# LIVRE BLANC 2018

## CYBERSECURITE, CYBERDEFENSE & CYBERCRIMINALITE

**Panorama de la règlementation.**

LEXING
ALAIN BENSOUSSAN AVOCATS

[Page laissée intentionnellement blanche]

# LIVRE BLANC 2018

## CYBERSECURITE, CYBERDEFENSE & CYBERCRIMINALITE

**EDITORIAL**

**Didier Gazagne, Avocat - Directeur Business Unit Défense & Sécurité – Drones - Risques, Intelligence économique – Lexing Alain Bensoussan Avocats.**

## Tribune pour un « Code » de règles juridiques internationales applicable au cyberespace.

### Le Cyberespace, 5ème Champ de conflictualité.

Le cyberespace est défini par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques ».

Il s'agit du 5ème champ de conflictualité, après l'air, l'eau, l'espace, la terre et la mer.

Les trois éléments qui caractérisent le cyberespace, sont les réseaux physiques et virtuels, l'information et la donnée, la capacité de prolifération des outils malveillants du fait de la nature même du cyberespace.

### Le cyberespace n'échappe pas à toute régulation.

S'il faut louer le travail du Conseil de l'Europe, la Convention de Budapest est néanmoins aujourd'hui le seul texte à vocation internationale applicable et reconnu par les pays signataires. Toutefois, en raison de sa limitation géographique, la Convention de Budapest présente des restrictions pour la lutte contre les cybermenaces.

Or, les conflits qui se déroulent dans le cyberespace ne sauraient échapper, dans un système international et mondial fondé sur le droit, à toute régulation.

La France participe à un groupe d'Etats, sélectionnés au sein de l'ONU, avec pour mission de travailler à la formulation de recommandations pour le renforcement de la sécurité du cyberespace. Malgré les avancées de ce groupe d'Etats, limité à 20 pays, malgré leur

sélection en raison de leur représentativité, il reste trop restreint pour permettre une reconnaissance au niveau international de règles ou principes de droit du cyberespace.

## La mise en œuvre de la Convention de Budapest repose sur la seule bonne volonté des Etats - Vers une coopération opérationnelle renforcée.

Les recherches effectuées dans le cadre des missions d'études qui nous ont été confiées ont permis de relever que la mise en œuvre de la Convention de Budapest repose trop souvent vis-à-vis de certains Etats sur leur seule bonne volonté.

## La nécessité d'un « Code » intangible de règles juridiques au niveau international au regard des enjeux sécuritaires mondiaux.

Si certains experts craignent un risque de compromis a minima, l'adoption par la communauté internationale d'un « code » intangible de règles juridiques applicable au cyberespace au niveau mondial permettrait de spécifier un certain nombre de problématiques et de règles juridiques et d'aller plus loin que la Convention de Budapest.

L'adoption d'un « Code » international de règles juridiques du cyberespace ne doit pas être conçu comme un outil concurrent de la Convention de Budapest mais bien comme deux instruments juridiques, disposant chacun de leur spécificité et pouvant être complémentaire en fonction de leur champ d'application. En effet, certains considèrent qu'un « Code » international du cyberespace ne pourrait être en raison des nécessaires compromissions afin de plaire au plus grande nombre d'Etats, qu'un instrument juridique a minima.

## Le contenu prospectif d'un « Code » international de règles juridiques du cyberespace.

Le Groupe d'Experts Gouvernementaux (GGE) [1] des Nations unies sur la sécurité de l'information a conclu son dernier cycle de délibérations; que, bien qu'il ait été dans l'incapacité de produire un rapport de consensus en 2017, les rapports de 2015 et de 2013 s'appliquent, y compris – comme ces rapports l'affirment – le droit international, et en particulier la charte des Nations unies, essentielle au maintien de la paix et de la stabilité.

Le Groupe d'Experts Gouvernementaux (GGE) qui s'est réunie afin d'examiner les progrès de l'information et des télécommunications dans le contexte de la sécurité internationale n'est pas davantage parvenu à saisir l'opportunité de proposer l'adoption d'un « Code » international de règles juridiques du cyberespace. Ce « code » international présenterait en effet une grande avancée pour créer un instrument juridique international qui ne serait pas en conflit avec la Convention de Budapest, mais complémentaire à celle-ci.

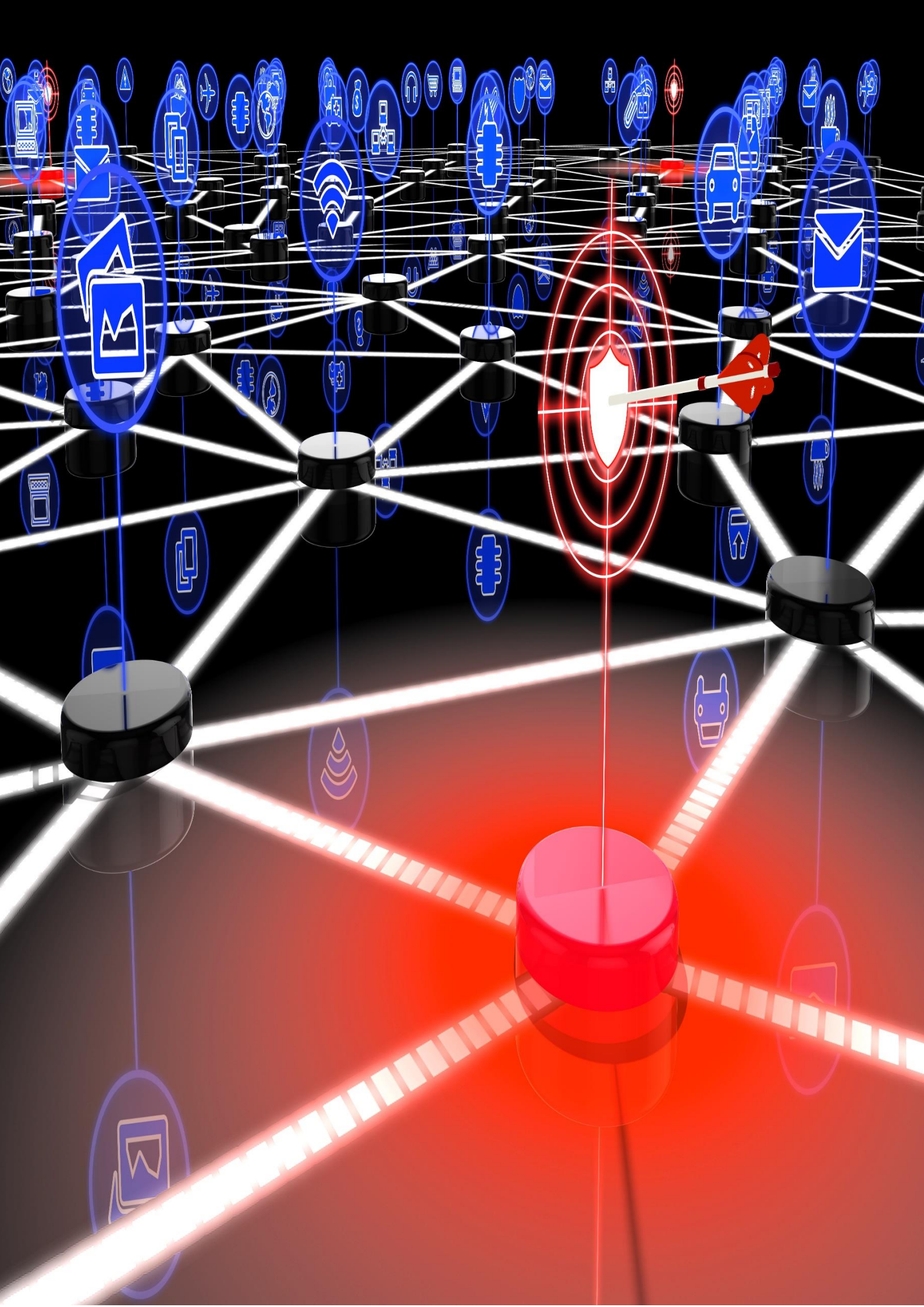
L'adoption au niveau international d'un « code » de règles juridiques du cyberespace permettrait de :

- de définir les termes « cyberespace » et « cyberconflit » ;
- de qualifier sur le plan juridique au niveau international une cyberattaque ;
- d'encadrer les conditions de légitime défense en cas de cyberattaque dans le cyberespace.

