalent dans la CITO

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 9 de l'HIPCAR – Atteinte à l'intégrité du système 1. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime: • entrave ou porte atteinte au fonctionnement d'un système informatique; ou • entrave ou porte atteinte à une personne qui utilise ou opère légalement un système informatique, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, entrave ou porte atteinte intentionnellement à un système informatique exclusivement réservé aux opérations des infrastructures critiques ou, s'il n'est pas exclusivement réservé aux opérations des infrastructures critiques, un système utilisé dans les opérations des infrastructures critiques et que cela affecte cette utilisation ou affecte lesdites infrastructures, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Article 199 bis** (...) quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données.	L'article 199 bis du Code pénal tunisien ne fait pas référence au fait que l'intention d'altérer ou de détruire doit être «*sans droit*». En outre, l'article 199 bis ne fait pas référence au fait «d'entraver ou de fausser intentionnellement» «par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques». La mention de ces actes permettrait de garantir que l'infraction décrit la signification de l'entrave ou de la distorsion. **Analyse des écarts** **Recommandation:** Utiliser la terminologie employée par la CB, dans son article 5, ou celle de l'article 9 de l'HIPCAR, en ajoutant l'expression *«altère ou détruit intentionnellement sans droit»* et les actes constitués par *«l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques».* Examiner également la question de savoir si la prévention et la poursuite en justice des attaques à l'encontre des infrastructures critiques nécessitent l'instauration d'une autre infraction séparée ou aggravée, comme lorsque le fonctionnement d'un système informatique est entravé à des fins terroristes (p. ex. l'entrave à un système stockant des registres boursiers pourrait les rendre inexacts, ou entraver le fonctionnement des infrastructures critiques)[453] (voir l'article 9, paragraphe 2, de l'HIPCAR, pour une suggestion de rédaction).

453. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 6 de la CB[454] **Abus de dispositifs** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit: a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition: i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus; ii. 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'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5, et b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.	**Pas d'équivalent**	**Analyse juridique** Cette infraction permettra de poursuivre en justice la production, la vente ou l'acquisition à des fins d'utilisation, ainsi que l'importation ou la distribution de codes d'accès et d'autres données informatiques utilisées pour commettre des cybercrimes. C'est ainsi, par exemple, que l'on peut accéder à un système informatique pour faciliter une attaque terroriste, en perturbant le réseau de distribution électrique d'un pays. Cette infraction permettra de poursuivre en justice la production, la vente ou l'acquisition à des fins d'utilisation, ainsi que l'importation ou la distribution de codes d'accès et d'autres données informatiques utilisées pour commettre des cybercrimes. Ces éléments apparaissent souvent lors de poursuites contre des logiciels malveillants. L'article9 de la CITO n'utilise pas l'expression *«sans droit»*. La terminologie utilisée dans la CB et l'HIPCAR est donc privilégiée. L'infraction tiendra également compte des dispositifs qui présentent un intérêt légitime tout en étant utilisés à des fins criminelles *(«double usage»)*. Cela inclura la terminologie *«principalement adapté»* utilisée dans la CB. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 6 de la CB ou de l'article 10 de l'HIPCAR comme guide pour la législation nationale. Il convient de noter que l'HIPCAR prévoit la possibilité de répertorier les dispositifs dans une annexe, si nécessaire. Une telle disposition pourrait s'avérer restrictive et exiger des mises à jour au fur et à mesure des progrès technologiques. La loi nationale devrait prévoir une excuse raisonnable, afin que les autorités chargées de l'application de la loi puissent utiliser des dispositifs à des fins de techniques d'enquête particulières (la terminologie de l'article 6, paragraphe 2 de la CB ou de l'article 10, paragraphe 2, de l'HIPCAR pourrait être utilisée comme guide).

454. Article 9 de la CITO et article 29, paragraphe 1, sous h), de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique. 3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article. **Article 10 de l'HIPCAR – Dispositifs illégaux** 1. Une personne commet une infraction si: a. sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, elle produit, vend, obtient pour utilisation, importe, exporte, distribue ou rend autrement disponible: i. un dispositif, notamment un programme informatique, conçu ou adapté pour commettre l'une des infractions définies par d'autres dispositions du Titre II de la présente loi; ou		

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
ii. un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'il soit utilisé par quiconque pour commettre une infraction définie par d'autres dispositions du Titre II de la présente loi; ou b. cette personne a en sa possession un élément mentionné à l'alinéa (i) ou (ii) avec l'intention qu'il soit utilisé par un tiers pour commettre une infraction telle que définie par d'autres dispositions du Titre II de la présente loi, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Cette disposition ne saurait être interprétée comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, ou la possession mentionnées au paragraphe 1 n'ont pas pour but de commettre une infraction établie conformément aux autres dispositions du Titre II de la présente loi, comme dans le cas de tests autorisés ou de protection d'un système informatique. 3. Un pays peut décider de ne pas criminaliser les dispositifs illégaux ou de limiter la criminalisation aux dispositifs énumérés dans un tableau.		

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 7 de la CB **Falsification informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la 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. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée. **Article 11 de l'HIPCAR – Falsification informatique** 1. Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, introduit, altère, efface ou supprime des données informatiques de manière intentionnelle et engendre ainsi des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques, que ces données soient directement lisibles et intelligibles ou non, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Article 172** Est puni de l'emprisonnement à vie et d'une amende de mille dinars, tout fonctionnaire public ou assimilé, tout notaire qui dans l'exercice de ses fonctions, commet un faux susceptible de causer un dommage public ou privé, et ce, dans les cas suivants: • en fabriquant, en tout ou partie, un document ou un acte mensonger, soit en altérant ou en dénaturant un document original par quelque moyen que ce soit, soit en apposant un sceau contrefait ou une signature, soit en attestant faussement l'identité ou l'état des personnes. • en fabriquant un document mensonger ou en dénaturant sciemment la vérité par quelque moyen que ce soit dans tout support, qu'il soit matériel ou immatériel, d'un document informatique ou électronique, d'un microfilm et d'une microfiche dont l'objet est la preuve d'un droit ou d'un fait générateur d'effets juridiques.	**Analyse juridique** L'infraction nationale concerne uniquement les fonctionnaires ou un notaire. L'incorporation de l'article 7 de la CB est conseillée pour lutter contre ce délit qui peut comprendre le hameçonnage et le harponnage. La terminologie propre à une fraude informatique doit être employée. Par exemple, les *«données informatiques»* (telles que celles utilisées dans les passeports électroniques par exemple) peuvent être introduites, altérées, effacées ou supprimées dans l'intention que des données non authentiques soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.[455] La terminologie employée dans la législation nationale est floue. Elle ne renvoie à aucune intention malhonnête et requiert une certaine forme de «*dommage*» sans définir précisément ce préjudice. C'est également le cas dans l'article10 de la CITO. Il convient dès lors de préférer la terminologie de l'article7 de la CB et de l'article11 de l'HIPCAR. L'article 11, paragraphe 2, de l'HIPCAR considère aussi l'envoi de plusieurs messages électroniques comme un délit aggravé. La terminologie utilisée à l'article 10 de la CITO ne fait référence à aucune intention malhonnête et requiert qu'un préjudice soit causé. La terminologie utilisée dans la CB et l'HIPCAR doit être privilégiée car elle ne requiert pas de préjudice. La CB et l'HIPCAR exigent uniquement la «*prise en compte*» des «*données non authentiques*». **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 7 de la CB ou de l'article 11 de l'HIPCAR comme guide pour la législation nationale.

455. http://www.coe.int/en/web/cybercrime/guidance-notes

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Si l'infraction susmentionnée est commise en envoyant des courriers électroniques multiples à partir ou au moyen de systèmes informatiques, la sanction sera une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux. **Article 10 de la CITO** **Infraction de falsification** L'utilisation de systèmes informatiques aux fins de détourner la vérité des données de façon à causer un préjudice et dans l'intention qu'elles soient utilisées comme étant authentiques. **Article 29, paragraphe 2, sous b), de la CUA** (...) 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. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.		*Examiner* si le *dommage* doit constituer un élément du délit (il serait préférable de ne pas utiliser le terme *dommage* car la falsification est commise dès lors que des données non authentiques ont été créées et *prises en compte*. Cela signifie que si un faux lien ou document est envoyé dans le cadre d'une escroquerie de harponnage, le délit est constitué dès que le destinataire le *prend en compte* (c'est-à-dire dès qu'il ouvre le courriel contenant le lien ou la pièce jointe), plutôt que de devoir démontrer qu'il a subi un dommage ou un préjudice.

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 8 de la CB[456] **Fraude informatique** Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de causer un préjudice patrimonial à autrui: a. par toute introduction, altération, effacement ou suppression de données informatiques; b. par 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. **Article 12 de l'HIPCAR – Fraude informatique** Une personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, provoque la perte d'un bien d'un tiers par l'une des manières suivantes: • introduction, altération, effacement ou suppression des données informatiques; • atteinte au fonctionnement d'un système informatique; avec l'intention frauduleuse ou malhonnête d'obtenir, sans droit, un avantage économique pour elle-même ou pour un tiers, est passible d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.	**Code pénal** **Article 199 ter** [...] quiconque aura introduit une modification de quelque nature qu'elle soit sur le contenu de documents informatisés ou électroniques originairement véritable, à condition qu'elle porte un préjudice à autrui.	**Analyse juridique** La législation nationale ne fournit aucune définition des termes *«informatisés»*, *«documents électroniques»* ou *«préjudice»*, ce qui peut être source d'incertitude. L'article 199ter ne fait pas référence à une intention frauduleuse ou délictueuse sans droit: une fraude informatique renvoie à un auteur tentant de tirer un avantage économique pour lui-même ou pour autrui. La conduite frauduleuse sans autorisation visée dans la CITO fait défaut et pourrait créer de l'incertitude. Les termes *«préjudice»*, *«bénéficiaires»* ou *«de façon illicite»* ne sont pas définis dans la CITO, ce qui peut générer une incertitude plus grande et empêcher la criminalisation de la conduite visée. La terminologie de l'article8 de la CB ou de l'article12 de l'HIPCAR est à privilégier. **Analyse des écarts** **Recommandation:** Définir les termes *«informatisés»*, *«documents électroniques»* ou *«préjudice»* et confirmer qu'il existe une intention frauduleuse ou malhonnête sans droit, en utilisant la terminologie de la CB ou de l'HIPCAR.

456. Article 11 de la CITO et article 29, paragraphe 2, sous d), de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 9 de la CB[457] **Infractions se rapportant à la pornographie enfantine** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit: a. la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique; b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique; c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique; d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique; e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques. 2. Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle: a. un mineur se livrant à un comportement sexuellement explicite; b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;	**Code pénal** **Article 226 bis** Est puni de six mois d'emprisonnement et d'une amende de mille dinars quiconque porte publiquement atteinte aux bonnes mœurs ou à la morale publique par le geste ou la parole ou gène intentionnellement autrui d'une façon qui porte atteinte à la pudeur. Est passible des mêmes peines prévues au paragraphe précédent, quiconque attire publiquement l'attention sur une occasion de commettre la débauche, par des écrits, des enregistrements, des messages audio ou visuels, électroniques ou optiques. **Loi organique n°2016-61, du 3août2016, relative à la prévention et la lutte contre la traite des personnes.** **Article 1** La présente loi vise à prévenir toutes formes d'exploitation auxquelles pourraient être exposées les personnes, notamment, les femmes et les enfants, à lutter contre leur traite, en réprimer les auteurs et protéger et assister les victimes. Elle vise également à promouvoir la coordination nationale et la coopération internationale dans le domaine de la lutte contre la traite des personnes dans le cadre des conventions internationales, régionales et bilatérales ratifiées par la République Tunisienne.	**Analyse juridique** L'article9 de la CB et l'article13 de l'HIPCAR protègent les enfants en érigeant en infraction pénale la diffusion, la transmission, la mise à disposition, la proposition, la production et la possession d'images indécentes représentant des enfants. L'article226bis ne fait pas référence aux images indécentes représentant des enfants. La loi organique n°2016-61 du 3août2016 relative à la prévention et la lutte contre la traite des personnes ne fait pas spécifiquement référence à la pornographie enfantine, mais davantage à la prostitution des enfants et leur exploitation au travers de scènes pornographiques. Cela signifie que l'infraction concernerait les personnes impliquées dans la prostitution d'enfants victimes de traite dans le but d'obtenir des images indécentes. L'expression «L'obtention d'avantages de quelque nature que ce soit» n'est pas définie. **Analyse des écarts** **Recommandation:** L'article 9 de la CB et l'article 13 de l'HIPCAR devraient être utilisés comme précédent pour la législation nationale.

457. Article 12 de la CITO et article 29, paragraphe 3, sous a) à sous d), de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite. 3. Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans. 4. Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e., et 2, alinéas b. et c. **Article 13 de l'HIPCAR – Pédopornographie ou pornographie infantile** 1. Une personne qui, de manière intentionnelle et sans motif ou justification légitime: • produit de la pornographie mettant en scène des enfants à des fins de diffusion par l'intermédiaire d'un système informatique; • offre ou met à disposition, via un système informatique, des contenus pédopornographiques; • diffuse ou transmet via un système informatique des contenus pédopornographiques; • se procure et/ou obtient des contenus pédopornographiques pour elle même ou pour un tiers, via un système informatique; • possède des contenus pédopornographiques sur un système informatique ou un moyen de stockage des données informatiques; ou • obtient, en connaissance de cause, l'accès, via les technologies de l'information et de la communication, à des contenus pédopornographiques,	Art. 2 - On entend au sens de la présente loi, par les termes suivants: 5 ..... Exploitation économique ou sexuelle des enfants dans le cadre de leur emploi. 6 ..... 7. Exploitation sexuelle: L'obtention d'avantages de quelque nature que ce soit en livrant une personne à la prostitution ou tout autre type de services sexuels notamment, son exploitation dans des scènes pornographiques, à travers la production ou la détention ou la distribution, par quelconque moyen, de scènes ou matériels pornographiques.	

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Si la personne établit que les contenus pornographiques servent uniquement à des fins de répression, cela constitue une décharge face à une accusation formulée au titre des paragraphes (1)(b) à (1)f). 3. Un pays peut ne pas criminaliser le comportement décrit à l'article 13, paragraphe 1, sous d) et f).		
Article10 de la CB [458] **Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.	**La loi n°2009-33 du 23juin2009, modifiant et complétant la loi n°94-36 du 24février1994 relative à la propriété littéraire et artistique** [459]	**Analyse juridique** Les autorités chargées de l'application de la loi utilisent au niveau international les infractions relatives à la violation des droits d'auteur numériques comme conduite criminelle pour enquêter et lancer des poursuites contre plusieurs formes de cybercriminalité (les crimes tels que le hameçonnage, la fraude électronique, la falsification électronique, les sites Internet frauduleux et le vol/la violation de données). L'une des infractions sous-jacentes dans de nombreux dossiers semble être la violation des droits d'auteur numériques. La cyberattaque de Sony[460] constitue l'un des exemples récents où les infractions et les procédures associés à la cybercriminalité, au vol de données/à l'espionnage industriel et la violation des droits d'auteur se complètent mutuellement. La loi n°2009-33 du 23juin2009, modifiant et complétant la loi n°94-36 du 24février1994 protégera l'innovation des entreprises et des citoyens du 21è siècle.

458. Article 17 de la CITO sans équivalent dans la CUA
459. Texte intégral en anglais: http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2009/2009G/052/Tg2009331.pdf ou http://www.jurisitetunisie.com/tunisie/codes/prop_int/prop_int1000.html
460. https://en.wikipedia.org/wiki/Sony_Pictures_hack

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. 3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.		

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 17 CITO - Infractions relatives à la violation des droits d'auteur et des droits connexes La violation des droits tels que définis dans la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel et la violation des droits connexes afférents aux droits d'auteur tels que définis par la loi de l'État partie, lorsque le fait commis est intentionnel et n'est pas commis pour un usage personnel.		
Article 11 de la CB[461] **Tentative et complicité** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise. 2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.	**Pas d'équivalent**	**Analyse juridique** La prise en compte des actes de tentative et de complicité d'autrui en vue de la commission d'infractions s'avère essentielle pour poursuivre en justice ceux qui auraient pu aider ou auraient encouragé la perpétration d'actes relevant de la cybercriminalité. L'article 19 de la CITO prévoit aussi la tentative. **Analyse des écarts** **Recommandation:** Utiliser l'article 11 de la CB et l'article 19 de la CITO (sans référence à la tentative) comme guide pour la législation nationale.

461. Article 29, paragraphe 2, sous f), de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 19 de la CITO - Tentative et complicité dans la perpétration des infractions 1. La complicité dans la perpétration de toute infraction prévue au présent chapitre avec l'existence de l'intention de commettre l'infraction selon la loi de l'État partie. 2. La tentative de commettre les infractions prévues au chapitre 2 de la présente convention. 3. Chaque État partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.		
Article 12 de la CB[462] **Responsabilité des personnes morales** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé: a. sur un pouvoir de représentation de la personne morale; b. sur une autorité pour prendre des décisions au nom de la personne morale; c. sur une autorité pour exercer un contrôle au sein de la personne morale.	**Pas d'équivalent**	**Analyse juridique** Cette disposition s'avère essentielle pour que la responsabilité pénale des personnes morales (par exemple, les sociétés commerciales) puisse être engagée. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 12 de la CB comme guide pour la législation nationale.

462. Article 20 de la CITO et article 30, paragraphe 2, de la CUA

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité. 3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative. 4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.		