[1] https://cd-geneve.delegfrance.org/19-au-23-juin-2017-New-York-4eme-session-du-Groupe-d-experts-gouvernementaux

L’actualité internationale récente sur l’attribution de cyberattaques, pourrait nécessiter l’instauration d’un « Code » international du cyberespace afin de définir également les conditions de réponse à incident, à moins de considérer que l’automatisation systématique de la réponse à incident soit considérée comme une perspective.

[Page laissée intentionnellement blanche]



# SOMMAIRE

## INTRODUCTION

La Convention de Budapest reste aujourd'hui le traité international le plus efficace sur la cybercriminalité. Le livre blanc réalisé par le Cabinet Lexing Alain Bensoussan Avocats, propose une analyse des réponses en matière de réglementation sur la cybercriminalité d'un panorama de pays sur les cinq continents.

En effet la cybercriminalité est un enjeu stratégique national dont de nombreuses actions sont en cours pour améliorer l'organisation des Etats, adapter le cadre juridique, engager des relations avec des partenaires étrangers de confiance.

En janvier 2017, la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces a mis en ligne un rapport n°1 sur l'état de la menace au numérique en 2017.

L'un des enjeux, développé dans ce rapport est la preuve numérique et notamment l'accès à la preuve numérique comme atout important dans les investigations des cybermenaces. Pour parvenir à la constitution de cette preuve numérique, il est nécessaire d'avoir un régime juridique adapté[2].

Dans l'attente d'un protocole additionnel à la convention du Budapest portant sur l'accès et l'échange de preuves numériques, le rapport sur la lutte contre la cybercriminalité du 27 juillet 2017[3] précise qu'une approche européenne commune en matière de justice pénale dans le cyberespace constitue une priorité dans la mesure où elle améliorera le respect de l'état de droit dans le cyberespace et facilitera l'obtention de preuve électroniques dans le cadre de procédures pénales.

L'objectif général de ce livre blanc est de faire découvrir et mieux connaître les dispositifs nationaux adoptés en matière de cybersécurité et de cyberdéfense et de lutte contre la cybercriminalité.

Grâce à la réalisation de fiches pays réparties dans les cinq continents une approche internationale est donnée sur la réglementation en matière de criminalité.

Plusieurs critères ont été sélectionnés pour permettre une certaine comparaison entre pays ou entre continent.

Les critères sélectionnés sont les suivants :

- le cadre juridique en matière de cybercriminalité ;

---

[2] Rapport n°1 de la Délégation ministérielle aux industrie de sécurité et à la lutte contre les cybermenaces de janvier 2017 sur l'Etat de la menace lié au numérique en 2017 https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi_wevArNzWAhXMDxoKHR8jAeIQFggsMAE&url=https%3A%2F%2Fwww.interieur.gouv.fr%2Fcontent%2Fdownload%2F101311%2F797853%2Ffile%2FEtat-de-la-menace-Janvier-2017.pdf&usg=AOvVaw3W9xzc2hW0tobu6g2OvNLV

[3] Rapport du Parlement européen du 25 juillet 2017 sur la lutte contre la cybercriminalité http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0272+0+DOC+XML+V0//FR

- les moyens procéduraux utilisés ;
- les forces judiciaires existantes en matière de cybercriminalité ;
- la stratégie nationale du pays en matière de cyberdéfense ou de cybersécurité ;
- l'existence d'un partenariat public-privé.

Sur une majorité des fiches pays une actualité est introduite pour donner la dernière tendance du pays en matière de cybercriminalité.

Un tableau vous permet en synthèse de connaître les informations utiles en matière de cybercriminalité sur un échantillon de 30 pays répartis par sur 5 continents.

Enfin un glossaire permet de maîtriser les notions qui entourent la cybercriminalité.


admin
********

## 1. NOTION DE CYBERSECURITE

1. L'Anssi (Agence nationale de la Sécurité des Systèmes d'Information) a définit la cybersécurité comme un « état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

2. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

3. Le terme cybersécurité[4] désigne l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formation, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité et authenticité, confidentialité, preuve et non-répudiation).

4. La cybersécurité concerne la sécurité de chaque Etat. C'est pourquoi une grande majorité des Etats ont reconnu la nécessité de s'organiser et d'assurer la sécurité et la défense de leurs systèmes techniques.

5. Des stratégies nationales de cybersécurité et cyberdéfense sont nées afin de lutter contre la cybercriminalité.

## 2. NOTION DE CYBERCRIMINALITE

6. La cybercriminalité regroupe trois types d'infractions :

- les infractions spécifiques aux technologies de l'information et de la communication : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements non autorisés de données personnelles (comme la cession illicite des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions ;
- les infractions liées aux technologies de l'information et de la communication : cette catégorie regroupe la pédopornographie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes privées et non aux personnages publics, les atteintes aux biens ;
- les infractions facilitées par les technologies de l'information et de la communication, que sont les escroqueries en ligne, le blanchiment d'argent, la contrefaçon ou toute autre violation de propriété intellectuelle.

[4] Nicolas Arpagian, La Cybersécurité, PUF, coll. « Que sais-je ? », 26 août 2015

7. La Convention sur la cybercriminalité du Conseil de l'Europe, aussi connu sous le nom de Convention de Budapest est le seul instrument international juridiquement contraignant conçu expressément pour lutter contre la cybercriminalité.

8. La Convention de Budapest sert de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties.

9. La convention sur la cybercriminalité de 2001 poursuit trois objectifs déterminés :

- l'harmonisation des législations des États signataires ;
- la modernisation de ces législations, notamment en matière procédurale ;
- l'amélioration de la coopération internationale en matière d'extradition et d'entraide répressive.

10. Le premier axe est l'harmonisation des législations nationales en ce qui concerne la définition des infractions répertoriées par la Convention. Il s'agit donc d'incriminer quatre séries d'infractions qui sont :

- les infractions informatiques : falsification et fraude informatique ;
- les infractions de contenu : la pornographie enfantine. Le protocole additionnel inclut la propagation via Internet d'idées racistes et xénophobes ;
- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le partage non autorisé via Internet des œuvres protégées ;
- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données ou des systèmes.

11. Ensuite, le deuxième axe, d'ordre procédural, définit les moyens d'enquêtes et de poursuites pénales les mieux adaptés à la mondialisation du réseau Internet. La Convention prévoit des règles pour garantir les droits des individus, mais aussi pour faciliter la conduite d'enquête. En ce sens, on peut citer, entre autres, les règles régissant la conservation des données stockées, la conservation et la divulgation rapide des données relatives au trafic, la perquisition des systèmes informatiques, la saisie de données informatiques, la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

12. Enfin, le troisième axe concerne la mise en place d'un système rapide et efficace de coopération internationale. À côté des formes traditionnelles de coopération pénale internationale, prévues notamment par les Conventions européennes d'extradition et d'entraide judiciaire, la Convention sur la cybercriminalité prévoit des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention. Ces conditions sont exigées afin que les autorités judiciaires et les services de police d'un État membre puissent agir pour le compte d'un autre État dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières. En outre, toute donnée obtenue devrait être rapidement communiqué à l'État intéressé.