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques **Article 3[463] – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe. 2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. 3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.	**Loi organique n°2015-26, du 7août2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent.** **Article 14** Est coupable d'infraction terroriste quiconque commet l'un des actes suivants: Premièrement:…… Septièmement: causer des dommages aux propriétés publiques ou privées, aux ressources vitales, aux infrastructures, aux moyens de transport ou de communication, aux systèmes informatiques ou aux services publics, Huitièmement: accusation d'apostasie ou en faire appel, ou inciter à la haine, à l'animosité entre les races, les doctrines et les religions ou en faire l'apologie.	**Analyse juridique** L'article14 de la législation nationale ne fait pas spécifiquement référence à la diffusion par l'intermédiaire d'un système informatique. L'article 3, paragraphe 1, sous e), de la CUA inclut la création et le téléchargement d'éléments racistes et xénophobes par le biais d'un système informatique, plutôt que leur simple diffusion ou mise à disposition (mais sans inclure l'intention ou «sans droit»). La terminologie utilisée par la CB devrait être privilégiée. **Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 3 de la CB et du Protocole additionnel comme suggestion de précédent pour la législation nationale.

463. Article 29, paragraphe 3, sous e), de la CUA sans équivalent dans la CITO

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Protocole additionnel **Article4[464] – Menace avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) 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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 4 de la CB et du Protocole additionnel comme guide pour la législation nationale.
Protocole additionnel **Article 5[465] - Insulte avec une motivation raciste et xénophobe** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: l'insulte en public, par le biais d'un système informatique, (i) d'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 dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 5 de la CB et du Protocole additionnel comme guide pour la législation nationale.

464. Article 29, paragraphe 3, sous f), de la CUA sans équivalent dans la CITO
465. Article 29, paragraphe 3, sous g), de la CUA sans équivalent dans la CITO

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Protocole additionnel **Article 6[466] - Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité** 1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants: la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Utiliser la terminologie de l'article 6 de la CB et du Protocole additionnel comme guide pour la législation nationale.

466. Article 29, paragraphe 3, sous h), de la CUA sans équivalent dans la CITO

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
2. Une Partie peut: a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments; b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.		
Infractions additionnelles à revoir		
Infractions liées à l'identité **Article 14 de l'HIPCAR** Une personne qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise, sans motif ou justification légitime, un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un crime ou dans le cadre d'une telle activité, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. **Divulgation des détails d'une enquête**		**Analyse juridique** Cette infraction englobe la phase de préparation d'un délit de tromperie lié à l'identité. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Article 16 de l'HIPCAR Un fournisseur de services Internet qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle: • le fait qu'une injonction ait été émise; • toute action réalisée aux termes de l'injonction; ou • toute donnée collectée ou enregistrée aux termes de l'injonction, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne les violations de données et la divulgation d'informations sensibles susceptibles d'avoir des répercussions sur les enquêtes pénales. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.
Refus d'autoriser l'assistance **Article 17 de l'HIPCAR** 1. Une personne autre que le suspect qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, refuse intentionnellement d'autoriser une personne ou d'assister celle-ci, suite à une injonction telle que spécifiée aux articles 20 à 22467 commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou d'une amende maximale de [montant], ou les deux. 2. Un pays peut décider de ne pas criminaliser le refus d'autoriser l'assistance si d'autres recours efficaces existent.		**Analyse juridique** Cette infraction concerne les personnes qui ont connaissance d'éléments de preuve pertinents et refusent de coopérer. Souvent, les autorités chargées de l'application de la loi dépendent de ces personnes pour obtenir des éléments de preuve dans le cadre des enquêtes en matière de cybercriminalité. Le refus de fournir des mots de passe ou des codes d'accès à des dispositifs ou des données crypté(e)s (à savoir, *«des informations protégées par des clés de chiffrement»)* constitue une infraction séparée (l'article 53 de la loi britannique qui régit les pouvoirs d'enquête intitulée UK Regulation of Investigatory Powers Act 2000 (RIPA) [468] prévoit un délit pénal pour les personnes qui ne se conforment pas à l'article 49 de la RIPA Notice to disclose the «key» (Injonction de divulgation de la *«clé»*)). **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.

467. Perquisition et saisie, assistance et injonctions de produire
468. http://www.legislation.gov.uk/ukpga/2000/23/section/53

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Harcèlement au moyen de communications électroniques **Article 18 de l'HIPCAR** Toute personne qui, sans motif ou justification légitime ou en se prévalant à tort d'un motif ou d'une justification légitime, initie une communication électronique dans l'intention de contraindre, intimider, harceler ou provoquer une importante détresse émotionnelle chez une personne, en utilisant un système informatique pour encourager un comportement grave, répété et hostile, commet une infraction passible, en cas de condamnation, d'une peine de prison maximale de [durée] ou une amende maximale de [montant], ou les deux.		**Analyse juridique** Cette infraction sanctionne pénalement ceux qui harcèlent autrui en ligne (certains pays prévoient des sanctions pour les infractions liées au harcèlement non informatique) et cette sanction est recommandée pour les délits commis en ligne. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée.
Manipulation psychologique des enfants en ligne **Article 248e du Code pénal des Pays-Bas** Toute personne qui, au moyen d'un système de traitement automatisé des données ou en faisant usage d'un service de communications, propose une rencontre à une personne dont on sait ou, doit raisonnablement soupçonner qu'elle n'a pas encore atteint l'âge de seize ans, dans l'intention de commettre des actes contraires aux bonnes mœurs avec cette personne ou de confectionner une image de comportement sexuel dans lequel la personne est impliquée si elle entreprend un acte quelconque visant la réalisation de cette rencontre, est punie d'une peine d'emprisonnement de deux ans ou plus ou d'une amende de quatrième catégorie.		**Analyse juridique** Pour que l'infraction néerlandaise soit établie, une rencontre à des fins sexuelles est exigée, avec l'existence d'éléments de preuve d'échanges en ligne avec une intention sexuelle. Il doit également être prouvé qu'une rencontre a été prévue (à savoir, la date et le lieu). La disposition canadienne vise à éviter le leurre d'enfants par des adultes prédateurs en ligne. Cette infraction n'exige pas la perpétration d'une agression sexuelle. Cela implique que l'accusé ne doit pas nécessairement avoir rencontré la victime en personne. L'infraction est commise avant que toute mesure n'ait été adoptée en vue de perpétrer le délit en tant que tel. **Analyse des écarts** **Recommandation:** L'inclusion dans la législation nationale est conseillée en vue de criminaliser cette conduite préparatoire avant que l'infraction sexuelle soit commise.

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Code criminel canadien **Article 172.1 - Leurre** 1. Commet une infraction quiconque communique par un moyen de télécommunication avec: a. une personne âgée de moins de dix-huit ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée au paragraphe 153(1), aux articles 155, 163.1, 170 ou 171 ou aux paragraphes 212(1), (2), (2.1) ou (4); b. une personne âgée de moins de seize ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée aux articles 151 ou 152, aux paragraphes 160(3) ou 173(2) ou aux articles 271, 272, 273 ou 280; c. c. une personne âgée de moins de quatorze ans ou qu'il croit telle, en vue de faciliter la perpétration à son égard d'une infraction visée à l'article 281. Peine 2. Quiconque commet l'infraction visée au paragraphe (1) est coupable: a. soit d'un acte criminel passible d'un emprisonnement maximal de dixans, la peine minimale étant de un an; b. soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire et passible d'un emprisonnement maximal de dix-huit mois, la peine minimale étant de quatre-vingt-dixjours.		

Infractions		
Convention de Budapest sur la cybercriminalité («CB»)	**Législation nationale**	**Commentaires**
Présomption 3. La preuve que la personne visée aux alinéas (1)a), b) ou c) a été présentée à l'accusé comme ayant moins de dix-huit, seize ou quatorze ans, selon le cas, constitue, sauf preuve contraire, la preuve que l'accusé la croyait telle. Moyen de défense 4. Le fait pour l'accusé de croire que la personne visée aux alinéas (1)a), b) ou c) était âgée d'au moins dix-huit, seize ou quatorze ans, selon le cas, ne constitue un moyen de défense contre une accusation fondée sur le paragraphe (1) que s'il a pris des mesures raisonnables pour s'assurer de l'âge de la personne.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 19 de la CB[469] **Perquisition et saisie de données informatiques stockées** 1. 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.	**Pas d'équivalent**	**Analyse juridique** Il s'agit du pouvoir d'enquête le plus essentiel, et il devrait faire référence à l'accès plutôt qu'à la perquisition. Dans le Rapport explicatif de la CB, le terme *«Perquisitionner»* signifie *«chercher, lire, inspecter ou examiner des données»*. Il inclut aussi les notions de recherche de données et d'examen des données. Le terme *«accéder»*, quant à lui, a un sens neutre et est plus fidèle à la terminologie informatique (également utilisée aux articles 26 et 27 de la CITO).[470]

469. Article 3 de la CUA
470. Paragraphe191, page33 du Rapport explicatif de la CB

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. *Ces mesures incluent les prérogatives suivantes:* a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique;		**Analyse des écarts** **Recommandation:** La législation nationale pourrait intégrer la terminologie pertinente de la CB et de l'HIPCAR, afin d'inclure les définitions des expressions *système informatique*[471] et *données informatiques,*[472] et faire référence de manière uniforme au terme *accès*. Le terme «saisir» devrait être défini, de façon à garantir l'intégrité et pour les procédures spécifiques (article 3, paragraphe 16, de l'HIPCAR. ««Saisir» signifie: • *activer tout système informatique et moyen de stockage des données informatiques sur site;* • *faire et conserver une copie des données informatiques, en utilisant notamment l'équipement sur site;* • *maintenir l'intégrité de ces données informatiques stockées;* • *rendre inaccessible ou retirer les données informatiques du système informatique accédé;* • *sortir sur imprimante les données informatiques; ou* • *saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques».* L'article 21 de l'HIPCAR prévoit la législation nécessaire afin de garantir qu'une assistance sera apportée par ceux qui disposent de connaissances spécialisées concernant le lieu où se trouvent les éléments de preuve pertinents (il pourrait donc être utilisé comme guide). L'article 17 de l'HIPCAR aborde également les infractions dans le cadre desquelles l'assistance a été refusée sans excuse légitime.