[Page laissée intentionnellement blanche]

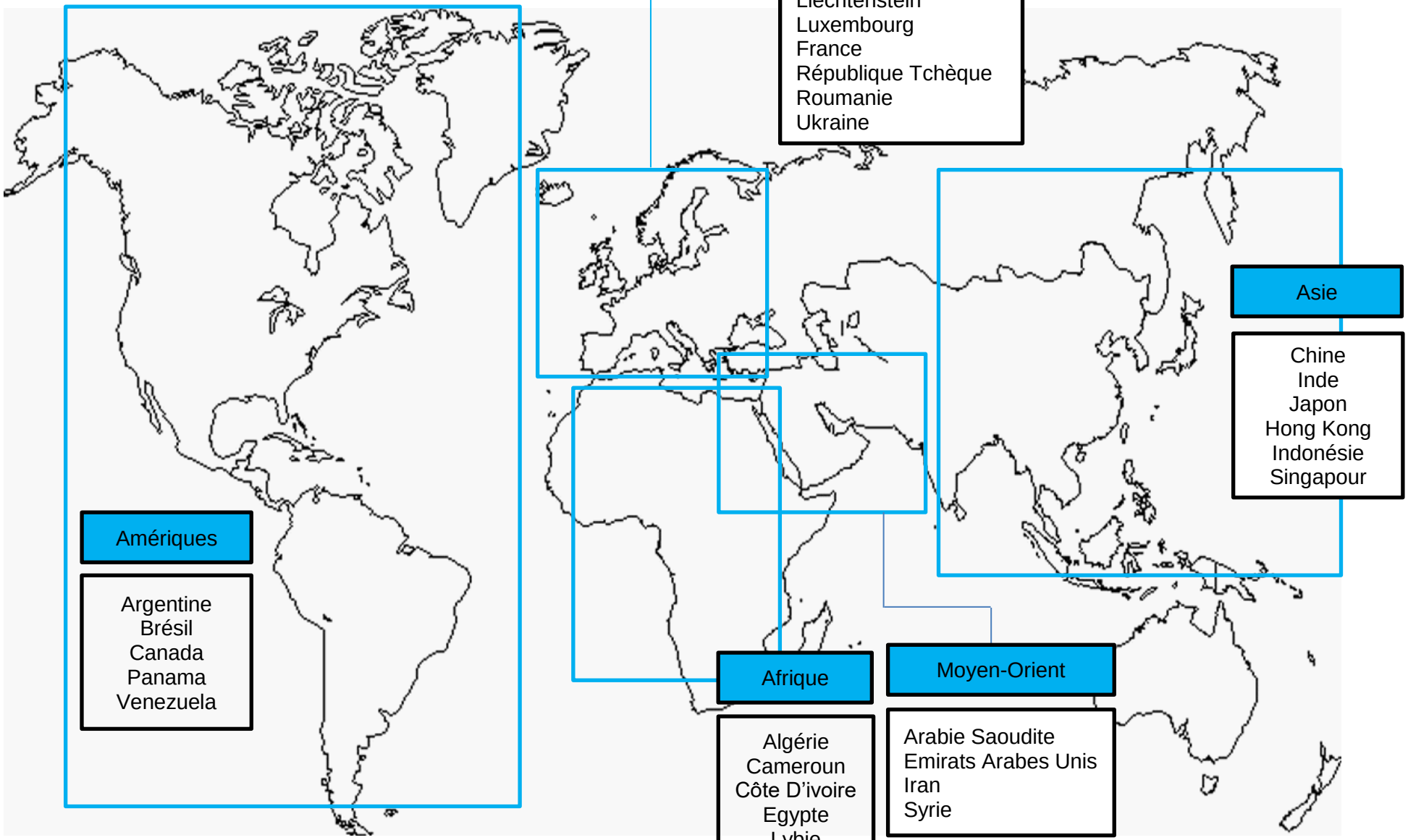
# Cybercriminalité dans le monde

AMERIQUES – AFRIQUE – EUROPE – MOYEN-ORIENT - ASIE

Plusieurs pays du monde ont été sélectionnés parmis 5 continents afin de présenter l'état du droit sur le cadre juridique des pays sélectionnés, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat et la une du pays sélectionnés en matière de cybercriminalité.

[Page laissée intentionnellement blanche]

## 3. SELECTION DES PAYS ETUDIES



[Page laissée intentionnellement blanche]

# Cybercriminalité en Afrique

*ALGERIE – CAMEROUN – [illegible] – LIBYE – MAROC - SOMALIE*

Plusieurs pays du continent africain ont été sélectionnés afin de présenter l'état du droit sur le cadre juridique du pays, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat du pays et la une du pays en matière de cybercriminalité.

## ALGERIE

**Cadre juridique**. L'Algérie n'est pas signataire de la convention de Budapest sur la cybercriminalité.

Le droit algérien comporte une loi spécifique à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, loi n°09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009.

Cette loi vient compléter le code pénal algérien afin que le droit algérien comprenne la majorité des incriminations informatiques présentes dans la Convention de Budapest (9/10).

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée le 27 juin 2014. Elle n'a cependant pas encore été ratifiée par l'Algérie.

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit algérien grâce à la loi n°09-04 permettant ainsi de prendre des mesures pour conserver les données de trafic ou les données stockées, intercepter des données, mettre sur écoute téléphoniques ou encore utiliser la géolocalisation (6/6).

**Forces judiciaires**. L'Algérie possède une cellule de cybercriminalité au sein de la Gendarmerie. Le centre de prévention et de lutte contre la criminalité informatique et la cybercriminalité (CPLCIC). Le centre est composé de trois bureaux, le premier est lié à la cyber-enquête, le second veille sur Internet et le troisième relève de la sécurité numérique.

Les magistrats algériens sont également formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit algérien grâce à une loi relative aux infractions liées aux technologies de l'information et de la communication.

L'Algérie dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Algérie est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. L'Algérie n'est pas encore dotée d'une stratégie de cybersécurité.

L'Algérie possède également un CERT national, DZ-CERT.

Concernant les forces armées et services non gouvernementaux, relatifs à la cybercriminalité.

**Partenariat**. L'Algérie n'a pas encore développé de partenariats public-privé.

**A LA UNE**

**Un programme de sensibilisation visant à protéger les mineurs contre la cybercriminalité sera bientôt lancé par le commandement de la gendarmerie nationale.**

## CAMEROUN

**Cadre juridique**. Bien que le Cameroun ne soit pas signataire de la Convention de Budapest, le droit camerounais possède une loi spécifique à la cybercriminalité, la Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité.

Cette loi n°2010/012 complétée par la loi relative au droit d'auteur permet au droit camerounais de comprendre une partie des toutes incriminations informatiques présentes dans la Convention de Budapest (8/10).

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée. Le Cameroun n'a cependant pas encore ratifié la convention.

**Moyens procéduraux**. Certains moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit camerounais permettant ainsi de prendre des mesures pour conserver les données de trafic ou les données stockées, intercepter des données, mettre sur écoute téléphoniques (4/6).

**Forces judiciaires**. Le Cameroun ne possède pas de cellule cybercriminalité. Il existe en revanche une Agence nationale des technologies de l'information et de la communication (Antic).

Les magistrats camerounais ne sont pas formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit camerounais grâce à une loi relative à la cybersécurité et à la cybercrimialité.

Le Cameroun dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Cameroun est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. Le Cameroun ne s'est pas encore doté d'une stratégie de cybersécurité.

Le Cameroun possède également un CERT national

Le Cameroun n'a pas encore de forces armées et services non gouvernementaux relatives à la lutte contre la cybercriminalité.

**Partenariat**. Le Cameroun n'a pas encore développé de partenariats public-privé.

**A LA UNE**

**Lors du séminaire débit décembre 2016 sur l'Information et la sensibilisation à la cybersécurité, l'ANTIC réaffirme ses travaux : couvrir trois grands axes que sont : l'audit de sécurité, la veille sécuritaire, et la certification électronique au Cameroun.**

## COTE D'IVOIRE

**Cadre juridique**. Bien que la Côte d'Ivoire ne soit pas signataire de la Convention de Budapest, le droit ivoirien possède une loi spécifique à la cybercriminalité, loi n°2013-451 relative à la lutte contre la cybercriminalité.

Cette loi n°2013-451 permet au droit ivoirien de comprendre toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée. La Côte d'Ivoire n'a cependant pas encore ratifié la convention.

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit ivoirien permettant ainsi de prendre des mesures pour conserver les données de trafic ou les données stockées, intercepter des données (6/6).

**Forces judiciaires**. La Côte d'Ivoire ne possède pas de cellule de cybercriminalité. Il existe cependant une Direction de l'Informatiques et des Traces Technologiques (DITT) de la police scientifique ainsi qu'une plateforme de lutte contre la Cybercriminalité PLCC et un laboratoire de criminaliste Numérique LCN.

Les magistrats ivoiriens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit ivoirien. Il existe seulement une loi relative à l'extradition mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

La Côte d'Ivoire dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La Côte d'Ivoire est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. La Côte d'Ivoire ne s'est pas encore dotée d'une stratégie de cybersécurité.

La Côte d'Ivoire possède un CERT national, CI-CERT.

L'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) est l'autorité nationale en matière de TIC et de cybersécurité.

**Partenariat**. La Côte d'Ivoire n'a pas encore développé de partenariats public-privé.

**A LA UNE**

**Les escroqueries sur Internet en Côte d'Ivoire ont baissé grâce à l'arrestation de plusieurs cybercriminels ces dernières années. En la matière, l'une des dernières arrestations a été réalisée par les autorités ivoiriennes en octobre 2016 contre un fraudeur professionnel répondant au nom de « Commissaire 5500 ».**

## EGYPTE

**Cadre juridique**. L'Egypte n'est pas signataire de la convention de Budapest.

Le droit égyptien ne comporte pas de loi spécifique à la cybercriminalité.

Il n'existe pas d'incriminations propres à la lutte contre la cybercriminalité en Egypte.

Le code pénal égyptien comprend très peu d'incriminations informatiques présentes dans la Convention de Budapest (3/10).

Seules la pornographie enfantine, la propriété intellectuelle et les droits connexes sont présents dans le droit égyptien.

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée. L'Egypte n'a cependant pas encore ratifié la convention.

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le droit égyptien (1/6).

Les moyens procéduraux classiques tels que la perquisition et la saisie sont inscrits dans le Code de procédure pénale égyptien.

**Forces judiciaires**. L'Egypte ne possède pas de cellule de cybercriminalité.

Les magistrats égyptiens ne sont pas formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit égyptien. Seuls les articles 553 à 568 du code de procédure pénale relatifs à la coopération internationale en matière pénale existent dans le droit égyptien mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

L'Egypte dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Egypte est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. L'Egypte ne s'est pas encore dotée d'une stratégie nationale de cybersécurité.

L'Egypte possède un CERT national, EG-CERT.

L'Egypte n'a pas encore de forces armées et services non gouvernementaux relatives à la lutte contre la cybercriminalité.

**Partenariat**. L'Egypte n'a pas encore développé de partenariats public-privé.

**A LA UNE**

**Un comité national travaille à l'élaboration d'une politique nationale de cybersécurité.**

**Des programmes de renforcement de compétences à l'endroit des professionnels exposés à la cybercriminalité sont régulièrement organisés, 17 entités égyptiennes dispose de la certification ISO/IEC 27001.**

## LIBYE

**Cadre juridique**. La Lybie n'est pas signataire de la Convention de Budapest.

Le droit libyen ne comporte pas de loi spécifique à la cybercriminalité.

Le droit libyen ne comprend pas de dispositions spécifiquement dédiées à la lutte contre la cybercriminalité. Les articles du Code pénal cités ici sont les dispositions de droit commun susceptibles de couvrir les infractions propres à ce domaine.

Le Code pénal libyen complété par la loi relative à la propriété intellectuelle ne comprend pas toutes les incriminations informatiques (8/10) présentes dans la Convention de Budapest.

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée. La Libye n'a cependant pas encore ratifié la convention.

**Moyens procéduraux**. Le droit libyen ne comprend pas de dispositions spécifiquement dédiées à la lutte contre la cybercriminalité. Les articles du Code de procédure pénale cités ici sont des dispositions de droit commun.

Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code de procédure pénale libyen (2/6).

Les moyens procéduraux classiques tels que la perquisition et la saisie sont inscrits dans le Code de procédure pénale libyen.

**Forces judiciaires**. La Libye ne possède pas de cellule cybercriminalité.

Les magistrats libyens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit libyen.

La Libye dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La Libye est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. La Libye ne s'est pas encore dotée d'une stratégie de cybersécurité. Cependant, l'agence NISSA en particulier et le Ministère de l'Informatique et des Communications sont les autorités responsables de son élaboration.

La Libye possède un CERT national, Libya-CERT.

La Libye n'a pas encore de forces armées et services non gouvernementaux relatives à la lutte contre la cybercriminalité.

**Partenariat**. La Libye n'a pas encore développé de partenariats public-privé.

**MAROC**

**Cadre juridique**. Le Maroc n'est pas signataire de la Convention de Budapest. Le Maroc a cependant adopté en 2003 une loi concernant les infractions relatives aux systèmes de traitement automatisé de données.

Cette loi, le code pénal marocain et la loi relative au droit d'auteur permettent au droit marocain de comprendre presque toutes les incriminations informatiques (9/10) présentes dans la Convention de Budapest.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code de procédure pénale marocain (1/6).

Les moyens procéduraux classiques tels que la perquisition et la saisie sont inscrits dans le Code de procédure pénale marocain.

**Forces judiciaires**. Le Maroc ne possède pas de cellule de cybersécurité.

Les magistrats marocains ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit marocain. Seuls les articles 718 à 750 du code de procédure pénale relatifs à la coopération internationale en matière pénale existent dans le droit marocain mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

Le Maroc dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Maroc est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. Le Maroc s'est doté d'une stratégie de cybersécurité : « the National Strategy of Cybersecurity. Il s'est doté également d'une stratégie nationale relative à la société de l'information et de l'économie numérique de 2013.

Le Maroc possède un CERT national, maCERT.

Depuis 2011, la Direction générale de la sécurité des systèmes d'information (Décret n° 2.11.509) est l'autorité nationale en matière de cybersécurité. Un comité stratégique de la SSI (Décret n° 2.11.508) a également été mis en place la même année. Ces deux entités sont placées sous l'autorité de la direction de la défense nationale.

**Partenariat**. Le Maroc n'a pas encore développé de partenariats public-privé.

**A LA UNE**

**Le plan d'activité pour l'année 2016 en matière de lutte contre la cybercriminalité est :**

- **ateliers de formation (maîtrise des risques majeurs de cybercriminalité, gouvernance SI et stratégie de la cybersécurité, cyber-attaques et cybersécurité ;**
- **symposium national de cybersécurité et cybercriminalité ;**
- **sensibilisation du public ;**
- **conférence internationale de cybersécurité ;**
- **forum euro-africain**.

## SOMALIE

**Cadre juridique**. La Somalie n'est pas signataire de la Convention de Budapest.

Le droit somalien ne comporte pas de loi spécifique à la cybercriminalité.

Le Code pénal somalien n'est pas disponible. Il n'est pas possible d'identifier si le droit somalien comprend les incriminations informatiques présentes dans la Convention de Budapest.

**Moyens procéduraux**. Le Code de procédure pénal somalien n'est pas disponible. Il n'est pas possible d'identifier si les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit somalien.

**Forces judiciaires**. La Somalie ne possède pas de cellule de cybercriminalité.

Les magistrats somaliens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. L'indisponibilité des sources juridiques ne permet pas de connaître si les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit somalien.

La Somalie ne dispose pas d'accords bilatéraux relatifs à l'entraide en matière pénale, à l'extradition.

La Somalie est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. La Somalie ne s'est pas encore dotée d'une stratégie de cybersécurité.

La Somalie de possède pas de CERT national.

La Somalie n'a pas encore de forces armées et services non gouvernementaux relatives à la lutte contre la cybercriminalité.