471. Voir l'article 1, sous a), de la CB: «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 » **ou** l'article 3, paragraphe 5, de l'HIPCAR: «un dispositif ou un groupe de dispositifs interconnectés ou reliés, y compris Internet, qui, conformément à un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions».

472. Voir l'article 1, sous b), de la CB: «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» **ou** l'article3, paragraphe6, de l'HIPCAR: «Données informatiques désigne toute représentation de faits, de concepts, d'informations (textes, sons ou images), de codes ou d'instructions lisibles par une machine, dans un format permettant d'être traité par un système informatique, notamment un programme pouvant faire exécuter une fonction à un système informatique».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2. 5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et15. **Article 20 de l'HIPCAR – Perquisition et saisie** 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment], qu'il existe de bonnes raisons [de soupçonner] [de croire] qu'il peut exister dans un lieu un objet ou des données informatiques: • pouvant être considérés comme importants pour servir de preuve à une infraction; ou • ayant été obtenus par une personne suite à une infraction,		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
le magistrat [peut] [doit] émettre un mandat autorisant un agent [de répression] [de police], avec toute l'assistance pouvant être nécessaire, d'entrer dans le lieu pour perquisitionner et saisir l'objet ou les données informatiques en question, notamment perquisitionner ou accéder de manière similaire à: i. un système informatique ou une partie d'un tel système et aux données informatiques qui y sont stockées; et ii. un moyen de stockage des données informatiques dans lequel les données informatiques peuvent être stockées sur le territoire du pays. 2. Si un agent de [répression] [police] qui entreprend une perquisition sur la base de l'Article 20(1) a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, l'agent sera en mesure d'étendre rapidement la perquisition ou l'accès similaire à l'autre système. 3. Un agent de [répression] [police] qui entreprend une perquisition a le pouvoir de saisir ou d'obtenir de façon similaire les données informatiques auxquelles il a accédé en vertu du paragraphe 1 ou 2.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 21 de l'HIPCAR – Assistance Toute personne n'étant pas suspectée d'un crime, mais qui a connaissance du fonctionnement du système informatique ou des mesures appliquées pour protéger les données informatiques qui s'y trouvent et qui font l'objet d'une perquisition aux termes de l'Article 20 doit permettre et assister la personne autorisée à effectuer la perquisition, si cela est requis et exigé de manière raisonnable, à: • fournir des informations permettant de prendre les mesures mentionnées à l'Article 20; • accéder et utiliser un système informatique ou un moyen de stockage de données informatiques pour effectuer une perquisition sur toutes les données informatiques disponibles ou sur le système; • obtenir et copier ces données informatiques; • utiliser l'équipement pour faire des copies; et • obtenir un résultat intelligible d'un système informatique dans un format simple admissible à des fins de procédures légales. **Article 26 de la CITO - Perquisition de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder à: a. un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui sont stockées dans ou sur celui-ci;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
b. un milieu ou un support de stockage informatique dans, ou sur lequel sont stockées des données informatiques. 2. Chaque État partie adopte les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à perquisitionner ou à accéder à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe (1-a) s'il y a des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci, situé sur son territoire, et que ces données sont légalement accessibles ou disponibles dans le système initial, la perquisition et l'accès peuvent être étendus à l'autre système. **Article 27 de la CITO - Saisie de données stockées** 1. Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à saisir et à sécuriser les données informatiques pour lesquelles l'accès a été réalisé en application du paragraphe (1-) de l'article 26 de la présente convention. Ces mesures incluent les prérogatives suivantes: a. saisir et sécuriser 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;		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. enlever ou rendre inaccessibles ces données du système informatique consulté. 2. Chaque État partie adopte les mesures nécessaires pour permettre aux autorités compétentes d'ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les systèmes informatiques aux fins de fournir les informations nécessaires pour permettre l'application des mesures visées par les paragraphes2 et3 de l'article26 de la présente Convention.		
Article 16 de la CB[473] **Conservation rapide de données informatiques stockées** 1. 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.	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir de procédure est important pour garantir la préservation des données vulnérables par rapport à la suppression ou la perte.

473. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour 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. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles14 et 15.		**Analyse des écarts** **Recommandation:** Ce pouvoir rapide d'obtention de DBA, de métadonnées et de contenus transactionnels et stockés s'avère essentiel dans le cadre des enquêtes relevant de la cybercriminalité, afin de s'assurer de la disponibilité des éléments de preuve à des fins de perquisition, d'accès, de saisie et d'analyse. La terminologie utilisée à l'article 16 de la CB, à l'article 23 de l'HIPCAR et à l'article 23 de la CITO pourrait être utilisée. La législation nationale nécessitera la définition suffisante des termes *«données relatives aux abonnés ou DBA»*,[474] *«données de trafic »*[475] et *« Fournisseur de service de communication»*[476] *pour garantir leur préservation.* Il conviendrait de prévoir une durée de conservation raisonnable selon les circonstances et permettre l'extension de la demande dans certaines circonstances exigeantes (la CB et la CITO prévoient 90jours et l'HIPCAR 7jours). L'expérience montre que le délai de 90jours est trop court en matière de cyber-enquêtes et qu'il devrait être plus près des 180 jours avec une possibilité d'extension.

474. Voir l'article 2, paragraphe 9, de la CITO: «*Toutes informations existantes chez le fournisseur de services relatives aux utilisateurs de services à l'exception des informations à travers lesquelles on peut connaître : a. le type de services de communications utilisés, les conditions techniques et la période desdits services; b. l'identité de l'utilisateur, son adresse postale ou géographique ou son téléphone, les renseignements de paiement disponibles sur la base d'un contrat ou d'un arrangement de services ; c. Toutes autres informations sur le site de montage des équipements de communication sur la base d'un contrat de services*».

475. Voir l'article 1, sous d), de la CB: ««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» **ou** l'article 3, paragraphe 18, de l'HIPCAR: «Données relatives au trafic» désigne les données informatiques: a. ayant trait à une communication passant par un système informatique; et b. générées par un système informatique en tant qu'éléments de la chaîne de communication; et c. indiquant l'origine, la destination, l'itinéraire, l'heure, la taille et la durée de la communication ou le type de services sous-jacents».

476. Voir l'article1, sous c), de la CB: «*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*» **ou** l'article2, paragraphe2, de la CITO: «*toute personne physique ou morale, publique ou privée, qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ou qui procède au traitement ou au stockage des informations pour le service de communication ou ses uti*lisateurs».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 23 de l'HIPCAR – Conservation rapide Si un agent [des forces de l'ordre] [de police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne de veiller à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée. **Article 23 de la CITO - Conservation rapide de données stockées dans un système informatique** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir la conservation rapide de données stockées, y compris les données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont susceptibles de perte ou de modification.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque État partie adopte les mesures nécessaires concernant le paragraphe 1-, au moyen d'une injonction ordonnant à une personne de conserver les données spécifiées se trouvant en sa possession ou sous son contrôle, et pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée maximale de 90 jours renouvelable, afin de permettre aux autorités compétentes de procéder aux investigations et recherches. 3. Chaque État partie adopte les mesures nécessaires pour obliger la personne chargée de conserver les données à garder le secret des procédures pendant la durée légale prévue par son droit interne.		
Article 17 de la CB[477] **Conservation et divulgation partielle rapides de données relatives au trafic** 1. 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. pour 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	**Pas d'équivalent**	**Analyse juridique** Ce pouvoir procédural s'avère particulièrement important pour garantir que les FSC mettent à disposition des adresses IP susceptibles de permettre de localiser l'auteur d'un cybercrime. **Analyse des écarts** **Recommandation:** Le pouvoir de conservation rapide et la divulgation des données de trafic devraient être inclus dans la législation, afin de contribuer à l'efficacité des enquêtes en matière de cybercriminalité. La terminologie de l'article 17 de la CB, des articles 23 et 24 de l'HIPCAR et de l'article 24 de la CITO pourrait être utilisée à de tels effets. La définition des expressions «données de trafic» et «Fournisseur de services de communications» sera également nécessaire.[478]

477. Pas d'équivalent dans la CUA
478. Voir les définitions ci-dessus

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 23 de l'HIPCAR – Conservation rapide** Si un agent [des forces de l'ordre] [de police] est convaincu qu'il existe des raisons de croire que les données informatiques raisonnablement nécessaires aux besoins d'une enquête criminelle sont particulièrement susceptibles d'être perdues ou modifiées, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne de veiller à ce que les données spécifiées dans la notification soient conservées pendant une période maximale de sept (7) jours, tel que spécifié dans la notification. Cette période peut être étendue au-delà de sept (7) jours si, sur une demande ex parte, un [juge] [magistrat] autorise une prolongation pour une autre période spécifiée.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 24 de l'HIPCAR – Divulgation partielle des données de trafic Si un agent de [répression] [police] est convaincu que les données stockées dans un système informatique font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il peut, en envoyant une notification écrite à une personne qui contrôle des données informatiques, exiger de cette personne qu'elle divulgue suffisamment de données de trafic associées à une communication spécifique, afin d'identifier: a. les fournisseurs de services Internet; et/ou b. l'itinéraire de la communication. **Article 24 de la CITO - Conservation rapide et divulgation partielle de données relatives au trafic** Chaque État partie s'engage à adopter les mesures nécessaires relatives aux données de trafic pour: 1. veiller à la conservation rapide des données relatives au trafic, sans tenir compte qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; 2. assurer la divulgation rapide aux autorités compétentes prés l'État partie ou à une personne désignée par ces autorités, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par l'État partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 18 de la CB[479] **Injonction de produire** 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: a. à 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 b. à 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. 2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. 3. Aux fins du présent article, 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, et permettant d'établir:	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une disposition essentielle pour la réalisation d'enquêtes efficaces en matière de cybercriminalité, et son absence aura un impact sur les poursuites devant les tribunaux et la coopération internationale. **Analyse des écarts** **Recommandation:** Ce pouvoir essentiel s'avère nécessaire pour s'assurer que les FSC opérant en Tunisie fournissent les DBA, les données de trafic et les informations sur les contenus stockés. La définition des expressions *«données informatiques», «données relatives aux abonnés ou DBA», «données de trafic» et «Fournisseur de services de communication»* sera également nécessaire.[480] *L'*article 25 de la CITO est un modèle et qui contient différentes définitions, notamment pour les expressions *«système informatique»,*[481] *«fournisseur de services»*[482] *et «données relatives aux abonnés ou DBA»*[483]. Il serait souhaitable de pouvoir également définir les expressions «données relatives aux abonnés ou DBA» et «données de trafic», car différents types de preuves pourront être produits par les FSC. En outre, ce pouvoir exigera des personnes et de toutes les autres entités (sociétés commerciales, institutions financières et autres organisations) qui détiennent des données de les remettre aux autorités chargées de l'application de la loi. L'article 18 de la CB et l'article 22 de l'HIPCAR pourraient constituer des guides pour une application uniforme des définitions.

479. Pas d'équivalent dans la CUA
480. Voir les définitions ci-dessus
481. Article 2, paragraphe 1, de la CITO: «*tout moyen matériel ou moral, ou ensemble de dispositifs interconnectés ou non, utilisés pour stocker des informations, les classer, les organiser, les restituer, les traiter, les développer et les échanger suivant des commandes et des instructions qui y sont stockées et ceci comprend toutes les entrées et sorties câblées à elles ou non par un système ou un réseau*».
482. Article2, paragraphe2, de la CITO voir ci-dessus
483. Article 2, paragraphe 3, de la CITO: «*tout ce qui peut être stocké, traité*, émis et transmis au moyen d'*un système informatique, tels que les chiffres, les lettres, les symboles et autres*».

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services. **Article 22 de l'HIPCAR – Injonction de produire** Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent de [répression] [police], que des données informatiques spécifiées, qu'une version imprimée ou que d'autres informations font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle ou d'une procédure pénale, il peut ordonner: • à une personne sur le territoire de [État prenant les dispositions] qui contrôle un système informatique, de produire, à partir du système, des données informatiques spécifiées ou une version imprimée ou une autre forme de sortie intelligible de ces données; ou • à un fournisseur de services Internet en [État prenant les dispositions], de produire des informations sur les personnes qui sont abonnées au service ou qui utilisent autrement ce service.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 CITO - Injonction de produire les informations Chaque État partie s'engage à adopter les mesures qui se révèlent nécessaires pour habiliter les autorités compétentes à ordonner: 1. à toute personne présente sur son territoire de communiquer les données spécifiées, en sa possession, qui sont stockées dans un système informatique ou sur un support de stockage informatique; 2. à tout fournisseur de services offrant des prestations sur le territoire de l'État partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.		
Article 21 de la CB[484] **Interception de données relatives au contenu** 1. 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	**Loi organique n°2016-61, du 3août2016, relative à la prévention et la lutte contre la traite des personnes.** **Article 42** Est puni de cinq ans d'emprisonnement et d'une amende de cinq mille dinars quiconque, en dehors des cas autorisés par la loi, procède intentionnellement à l'interception des communications et des correspondances ou de la surveillance audiovisuelle sans observer les dispositions légales. La tentative est punissable.	**Analyse juridique** Ce pouvoir est déjà prévu dans la législation nationale et des garanties et des exigences/ procédures permettant de contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques en Tunisie s'avèrent nécessaires. La législation nationale ne contient pas de disposition explicite concernant la collecte de données en temps réel. Toutefois, la restriction de l'utilisation de la technique d'interception est rigoureuse. **Analyse des écarts** **Recommandations:** Il conviendrait d'obliger les FSC opérant en Tunisie à coopérer à la collecte en temps réel des contenus. Des garanties devraient par ailleurs être incorporées afin d'assurer que la collecte a lieu selon des modalités légales, raisonnables et proportionnées. Il conviendrait de revoir l'article 29 de la CITO, l'article 21 de la CB et l'article 26 de l'HIPCAR, afin d'en incorporer les termes dans la législation nationale.

484. Pas d'équivalent dans la CUA

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
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. 2. Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.	**Loi organique n°2015-26, du 7août2015, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent.** **Article 64** Est puni de cinq ans d'emprisonnement et d'une amende de cinq mille dinars quiconque, en dehors des cas autorisés par la loi, procède intentionnellement à l'interception des communications et des correspondances ou de la surveillance audiovisuelle sans observer les dispositions légales. La tentative est punissable.	

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 26 de l'HIPCAR – Interception des données relatives au contenu 1. 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que le contenu d'une communication électronique est raisonnablement nécessaire aux besoins d'une enquête criminelle, il [peut] [doit]: • ordonner à un fournisseur de services Internet dont les services sont disponibles en [État prenant les dispositions], en utilisant des moyens techniques, de collecter ou d'enregistrer ou de permettre aux autorités compétentes ou de les assister à collecter ou enregistrer les données de contenu associées à des communications spécifiées transmises par l'intermédiaire d'un système informatique; ou • autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer lesdites données, à l'aide de moyens techniques. 2. Un pays peut décider de ne pas mettre en œuvre l'article 26. **Article 29 de la CITO - Interception de données relatives au contenu** 1. Chaque État partie s'engage à adopter les mesures législatives nécessaires concernant un éventail d'infractions prévues par son droit interne, pour permettre aux autorités compétentes:		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
a. de collecter ou d'enregistrer par l'application de moyens techniques existant sur le territoire de l'État partie, ou b. de prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer en temps réel les données relatives au contenu des communications spécifiques sur son territoire, transmises au moyen d'un système informatique. 2. Lorsque l'État partie, en raison de son système juridique interne, ne peut adopter les mesures énoncées au paragraphe (1- a), il peut adopter d'autres mesures qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel de données relatives au contenu des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire. 3. Chaque État partie adopte les mesures nécessaires pour obliger un fournisseur de services à garder le secret de toute information lors de l'exécution des pouvoirs prévus au présent article.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 20 de la CB[485] **Collecte en temps réel des données relatives au trafic** 1. 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. 2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.	**Pas d'équivalent**	**Analyse juridique** Il n'existe pas de pouvoir de procédure spécifique à la collecte des données de trafic en temps réel. Un seuil plus bas pourrait permettre de collecter les données de trafic en temps réel, ce qui constituerait un outil d'enquête essentiel. Dans certaines situations, le seuil légal supérieur permettant de sécuriser les contenus n'est pas établi par le demandeur, mais un seuil plus bas permettant de sécuriser le trafic pourrait l'être. Une distinction devrait donc être faite entre collecte en temps réel des contenus stockés et collecte des données de trafic. Des garanties et des exigences/procédures permettant de contraindre les FSC à coopérer en vue de la collecte ou de l'enregistrement des données relatives aux contenus en temps réel des communications spécifiques en Tunisie s'avèrent nécessaires. **Analyse des écarts** **Recommandations:** Il conviendrait d'instaurer un pouvoir spécifique permettant la collecte de données de trafic en temps réel et de contraindre les FSC opérant en Tunisie à coopérer à la collecte des contenus en temps réel. Des garanties devraient par ailleurs être incorporées afin d'assurer que la collecte est légale, raisonnable et proportionnée au vu des circonstances. La terminologie utilisée à l'article 28 de la CITO pourrait être envisagée, mais elle ne fait pas référence à la collecte rapide en temps réel. L'article 20 de la CB et l'article 25 de l'HIPCAR devraient être utilisés comme guide pour la législation nationale.