**Partenariat**. La Somalie n'a pas encore développé de partenariats public-privé

| Questions | ✓ Oui<br>✗ Non | Algérie | Cameroun | Côte d'ivoire | Egypte | Libye | Maroc | Somalie |
|---|---|---|---|---|---|---|---|---|
| **Cadre juridique** | | | | | | | | |
| Le pays est-il signataire à la Convention de Budapest ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Exite -t-il des lois nationales spécifiques à la cybercriminalité ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il des dispositions dans le Code pénal ? | | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✗ |
| Existe-t-il des dispositions dans le Code de procédure pénale ? | | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| **Cyber incrimination** | | | | | | | | |
| L'incrimnation accès illégal existe-t-elle dans législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| L'incrimination interception illégale existe-t-elle dans la législation ? | | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| L'incrimination atteinte intégrité données existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| L'incrimination atteinte intégrité système existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| L'incrimination abus de dispositif existe-t-elle dans la législation du pays ? | | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| L'incrimination falsification informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| L'incrimination fraude informatique existe-t-elle dans la législation du pays ? | | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| Des incriminations relatives à la pornorgraphie infantine existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Des incrimination relatives à la propriété intellectuelle et aux droits connexes existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des autres cyber incriminations hors Convention de Budapest existent-elles dans la législation du pays ? | | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| **Moyens de procédure** | | | | | | | | |
| Des moyens de procédure relatifs à la conservation données existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à l'injonction de produire existent-ils dans la législation du pays ? | | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à la perquisition et à la saisie existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Des moyens de procédure relatifs à l'interception données existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Des moyens de procédure relatifs aux écoutes téléphoniques existent-ils dans la législation du pays? | | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| Des moyens de procédure relatifs à la géolocalisation existent-ils dans la législation du pays ? | | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

| Questions | ✓ Oui<br>✗ Non | Algérie | Cameroun | Côte d'ivoire | Egypte | Libye | Maroc | Somalie |
|---|---|---|---|---|---|---|---|---|
| **Forces judiciaires** | | | | | | | | |
| Existe-t-il des organisations liées à la cybercriminalité, cyberdéfense ou cybersécurité dans le pays ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il une cellule cybercriminalité dans le pays ? | | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Existe-il- des Magistrats spécialisés dans le domaine de la cybercriminalité dans le pays ? | | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Coopération internationale** | | | | | | | | |
| Des dispositions relatives à l'entraide existent-elles dans la législation du pays ? | | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Des dispositions relatives à l'extradition existent-elles dans la législation du pays ? | | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ |
| Le pays appartient-il à des organisations relatives à la coopération internationale? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Le pays a-t-il signé des accords bilatéraux ou régionaux ou internationaux relatif à l'entraide en matière pénale ou à l'extradition ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des points de contact 24/7 dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Stratégie nationale** | | | | | | | | |
| Existe-t-il une stratégie cybersécurité dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il une stratégie cybercriminalité dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il une stratégie nationale cyberdéfense dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il une autorité nationale dans le pays ? | | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il des CERTS dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Existe-t-il des FASG dans le pays ? | | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

[Page laissée intentionnellement blanche]

# Cybercriminalité en Amériques

*ARGENTINE – BRESIL – CANADA – PANAMA - VENEZUELA*

Plusieurs pays du continent américain ont été sélectionnés afin de présenter l'état du droit sur le cadre juridique du pays, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat du pays et la une du pays en matière de cybercriminalité.

## ARGENTINE

**Cadre juridique**. L'Argentine n'a pas signé la convention de Budapest sur la cybercriminalité. Cependant l'Argentine a demandé à être invitée à adhérer à la Convention du Conseil de l'Europe sur la cybercriminalité.

Le droit argentin comporte une loi spécifique aux délits informatiques, "Loi n° 26.388 Delitos informaticos". Cette loi vient compléter le code pénal argentin afin que le droit argentin comprenne toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

Une incrimination spécifique au droit argentin a également été incorporée dans le Code pénal tel que l'accès à une base de données personnelles.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code de procédure pénale argentin ni dans la loi sur la cybercriminalité de juin 2008 (2/6).

Seuls les moyens procéduraux classiques tels que la perquisition, la saisie et l'injonction de produire sont inscrits dans le Code de procédure pénale argentin.

**Forces judiciaires**. L'Argentine ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats argentins ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit argentin. Seule une loi relative à la coopération internationale en matière pénale ("Ley de cooperacion internacional en materia penal, Ley n°24.767") existe dans le droit argentin mais elle n'est pas spécifique à la lutte contre la cybercriminalité.

L'Argentine dispose de nombreux accords régionaux (inter-américains), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Argentine est membre d'une organisation internationale ITU-IMPACT et d'organisations régionales telles que, Organisation des Etats américains (OAS).

**Stratégie nationale**. L'Argentine s'est dotée d'une stratégie de cybersécurité et cyberdéfense en 2013.

L'Argentine possède également un CERT national, ArCERT.

Concernant les forces armées et services non gouvernementaux, l'Argentine a notamment créée un Programme national d'information sur les infrastructures critiques et la cybersécurité.

Les autorités de référence en matière de cybersécurité sont:
Oficina Nacional de Tecnologías de Información (ONTI) ;Undersecretary of CIIP and Cybersecurity ;The National Directorate of CIIP and Cybersecurity ; Argentine Federal Police ; Argentine National Gendarmerie (ANG) ;

**Partenariat**. L'Argentine n'a pas encore développé de partenariats public-privé.

**BRESIL**

**Cadre juridique**. Le Brésil n'est pas signataire de la Convention de Budapest sur la cybercriminalité.

Le droit brésilien comporte des lois spécifiques à la cybercriminalité, il peut être cité la loi 8,137/1990, la loi 8,069/1990,la loi 9,100/1995, la loi 9,296/1996, la loi 9,504/1997, la loi 9,983/2000, la loi 11,829/2008, la 12,735/2012 ou encore la loi 12,737/2012. Ces lois sont complétées par le code pénal brésilien afin que le droit brésilien comprenne un large éventail incriminations informatiques qui se rapprochent de celles présentes dans la Convention de Budapest (10/10).

D'autres incriminations spécifiques au droit brésilien ont également été incorporées dans le code pénal dans des domaines particuliers tels que les finances publiques ou les systèmes
automatisés des données utilisées par le service électoral.

**Moyens procéduraux**. Les moyens procéduraux classiques tel que la perquisition, la saisie qui sont présents dans la Convention de Budapest trouvent un parallèle dans le code de procédure pénale brésilien (3/6). La loi n° 9.296 de 1996 permet l'interception de données et les écoutes téléphoniques.

**Forces judiciaires**. Le Brésil ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats brésiliens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale sont présentes dans le droit brésilien grâce à une loi brésilienne relative à la coopération international en matière pénale ("Lei n° 6.815 - Estatuto do Estrangeiro").

Le Brésil dispose de nombreux accords régionaux (inter-américains), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Brésil est membre d'une organisation internationale ITU-IMPACT et d'organisations régionales telles qu'Inter-American Committee against Terrorism (CICTE), Organisation des Etats américains (OAS).

**Stratégie nationale**. Le Brésil s'est doté d'une stratégie générale sur les technologies de l'information et de la communication. Le Brésil dispose d'un décret n ° 6703 de 2008 sur la stratégie de défense nationale.

Le Brésil possède également un CERT national, CERT.br, d'un CSIRT gouvernemental et plusieurs CERT sectoriels.

Concernant les forces armées et services non gouvernementaux, le Brésil a notamment un Conseil de défense nationale, une agence de renseignement (ABIN), la Chambre des Affaires étrangères et de la Défense nationale (CREDEN) qui comporte une l'équipe technique de la Sécurité cybernétique.

**Partenariat**. Le Brésil n'a pas encore développé des partenariats public-privé.

## CANADA


**Cadre juridique**. Le Canada a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2001. La Convention entrera en vigueur sur son territoire le 1er novembre 2015 soit plus de 9 ans après la France.