485. Article 31, paragraphe 3, sous e) – Noter que l'article 28 de la CITO fait référence à la collecte rapide, plutôt qu'à la collecte en temps réel

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet. 4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15. **Article 25 de l'HIPCAR - Collecte des données de trafic** 1. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe des motifs raisonnables de [suspecter] [croire] que les données de trafic associées à une communication spécifiée sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] ordonner à une personne qui contrôle lesdites données de: • collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifique; ou • permettre à un agent [des forces de l'ordre] [de police] spécifié de collecter ou enregistrer ces données et l'assister dans cette tâche.		

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Si un [juge] [magistrat] est convaincu, sur la base d'une demande faite par un agent [des forces de l'ordre] [de police], appuyée par [des informations obtenues sous serment] [une déclaration sous serment] qu'il existe de bonnes raisons de [suspecter] [croire] que les données de trafic sont raisonnablement nécessaires aux besoins d'une enquête criminelle, il [peut] [doit] autoriser un agent [des forces de l'ordre] [de police] à collecter ou enregistrer les données de trafic associées à une communication spécifiée durant une période spécifiée à l'aide de moyens techniques. 3. Un pays peut décider de ne pas mettre en œuvre l'article 25.		
		Obligation de divulgation et clés de chiffrement Dans la mesure où les terroristes et les criminels organisés utilisent systématiquement des applications[486] de messagerie cryptée, on pourrait envisager un pouvoir viable permettant d'ordonner la remise des clés pour les mots de passe afin de déverrouiller les dispositifs[487]. **Analyse des écarts** **Recommandation:** Nous ne sommes pas parvenus à déterminer si de tels pouvoirs existaient en Tunisie (mais ce pouvoir permettrait aux autorités chargées de l'application de la loi de contraindre les propriétaires à déverrouiller les dispositifs).

486. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, n°24 (15juin2015): 16-18. Academic Search Premier, EBSCOhost (consulté le 29 février 2016).
487. Pour obtenir un exemple, se reporter à l'article 49 de la loi britannique qui régit les pouvoirs d'enquête intitulée Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procédure		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
		Obligations en matière de conservation des données[488] Ledit pouvoir pourrait permettre aux autorités chargées de l'application de la loi de: 1. retracer et identifier la source d'une communication; 2. identifier la destination d'une communication; 3. identifier la date, l'heure et la durée d'une communication, et 4. identifier le type de communication. La Tunisie ne prévoit pas une telle obligation[489]

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 22 de la CB **Compétence** 1. 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 articles2 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 ressortis-sants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.	**Pas d'équivalent**	**Analyse juridique** En l'absence de champ d'application clairement défini en matière de cyber-crimes, de nature internationale, toute législation sera restreinte. **Analyse des écarts** **Recommandation:** La législation nationale doit garantir que la compétence est définie selon les termes utilisés à l'article 22 de la CB, à l'article 19 de l'HIPCAR ou à l'article 30 de la CITO. En cas de conflit de compétence, il conviendrait de tenir compte des lignes directrices relatives à la détermination de la juridiction compétente pour juger une infraction (voir le document intitulé Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (révisé en 2016)).[490]

488. En 2006, l'UE a publié une directive relative à la conservation des données (les États membres de l'UE devaient stocker les données afférentes aux télécommunications électroniques pendant au moins six mois et tout au plus 24mois, à des fins de recherche, de détection et de poursuite des infractions graves). En 2014, la Cour de justice de l'UE a annulé la directive relative à la conservation des données, estimant qu'elle ne prévoyait pas suffisamment de garanties contre les ingérences dans les droits à la vie privée et à la protection des données. En l'absence de directive valable de l'UE portant sur la conservation des données, les États membres peuvent toujours mettre en place un régime applicable à la conservation des données. Les régimes nationaux sont disponibles à l'adresse suivante: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

489. Examen de la législation type à l'échelle mondiale de l'ICMEC page 40

490. http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à1.d du présent article ou dans une partie quelconque de ces paragraphes. 3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition. 4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne. 5. 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.* **Article 19 de l'HIPCAR – Juridiction** *La présente loi s'applique à tout acte ou omission commis:* • sur le territoire de [État prenant les dispositions]; • sur un bateau ou un avion immatriculé en [État prenant les dispositions]; • par un citoyen de [État prenant les dispositions] en dehors de la juridiction de tout pays ; ou		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
par un citoyen de [État prenant les dispositions] en dehors du territoire de [État prenant les dispositions], si le comportement de la personne constitue également une infraction aux termes de la loi du pays dans lequel ladite infraction est commise. **Article 30 CITO - Compétence** 1. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence à l'égard de toute infraction prévue par le chapitre 2 de la présente convention lorsque l'infraction est commise en tout ou en partie: a. sur le territoire de l'État partie; b. à bord d'un navire battant pavillon de l'État partie; c. à bord d'un aéronef immatriculé selon les lois de l'État partie; d. par l'un des ressortissants de l'État partie, si l'infraction est punissable selon le droit interne du lieu où elle a été commise ou si elle ne relève de la compétence territoriale d'aucun État; e. lorsque l'infraction porte atteinte à l'un des intérêts suprêmes de l'État. 2. Chaque État partie s'engage à adopter les mesures nécessaires pour établir sa compétence sur les infractions prévues par l'article 31 paragraphe 1- de la présente convention dans les cas où l'auteur présumé de l'infraction est présent sur le territoire dudit État partie et ne peut être extradé vers une autre partie au seul titre de sa nationalité, après une demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
3. Lorsque plusieurs États parties revendiquent la compétence judiciaire à l'égard d'une infraction visée dans la présente convention, la priorité sera accordée à la demande de l'État, dont l'infraction a porté atteinte à la sécurité ou aux intérêts, ensuite l'État sur le territoire duquel a été commise l'infraction et après l'État dont la personne réclamée est un ressortissant. Lorsque toutes ces circonstances sont réunies la priorité sera accordée à l'État qui a présenté en premier la demande d'extradition.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 35 de la CB[491] **Réseau 24/7** 1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes: a. apport de conseils techniques; b. conservation des données, conformément aux articles 29 et 30; c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects. 2. a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée. b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.	**Pas d'équivalent**	**Analyse juridique** *Il s'agit d'un mécanisme essentiel pour disposer de capacités d'enquête efficaces en matière de cybercriminalité.* **Analyse des écarts** **Recommandation:** *Cette mesure ne devrait pas exiger l'adoption de législation de mise en œuvre, et sous réserve des ressources, elle devrait être établie en tant que priorité. Les coordonnées de contact devraient être partagées concernant le point de contact unique désigné (SPOC), dans le pays, avec les autorités centrales à l'international et INTERPOL. Il conviendrait d'envisager la rédaction d'un protocole d'entente avec les agences nationales, de façon à ce que le SPOC dispose de l'autorité nécessaire pour entreprendre les actions requises dans le cadre d'une enquête internationale sur la cybercriminalité, en application du droit national et des traités. Le protocole d'entente devrait porter aussi bien sur les demandes entrantes que sur les demandes sortantes, et assurer un processus efficient et efficace.*

491. Article 43 de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 25 de la CB **Principes généraux relatifs à l'entraide** 1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. 2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35. 3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'État requis l'exige. L'État requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.		**Analyse juridique** L'article 25 de la CB permet son utilisation en tant qu'instrument pour faciliter l'entraide.[492] La Tunisie n'est pas partie à la CB, à la CITO ou à la CUA. Cela signifie que la Tunisie n'est partie à aucune convention internationale liée à la cybercriminalité, ce qui entravera les enquêtes internationales dans la mesure où les pouvoirs en matière de procédure n'auront pas de base juridique. Outre plusieurs traités bilatéraux, la Tunisie est également signataire de la CNUCTO.[493] L'article 18 de la CNUCTO constitue donc la base de l'entraide et de la mutualité/réciprocité.[494] Cela signifie qu'en l'absence de législation nationale, il est impossible de formuler des requêtes de conservation rapide des données informatiques stockées, de conservation et divulgation partielle rapides des données relatives au trafic, et de divulgation des données stockées et des données de trafic, ce qui restreint la coopération internationale que la Tunisie peut apporter aux États requérants. Voir l'AnnexeA pour connaître les types de demandes internationales envoyées par la Tunisie.

492. Il n'existe pas de disposition équivalente dans la CUA.
493. Ratifiée le 19 juin 2003
494. L'article 18 de la CNUCTO pourrait constituer la base de l'entraide judiciaire si la définition de la criminalité transnationale organisée est retenue. Il en est de même concernant l'Accord de Riyad sur la coopération judiciaire pour les États l'ayant ratifié).