L'entrée en vigueur du projet de loi C-13, la Loi sur la protection des Canadiens contre la cybercriminalité, le 9 mars 2015 a accéléré la ratification de la Convention de Budapest par le Canada.

Le droit canadien comporte une loi spécifique à la cybercriminalité, " loi sur la protection des canadiens contre la cybercriminalité".
Cette loi et la loi relative au droit d'auteur ont permis de compléter le Code criminel canadien et d'y faire apparaître presque toutes les incriminations informatiques présentes dans la Convention de Budapest (9/10).

Le fait de distribuer une image intime sans le consentement de la personne représentée est érigé en infraction au Canada.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code de procédure pénale canadien (3/6).
Les écoutes téléphoniques et la géolocalisation hors Convention de Budapest sont des moyens de procédure prévus par le droit canadien.

**Forces judiciaires**. Le Canada possède une cellule cybercriminalité, Groupe intégré de la criminalité technologique (GICT).

Les magistrats canadiens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale sont présentes dans le droit canadien grâce à deux lois canadiennes relatives à la coopération international en matière pénale ("Loi sur l'entraide judiciaire en matière criminelle" et "Loi sur l'extradition").

Le Canada dispose de nombreux accords régionaux (inter-américain), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Canada est membre d'organisations telles que l'Organisation des Etats américains (OAS) ou l'Organisation pour la sécurité et la coopération en Europe (OSCE).

**Stratégie nationale**. Le Canada s'est doté d'une stratégie de cybersécurité en 2010. Le Canada a également adopté un plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada.

Le Canada possède également de nombreux CERT, dont le CERT national, CCIRC Canadian Cyber Incident Response Centre.

Concernant les forces armées et services non gouvernementaux, le Canada a notamment la Gendarmerie royale du Canada, le Centre antifraude du Canada (CAFC), le Service canadien du renseignement de sécurité.

**Partenariat**. Le Canada n'a pas encore développé de partenariats public-privé.

## PANAMA

**Cadre juridique**. Le Panama a ratifié la Convention de Budapest sur la cybercriminalité le 5 mars 2014 permettant à la convention de rentrer en vigueur le 1er juillet 2014.
Le Panama est le deuxième pays d'Amérique Latine a avoir ratifié la Convention de Budapest.

Les dispositions relatives aux incriminations informatiques sont présentes dans le Code pénal panaméen et notamment dans le titre VIII dénommé : crimes contre la sécurité juridique des médias électroniques.

Le Code pénal panaméen complété par la loi relative au droit d'auteur comprend des dispositions relatives à presque toutes les incriminations informatiques présentes dans la Convention de Budapest (9/10).

D'autres incriminations spécifiques au droit panaméen ont également été incorporées dans le Code pénal tel que le fait d'effectuer des délits financier par la manipulation d'un ordinateur, des moyens frauduleux ou technologiques ou de détruire, dissimuler ou falsifier les livres de compte, les dossiers comptables, les états financiers ou autres informations financières d'une personne physique ou morale.

**Moyens procéduraux**. Les moyens procéduraux classiques tel que la perquisition, la saisie qui sont présents dans la Convention de Budapest trouvent un parallèle dans le code de procédure pénale panaméen (3/6). La loi loi n°16 de 2004 permet la collecte de données et l'interception des données.

**Forces judiciaires**. Le Panama ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybercriminatlité.

Les magistrats panaméens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit panaméen. Seuls les articles 2496 à 2516 du Code judiciaire panaméen relatifs à la coopération internationale en matière pénale existent dans le droit panaméen mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

Le Panama dispose de nombreux accords régionaux (inter-américain), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Panama est membre d'une organisation internationale ITU-IMPACT et d'organisations telles qu'Inter-American Committee against Terrorism (CICTE), Organisation des Etats américains (OAS).

**Stratégie nationale**. Le Panama s'est doté d'une stratégie de cybersécurité en 2013.

Le Panama possède un CERT national, CSIRT Panama.

L'autorité de référence en matière de cybersécurité est la Autoridad Nacional para la Innovación Gubernamental (AIG) créée et établie en 2009.

**Partenariat**. Le Panama n'a pas encore développé des partenariats public-privé.

**VENEZUELA**

**Cadre juridique**. Le Venezuela n'est pas signataire de la Convention de Budapest sur la cybercriminalité.

Le droit vénézuélien comporte une loi spécifique à la cybercriminalité, loi n°37313 "Ley Especial Contra los Delitos Informaticos" Cette loi est complétée par le code pénal vénézuélien afin que le droit vénézuélien comprenne toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code de procédure pénale vénézuélien. Seuls les moyens procéduraux classiques tels que la perquisition et la saisie sont inscrits dans le Code de procédure pénale vénézuélien (2/6).

**Forces judiciaires**. Le Venezuela possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité. Il possède cepedannt

Les magistrats vénézuéliens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit vénézuélien. Seuls les articles 382 à 390 du Code de procédure pénale relatifs à la coopération internationale en matière pénale existent dans le droit vénézuélien mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

Le Venezuela dispose de nombreux accords régionaux (inter-américain), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Venezuela est membre d'une organisation internationale ITU-IMPACT et d'organisations telles qu'Organisation des Etats américains (OAS)

**Stratégie nationale**. Le Venezuela ne s'est pas doté d'une stratégie de cybersécurité, de cybercriminalité ou de cyberdéfense.

Le Venezuela possède également un CERT national, VenCERT.

Concernant les forces armées et services non gouvernementaux, le Venezuela a notamment une Surintendance des services de certification électronique (SUSCERTE).

**Partenariat**. Le Venezuela n'a pas encore développé des partenariats public-privé.

| Questions | ✓ Oui<br>✗ Non | Argentine | Brésil | Canada | Panama | Venezuela |
|---|---|---|---|---|---|---|
| **Cadre juridique** | | | | | | |
| Le pays est-il signataire à la Convention de Budapest ? | | ✗ | ✗ | ✓ | ✓ | ✗ |
| Exite -t-il des lois nationales spécifiques à la cybercriminalité ? | | ✓ | ✓ | ✓ | ✗ | ✓ |
| Existe-t-il des dispositions dans le Code pénal ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des dispositions dans le Code de procédure pénale ? | | ✓ | ✓ | ✗ | ✓ | ✓ |
| **Cyber incrimination** | | | | | | |
| L'incrimnation accès illégal existe-t-elle dans législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination interception illégale existe-t-elle dans la législation ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination atteinte intégrité données existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination atteinte intégrité système existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination abus de dispositif existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✗ | ✗ | ✓ |
| L'incrimination falsification informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination fraude informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des incriminations relatives à la pornorgraphie infantine existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des incrimination relatives à la propriété intellectuelle et aux droits connexes existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des autres cyber incriminations hors Convention de Budapest existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ |
| **Moyens de procédure** | | | | | | |
| Des moyens de procédure relatifs à la conservation données existent-ils dans la législation du pays ? | | ✗ | ✗ | ✓ | ✗ | ✗ |
| Des moyens de procédure relatifs à l'injonction de produire existent-ils dans la législation du pays ? | | ✓ | ✗ | ✓ | ✗ | ✗ |
| Des moyens de procédure relatifs à la perquisition et à la saisie existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des moyens de procédure relatifs à l'interception données existent-ils dans la législation du pays ? | | ✗ | ✓ | ✗ | ✓ | ✓ |
| Des moyens de procédure relatifs aux écoutes téléphoniques existent-ils dans la législation du pays? | | ✓ | ✓ | ✓ | ✗ | ✓ |
| Des moyens de procédure relatifs à la géolocalisation existent-ils dans la législation du pays ? | | ✗ | ✓ | ✓ | ✗ | ✗ |

| Questions | ✓ Oui<br>✗ Non | Argentine | Brésil | Canada | Panama | Venezuela |
|---|---|---|---|---|---|---|
| **Forces judiciaires** | | | | | | |
| Existe-t-il des organisations liées à la cybercriminalité, cyberdéfense ou cybersécurité dans le pays ? | | ✗ | ✓ | ✓ | ✗ | ✗ |
| Existe-t-il une cellule cybercriminalité dans le pays ? | | ✗ | ✗ | ✓ | ✗ | ✗ |
| Existe-il- des Magistrats spécialisés dans le domaine de la cybercriminalité dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Coopération internationale** | | | | | | |
| Des dispositions relatives à l'entraide existent-elles dans la législation du pays ? | | ✓ | ✗ | ✓ | ✗ | ✗ |
| Des dispositions relatives à l'extradition existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Le pays appartient-il à des organisations relatives à la coopération internationale? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Le pays a-t-il signé des accords bilatéraux ou régionaux ou internationaux relatif à l'entraide en matière pénale ou à l'extradition ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des points de contact 24/7 dans le pays ? | | ✗ | ✗ | ✗ | ✓ | ✗ |
| **Stratégie nationale** | | | | | | |
| Existe-t-il une stratégie cybersécurité dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ |
| Existe-t-il une stratégie cybercriminalité dans le pays ? | | ✓ | ✗ | ✓ | ✓ | ✗ |
| Existe-t-il une stratégie nationale cyberdéfense dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ |
| Existe-t-il une autorité nationale dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des CERTS dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des FASG dans le pays ? | | ✓ | ✓ | ✓ | ✗ | ✓ |
| **Partenariat public/privé** | | | | | | |
| Existe-t-il des partenariats public-privé dans le pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ |

[Page laissée intentionnellement blanche]

# Cybercriminalité en Asie

## CHINE – INDE – JAPON - HONG KONG – INDONESIE - SINGAPOUR

Plusieurs pays du continent asiatique ont été sélectionnés afin de présenter l'état du droit sur le cadre juridique du pays, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat du pays et la une du pays en matière de cybercriminalité.

## CHINE


**Cadre juridique**. La Chine n'est pas signataire de la convention de Budapest sur la cybercriminalité.

Bien que le droit chinois ne comporte pas de loi spécifique à la cybercriminalité, la loi pénale chinoise comprend presque toutes les incriminations informatiques présentes dans la Convention de Budapest (9/10).

Le droit chinois incrimine la pratique des « human-flesh searches », une forme de harcèlement moral en ligne, ainsi que le refus d'améliorer la sécurité d'un système d'information sur ordre de l'autorité compétente.

**Moyens procéduraux**. La majorité des moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans la loi de procédure pénale chinoise et dans la loi sur la sécurité de l'état (5/6) permettant ainsi de prendre des mesures pour conserver les données de trafic ou les données stockées, intercepter des données, mettre sur écoute téléphoniques ou encore utiliser la géolocalisation.

**Forces judiciaires**. La Chine ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats chinois ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit chinois. Seules les deux lois relatives à la coopération internationale en matière pénale existent dans le droit chinois (loi relative à l'extradition et loi relative à l'entraide judiciaire en matière pénale) mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

La Chine dispose de nombreux accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La Chine est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. La Chine s'est dotée d'une stratégie de cybersécurité en 2014 et d'un programme, the National Medium- and Long-Term Program for Science and Technology Development (2006-2020).

La Chine possède également un CERT national, CNCERT/CC.

Concernant les forces armées et services non gouvernementaux, la Chine a un Ministère de l'Industrie et de la Technologie de l'information, une unité de cyber espionnage, National Network & Information Security Coordination Team, State Internet information Office, Ministry of Science and Technology, Central Internet Security and Informatization Leading Group.

**Partenariat**. La Chine n'a pas encore développée de partenariats public/privé.

**INDE**


**Cadre juridique**. L'Inde n'est pas signataire de la convention de Budapest sur la cybercriminalité.

En novembre 2000, l'Inde a adopté une loi consacrée aux technologies de l'information et à la lutte contre la cybercriminalité «Information Technology Act », qui a été modifiée en février 2009, précisant ainsi les dispositions relatives aux incriminations informatiques. Cette loi de 2000 et la loi relative au droit d'auteur permettent de faire apparaître dans le droit indien presque toutes les incriminations informatiques présentes dans la Convention de Budapest (9/10).

Une autre incrimination spécifique a également été incorporée dans droit indien, elle consiste à refuser l'accès ou à causer le refus d'accès à un système informatique à une personne habilitée.

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent quasiment tous un parallèle dans le droit indien et notamment dans la loi " Information Technology Act 2008 " (5/6). Les écoutes téléphoniques sont également des moyens de procédure hors Convention de Budapest prévus par le droit indien.

Le blocage de l'accès du public à une information et des dispositions spécifiques aux cybercafés sont également prévus par le droit indien.

**Forces judiciaires**. L'Inde possède une cellule cybercriminalité depuis 2000 " Cyber Crime Investigation Cell".

L'Inde dispose d'une capacité d'entraînement et de formation des forces judiciaires dédiées à la lutte contre la cybercriminalité.

L'Inde a également mis en place des juridictions spécialisées (Cyber Appellate Tribunal).

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit indien. Seule une loi relative à la coopération internationale en matière pénale existe dans le droit indien (« Extradition Act ») mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

L'Inde dispose également d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Inde est membre d'une organisation internationale ITU-IMPACT.

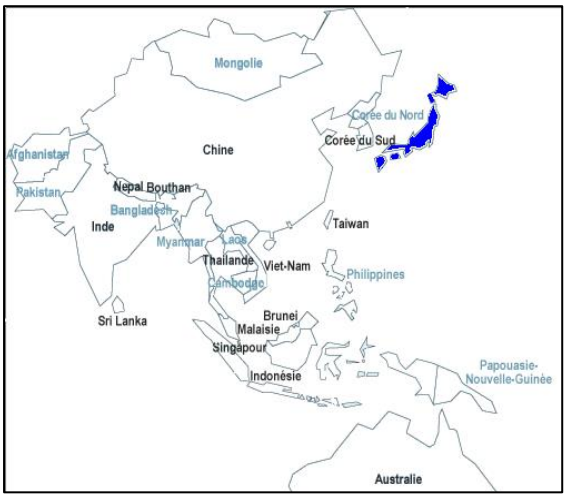
**Stratégie nationale**. L'Inde s'est dotée d'une stratégie de cybersécurité à partir de 2013 "National Cyber Security Policy (NCSP) " qui est complétée par un plan sur 5 ans en matière de cybersécurité ".

L'Inde possède également un CERT national, CERT-IN.

Concernant les forces armées et services non gouvernementaux, l'Inde a notamment le "Department of Electronics and Information Technology" et le "Ministry of Communications and Information Technology" responsable de l'implémentation de la stratégie national de cybersécurité du pays.

**Partenariat**. L'Inde a développé des partenariats public-privé avec des associations industrielles.

## JAPON




**Cadre juridique**. Le Japon a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2001. Il a ratifié la convention le 3 juillet 2012 permettant à la convention de rentrer en vigueur le 1er novembre 2012.

Le Japon a également adopté une loi consacrée à l'accès illégal aux systèmes d'information de 2013.
La loi « Act on Prohibition of Unauthorized Computer Acces » de 2013, le Code pénal japon et la loi relative au droit d'auteur permettent au droit japonais de comprend presque toutes les incriminations informatiques (8/10) présentes dans la Convention de Budapest grâce à l'entrée en vigueur de lois modifiant le Code pénal japonais.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas un parallèle dans le droit japonais (3/6).

Les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit japonais.

**Forces judiciaires**. Le Japon ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.
Les magistrats japonais ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit japonais grâce à une loi relative à la coopération international en matière pénale ("Law for International Assistance in Investigation and Other Related Matters").

Le Japon dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

**Stratégie nationale**. La stratégie nationale est composée d'une « Basic Policy of Critical Information Infrastructure Protection » de 2014 et d'une «Information Security Strategy for Protecting theNation » de 2013.