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale. 5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.		**Analyse des écarts** **Recommandation:** L'adoption d'une législation nationale s'avère nécessaire en matière de conservation rapide des données informatiques stockées et de conservation et divulgation partielle rapides des données relatives au trafic, mais aussi concernant les injonctions de produire. La CB, l'HIPCAR et la CITO peuvent servir de précédents concernant la conservation rapide des données informatiques stockées,[495] la conservation et la divulgation partielle rapides des données relatives au trafic,[496] la divulgation des données stockées[497] et la collecte rapide de données relatives au trafic[498]. Il conviendrait également d'envisager des dispositions applicables à l'interception en temps réel des données de trafic et des contenus[499]. En outre, un cadre est nécessaire en matière de coopération dans le contexte des enquêtes liées à la cybercriminalité, par le biais des conventions multilatérales, notamment l'article 27 de la CB et l'article 32 de la CITO.[500]

495. Article 29 de la CB, article 23 de l'HIPCAR et article 37 de la CITO
496. Article 30 de la CB, articles 23 et 24 de l'HIPCAR et article 38 de la CITO
497. Article 31 de la CB et article 39 de la CITO
498. Article 41 de la CITO
499. Articles 33 et 34 de la CB et articles 25 et 26 de l'HIPCAR
500. Il n'existe pas de dispositions équivalentes à la procédure d'entraide judiciaire dans la CUA

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 34 de la CITO - Procédures relatives aux demandes de coopération et d'assistance mutuelle 1. En l'absence de traité ou de convention d'assistance mutuelle et de coopération reposant sur la législation en vigueur entre l'État partie requérant et requis, les dispositions des paragraphes 2- à 9- du présent article s'appliquent. En cas d'existence de ces traités, lesdits paragraphes ne s'appliquent pas, à moins que les parties concernées ne décident d'appliquer tout ou partie desdites dispositions. 2. a. Chaque État partie désigne une autorité centrale chargée de transmettre les demandes d'assistance ou d'y répondre, de les exécuter ou de les transmettre aux autorités concernées pour exécution; b. les autorités centrales communiquent directement entre elles; c. chaque partie, au moment de la signature ou du dépôt des instruments de ratification, d'acceptation ou d'approbation, prend attache avec le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice et leur communique les noms et adresses, des autorités désignées particulièrement aux fins du présent article;		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
d. le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice établissent et tiennent à jour le registre des autorités centrales désignées par les États parties. Chaque État partie veille en permanence à l'exactitude des données figurant dans le registre. 3. Les demandes d'assistance mutuelle sous le présent article sont exécutées conformément aux procédures spécifiées par l'État partie requérant, sauf lorsqu'elles sont incompatibles avec la loi de l'État partie requis. 4. L'État requis peut surseoir les procédures entreprises quant à la demande si cela risquerait de porter préjudice aux enquêtes pénales conduites par ses autorités. 5. Avant de refuser ou de différer l'assistance, l'État requis doit, après avoir consulté l'État partie requérant, décider s'il peut être fait droit en partie, à la demande, ou sous réserve des conditions qu'il juge nécessaires. 6. L'État partie requis s'engage à informer l'État partie requérant de la suite donnée à l'exécution de la demande, en cas de refus ou d'ajournement, celui-ci doit motiver ce refus ou ajournement, et l'État partie requis doit informer l'État partie requérant des motifs rendant l'exécution de la demande définitivement impossible ou ceux l'ayant retardé de manière significative.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
7. L'État partie requérant peut demander à l'État partie requis de garder confidentiel le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si l'État partie requis ne peut faire droit à cette demande de confidentialité, il doit en informer l'État partie requérant lequel déterminera si la demande doit, néanmoins, être exécutée. 8. a. En cas d'urgence, les demandes d'assistance mutuelle peuvent être adressées directement aux autorités judiciaires de l'État partie requis par leurs homologues de l'État partie requérant. Dans un tel cas, une copie est adressée simultanément de l'autorité centrale de l'État partie requérant à son homologue dans l'État partie requis. b. Des communications et des demandes peuvent être formulées au titre du présent paragraphe par l'intermédiaire d'INTERPOL. c. Lorsqu'une demande a été formulée suivant le paragraphe a- et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité compétente et en informe directement l'État partie requérant. d. Les communications et les demandes effectuées en application du présent paragraphe qui n'incluent pas de mesures coercitives peuvent être transmises directement des autorités compétentes de l'État partie requérant à leurs homologues dans l'État partie requis.		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
e. Chaque État partie peut, au moment de la signature, de la ratification, de l'acceptation de l'approbation ou de l'adhésion, informer le secrétariat général du conseil des ministres arabes de l'intérieur et le secrétariat technique du conseil des ministres arabes de la justice que pour des raisons d'efficacité, les demandes faites suivant ce paragraphe devront être adressées à l'autorité centrale.		
Article 26 de la CB **Information spontanée** 1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.	**Pas d'équivalent**	**Analyse juridique** Il s'agit d'une procédure importante qui permet à un État d'avoir accès à des informations qui aideront un autre État à empêcher la cybercriminalité et à enquêter en la matière. Même si elles sont disponibles entre les États ayant ratifié la CITO (article 33 de la CITO), la Tunisie ne dispose pas de base juridique permettant le partage d'informations avec les États non signataires de la CITO, sauf si une requête officielle est adressée par le biais des canaux d'entraide habituels. L'article 18, paragraphes4 et5, de la CNUCTO, prévoit le partage spontané d'informations dans le cadre des affaires répondant à la définition d'infractions graves, transnationales[501] et impliquant un groupe criminel organisé[502]. Sans répondre à cette définition. Une requête officielle devra être envoyée aux États non signataires de la CITO, en empruntant les canaux de l'entraide habituels. Étant donné l'évolution rapide de la cybercriminalité, il s'agit d'un moyen efficace de coopérer avec d'autres États, et son absence empêche toute collaboration internationale efficace avec les États non signataires de la CITO.

501. Article 3, paragraphe 1, de la CNUCTO
502. Au sens de l'article 2, sous a), de la CNUCTO, l'expression «groupe criminel organisé» désigne «un groupe structuré de trois personnes ou plus existant depuis un certain temps et agissant de concert dans le but de commettre une ou plusieurs infractions graves ou infractions établies conformément à la présente Convention, pour en tirer, directement ou indirectement, un avantage financier ou un autre avantage matériel».

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières. **Article 33 de la CITO - Informations spontanées reçues** 1. Tout État partie peut, dans les limites de son droit interne et sans demande préalable, communiquer à un autre État des informations obtenues dans le cadre de ses enquêtes lorsqu'il estime que cela pourrait aider l'État partie destinataire à engager ou à mener des enquêtes concernant des infractions prévues à la présente convention ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cet État partie. 2. Avant de communiquer de telles informations, l'État partie qui les fournit peut demander à ce qu'elles restent confidentielles. Si l'État partie destinataire ne peut faire droit à cette demande, il doit en informer l'autre État partie, qui devra, à son tour déterminer si les informations en question devraient néanmoins être fournies. Si l'État partie destinataire accepte les informations aux conditions définies, il devra garder les informations entre les parties.		**Analyse des écarts** **Recommandation:** Utiliser l'article 18, paragraphes 4 et 5 de la CNUCTO, comme base pour le partage spontané d'informations relevant du champ d'application de cette dernière (avec des garanties concernant l'utilisation des éléments de preuve ou la divulgation d'informations sensibles à des tiers (notamment un autre État)).[503] Envisager l'adoption d'une législation fondée sur l'article 33 de la CITO ou l'article 26 de la CB.

503. Voir l'article 33, paragraphe 2, de la CITO

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 32 de la CB **Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public** Une Partie peut, sans l'autorisation d'une autre Partie: a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou b. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre État, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.		**Analyse juridique** Ce pouvoir de procédure permet à un État d'obtenir des contenus stockés dans un autre État dans des circonstances limitées. L'article 32, sous b), de la CB et l'article 40 de la CITO constituent une exception au principe de territorialité et permettent un accès transfrontalier unilatéral sans besoin d'entraide, s'il existe un consentement ou si les informations sont accessibles au public. Exemples de recours à ce pouvoir de procédure dans le cadre de l'article 32, sous b), de la CB: le message électronique d'une personne peut être stocké dans un autre État par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données.[504] ou Un individu suspecté de terrorisme est arrêté dans les règles alors que son courrier électronique (révélant probablement des preuves d'un délit) est ouvert sur sa tablette, son smartphone ou un autre dispositif. Si le suspect consent volontairement à ce que la police accède à son compte, et si cette dernière est certaine que les données de la boîte de messagerie se trouvent dans un autre État, elle peut accéder à ces dernières dans le cadre de l'article 32, sous b).

504. Paragraphe294, page53 du Rapport explicatif de la CB

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
Article 27 de l'HIPCAR – Logiciel de criminalistique 1. Si un [juge] [magistrat] est convaincu, sur la base d'[informations obtenues sous serment] [une déclaration sous serment] qu'il existe, dans une enquête relative à une infraction énumérée au paragraphe 7 ci-après, des motifs raisonnables de croire que les preuves essentielles ne peuvent être collectées en utilisant d'autres instruments énumérés au Titre IV, mais qu'elles font l'objet d'une demande raisonnable pour les besoins d'une enquête criminelle, il [peut] [doit], sur demande, autoriser un agent de [répression] [police] à utiliser un logiciel de criminalistique à distance pour effectuer la tâche spécifique exigée pour l'enquête et à l'installer sur le système informatique du suspect afin de recueillir les preuves pertinentes. La demande doit contenir les informations suivantes: • le suspect de l'infraction, si possible avec ses nom et adresse; et • une description du système informatique ciblé; et • une description de la mesure, de l'étendue et de la durée d'utilisation envisagées; • les raisons justifiant la nécessité de l'utilisation.	**Pas d'équivalent**	**Analyse des écarts** **Recommandation:** Prévoir ce pouvoir restreint de collecte unilatérale d'éléments de preuve dans la législation avec des garanties visant à assurer que les contenus seront légalement obtenus auprès de l'utilisateur.[505] La terminologie utilisée peut être celle de l'article 32 de la CB et de l'article 40 de la CITO. L'article 32, sous b), a été vivement critiqué et on pourrait envisager de demander le consentement de l'État dans lequel les données informatiques stockées sont localisées en plus de celui de l'utilisateur. L'article 27 de l'HIPCAR prévoit des logiciels de criminalistique, lesquels pourraient permettre d'accéder à un ordinateur situé dans un autre État. Plusieurs restrictions empêchent l'obtention des éléments de preuve par d'autres moyens. Une décision judiciaire est requise et ne peut s'appliquer qu'à certaines infractions, pendant une durée restreinte (3mois). L'obtention du consentement de l'autre État doit être envisagée lorsque des logiciels criminalistiques sont susceptibles de faire intrusion.

505. Il conviendrait également d'envisager les situations telles que l'absence de disponibilité de l'utilisateur (en cas de décès par exemple) et la possibilité d'obtenir le consentement dans un autre État.

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
2. Durant une telle enquête, il est nécessaire de veiller à ce que les modifications du système informatique du suspect se limitent aux modifications essentielles à l'enquête et que tout changement, si possible, ait lieu à la fin de l'enquête. Durant l'enquête, il est nécessaire de consigner • le moyen technique utilisé ainsi que la date et l'heure de l'application; • l'identification du système informatique et les détails des modifications effectuées durant l'enquête; et • toute information obtenue. • Les informations obtenues en utilisant ce logiciel doivent être protégées contre toute modification, toute suppression non autorisée et tout accès. 3. La durée de l'autorisation mentionnée à l'article 27(1) est limitée à [3mois]. Si les conditions d'autorisation ne sont plus respectées, les actions entreprises doivent immédiatement cesser. 4. L'autorisation d'installer le logiciel inclut l'accès à distance au système informatique du suspect. 5. Si le processus d'installation exige d'accéder physiquement à un endroit, il convient de satisfaire aux exigences de l'article 20. 6. Si nécessaire, un agent de [répression] [police] peut, conformément à l'injonction d'un tribunal émise selon les modalités de l'alinéa (1) ci-dessus, exiger que le tribunal ordonne à un fournisseur de services Internet d'aider au processus d'installation. 7. [Liste des infractions].		

Coopération internationale		
Bonnes pratiques internationales	**Législation nationale**	**Commentaires**
8. Un pays peut décider de ne pas mettre en œuvre l'article27. **Article 40 de la CITO - Accès transfrontière à des données informatiques** Un État partie peut, sans l'autorisation d'un autre État partie: 1. accéder à des données informatiques accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; 2. accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques situées dans un autre État partie s'il obtient le consentement volontaire et légal de la personne légalement autorisée à lui divulguer ces données au moyen du système informatique cité.		

Conclusion

L'analyse juridique et l'analyse des écarts ci-avant montrent que les PPVS doivent adapter et mettre à jour leur législation pour permettre la conduite d'enquêtes efficaces et garantir que leur législation nationale peut répondre aux menaces de cybercriminalité. Le processus législatif peut être lent, ce qui accroît la menace et le préjudice causés par la cybercriminalité. La priorité est de légiférer sur ces infractions lorsqu'aucune infraction n'est prévue dans la législation nationale et de garantir que les autorités chargées de l'application de la loi disposent des outils nécessaires pour enquêter efficacement sur leurs auteurs. La CB, l'HIPCAR et la CITO doivent servir de base pour rédiger et modifier la législation de façon à obtenir une application cohérente parmi l'ensemble des PPVS et permettre une utilisation réciproque par les États membres de l'UE. Cela permettra de garantir une conservation rapide et une collecte en temps réel du contenu et des données de trafic. À titre de priorité immédiate, des points de contact uniques disponibles 24h/24, 7j/7, doivent être mis en place afin de garantir une coopération internationale efficace et proactive.

Les principales recommandations découlant de l'analyse des écarts sont les suivantes:

- **Il est recommandé** d'encourager les PPVS qui ne l'auraient pas déjà fait à signer, ratifier et appliquer la Convention de Budapest et/ou la CITO pour permettre le dépôt de demandes d'EJ en vue de la collecte en temps réel de données de trafic, l'interception de contenus, la présentation d'injonctions de produire et l'échange spontané d'informations.
- **Il est recommandé** à chaque PPVS de désigner des interlocuteurs uniques afin de traiter les demandes d'EJ entrantes et sortantes urgentes et de se tenir à jour des procédures à suivre pour sécuriser les données des FSC par des moyens formels et informels.
- **Il est vivement recommandé** de mettre en place des procédures pour préserver les données afin de permettre l'envoi d'une demande d'EJ; en l'absence d'une telle préservation, les données seront effacées et la demande d'EJ ne pourra pas être exécutée.

Annexe A

Statistiques tunisiennes relatives aux commissions rogatoires

Origine des commissions rogatoires reçues par l'Agence technique des télécommunications tunisienne entre le 16avril2014 et le 10juin2017	
Type	**Nombre**
Unité de recherche et d'investigation de la Garde nationale	836
Centres de la police nationale	1372
Direction de la police judiciaire	454
Sous-division des affaires pénales	271
Justice	223
Direction de la sécurité sociale	65
Direction de la recherche et de l'investigation économique et financière	43
Unité de recherche criminelle sur les crimes terroristes	204
Autres	42
Total	**3510**

Thèmes des commissions rogatoires reçues par l'Agence technique des télécommunications tunisienne entre le 16avril2014 et le 10juin2017	
Identifiant de connexion du titulaire d'un compte Facebook	1290
Identification de l'utilisateur d'un téléphone mobile	1731
Identification d'un voleur informatique	193
Identification de l'exploitant d'une adresseIP	107
Identification du titulaire d'un compte Skype	7
Identification du titulaire d'un compte de messagerie électronique	70
Identification du propriétaire d'un site web	51
Identifiant de connexion du titulaire d'un compte Twitter	16
Identification du titulaire d'un compte YouTube	2
Extraction du contenu d'un téléphone mobile ou d'un ordinateur	26
Divers	17
Total	**3510**

Bibliographie

1. Déclaration d'Oliver Tambo, Union africaine, Johannesburg 2009
2. Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel
3. Convention arabe pour la lutte contre la cybercriminalité
4. Convention de Budapest sur la cybercriminalité du Conseil de l'Europe
5. Andy Greenberg (20avril 2011) Crypto Currency
6. Andy Greenberg (19novembre 2014) Hacker Lexicon: What is the dark web?
7. Arab Social Media Report 2017 Debbie Stephenson (27juillet2014) Spear Phishing: Who's Getting Caught?
8. Étude comparative de la Convention de l'Union africaine de Malabo et de la Convention de Budapest sur la cybercriminalité du 20 novembre 2016
9. Eric Tamarkin, (20 janvier 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73
10. Paragraphe 185 du rapport explicatif de la Convention de Budapest, n°10.
11. Rapport explicatif de la Convention sur la cybercriminalité, n°298.
12. Gercke, 10 Years Convention on Cybercrime, Computer Law Review International, 2011
13. 8è édition de l'examen de la législation type à l'échelle mondiale de l'ICMEC - Programme mondial cybersécurité de l'UIT/Groupe d'experts de haut niveau, Rapport stratégique mondial, 2008
14. Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.
15. Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East
16. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
17. R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime
18. Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.
19. Notes explicatives du Comité de la Convention sur la cybercriminalité - 1ermars2017
20. The Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies Legislation and Regulatory Procedures
21. Projet TOR: FAQ
22. Verdelho (2008) The effectiveness of international cooperation against cybercrime
23. Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials

Remerciements

Nous adressons nos plus sincères remerciements aux consultants scientifiques pour leur engagement et leur implication. Leur contribution a été essentielle pour l'élaboration de ce document.