Le Japon possède un plan de mise en œuvre de la stratégie « Information Security 2012 Annual Plan ».

Le Japon dispose d'un CERT national (JPCERT/CC).

Au Japon, le Centre national de sécurité de l'information (CNSI) est l'autorité de référence pour la mise en œuvre de la stratégie nationale de cybersécurité, D'autres organismes sont également impliqués :
- Information Security Policy Council (ISPC);
- Le Ministère De l'Economie, du Commerce et de l'Industrie (METI) ;
- Le Ministère de la Défense ;
- La National Police Agency ;
- Le Ministry of Internal Affairs and Communications (MIC).

**Partenariat**. Le Japon n'a pas encore développée de partenariats public/privé.

**A LA UNE**
**Un récent rapport sur la cybersécurité décrit les enjeux et les évolutions récentes de la collaboration franco-japonaise dans le domaine de la cybersécurité.**

## HONG KONG


**Cadre juridique**. Hong Kong n'est pas signataire de la Convention de Budapest.

Hong Kong n'a pas adopté de loi sur la cybercriminalité.

Bien que le droit hongkongais ne comporte pas de loi spécifique à la cybercriminalité, il comprend presque toutes les incriminations informatiques (9/10) présentes dans la Convention de Budapest.

**Moyens procéduraux**. Presque tous les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit hongkongais (5/6).

Les écoutes téléphoniques et la géolocalisation sont également des moyens de procédure hors Convention de Budapest prévus par le droit hongkongais.

**Forces judiciaires**. Hong Kong possède des unités dédiées à la lutte contre la cybercriminalité (Cybersecurity and Technology Crime Bureau, CSTCB).

Les magistrats hongkongais ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit hongkongais. Seules deux lois relatives à la coopération internationale en matière pénale existent dans le droit hongkongais (« Fugitive Offenders Ordinance in Hong Kong » et « Regulation Mutual legal assistance in criminal matters regulation in Hong Kong») mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

Hong Kong a conclu des accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

**Stratégie nationale**. Hong Kong possède une politique nationale de cybersécurité intitulée « Baseline IT Security Policy ».

Hong Kong dispose également d'un CERT national, HKCERT.

Un Comité (« Information Security Management Committee ») gère la mise en œuvre de la politique de cybersécurité.

**Partenariat**. Hong Kong n'a pas encore développée de partenariats public/privé.

## INDONESIE


**Cadre juridique**. L'Indonésie n'est pas signataire de la Convention de Budapest.

L'Indonésie a cependant adopté en 2008 une loi relative à l'information et aux transactions électroniques : «Electronic Information and Transactions Act».

Cette loi de 2008 permet de faire apparaître dans le droit indonésien toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le droit indonésien (3/6).

Seuls les moyens procéduraux classiques tels que la perquisition et la saisie et l'interception de données sur contenu sont inscrits dans le droit indonésien.

Les écoutes téléphoniques et la géolocalisation sont des moyens de procédure hors Convention de Budapest non prévus par le droit indonésien.

**Forces judiciaires**. L'Indonésie ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats indonésiens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit indonésien. Seules deux lois relatives à la coopération internationale en matière pénale existent dans le droit indonésien (« Extradition law » et « Mutual legal assistance law ») mais ces dispositions ne sont pas spécifiques à la lutte contre la cybercriminalité.

L'Indonésie dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Indonésie est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. L'Indonésie ne s'est pas encore dotée de stratégie nationale de cybersécurité/cyberdéfense.

L'Indonésie dispose d'un CERT national (Gov-CERT) et de quelques CERT sectoriels.

Plusieurs autorités de référence sont responsables de la mise en œuvre d'une stratégie de cybersécurité en Indonésie :

- Directorate of Information Security;
- Directorate of General of Informatics Applications;
- Ministry of Communication and Information Security.

**Partenariat**. L'Indonésie n'a pas encore développée de partenariats public/privé.

## SINGAPOUR


**Cadre juridique**. Singapour n'est pas signataire de la Convention de Budapest.

Singapour a cependant adopté en 1993 une loi sur la cybercriminalité : «Computer misuse and cybersecurity act».

Cette loi de 1993 et la loi relative au droit d'auteur permettent de faire apparaître dans le droit singapourien toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le droit singapourien (2/6).

Seuls les moyens procéduraux classiques tels que la perquisition, la saisie et l'injonction de produire sont inscrits dans droit singapourien.

Les écoutes téléphoniques et la géolocalisation sont des moyens de procédure hors Convention de Budapest non prévus par le droit singapourien.

**Forces judiciaires**. Singapour ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats singapouriens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit singapourien grâce à deux relative à la coopération international en matière pénale («Extradition Act» et «Mutual assistance in criminal matters act»).

Singapour dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

**Stratégie nationale**. Singapour dispose également d'une stratégie nationale de cybersécurité ("National Cyber Security Masterplan 2018").

Singapour dispose d'un CERT national (SingCERT), d'un CERT gouvernemental (GITSIR) et de plusieurs CERT sectoriels.

L'autorité de référence responsable de la mise en œuvre de la stratégie de cybersécurité à Singapour est le National Infocomm Security Committee, assistée de l'Infocomm Development Authority.

Singapour participe (à travers SingCERT) à plusieurs initiatives/organisations internationales dédiées à la cybersécurité :
- APCERT ;
- FIRST ;
- ASEAN CERT Incident Drill (ACID) ;
- TSUBAME Working Group (dirigé par le Japon) ;
- PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange) Project.

**Partenariat**. Singapour n'a pas encore développée de partenariats public/privé.

[Page laissée intentionnellement blanche]

| Questions | ✓ Oui<br>✗ Non | Chine | Inde | Japon | Hong Kong | Indonésie | Singapour |
|---|---|---|---|---|---|---|---|
| **Cadre juridique** | | | | | | | |
| Le pays est-il signataire à la Convention de Budapest ? | | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Exite -t-il des lois nationales spécifiques à la cybercriminalité ? | | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des dispositions dans le Code pénal ? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Existe-t-il des dispositions dans le Code de procédure pénale ? | | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |
| **Cyber incrimination** | | | | | | | |
| L'incrimnation accès illégal existe-t-elle dans législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination interception illégale existe-t-elle dans la législation ? | | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |
| L'incrimination atteinte intégrité données existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination atteinte intégrité système existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination abus de dispositif existe-t-elle dans la législation du pays ? | | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| L'incrimination falsification informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ |
| L'incrimination fraude informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des incriminations relatives à la pornorgraphie infantine existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des incrimination relatives à la propriété intellectuelle et aux droits connexes existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des autres cyber incriminations hors Convention de Budapest existent-elles dans la législation du pays ? | | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **Moyens de procédure** | | | | | | | |
| Des moyens de procédure relatifs à la conservation données existent-ils dans la législation du pays ? | | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à l'injonction de produire existent-ils dans la législation du pays ? | | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ |
| Des moyens de procédure relatifs à la perquisition et à la saisie existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Des moyens de procédure relatifs à l'interception données existent-ils dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| Des moyens de procédure relatifs aux écoutes téléphoniques existent-ils dans la législation du pays? | | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à la géolocalisation existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

| Questions | ✓ Oui<br>✗ Non | Chine | Inde | Japon | Hong Kong | Indonésie | Singapour |
|---|---|---|---|---|---|---|---|
| **Forces judiciaires** | | | | | | | |
| Existe-t-il des organisations liées à la cybercriminalité, cyberdéfense ou cybersécurité dans le pays ? | | ✗ | ✓ | ✗ | ✓ | ✗ | ✓ |
| Existe-t-il une cellule cybercriminalité dans le pays ? | | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Existe-il- des Magistrats spécialisés dans le domaine de la cybercriminalité dans le pays ? | | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| **Coopération internationale** | | | | | | | |
| Des dispositions relatives à l'entraide existent-elles dans la législation du pays ? | | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Des dispositions relatives à l'extradition existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Le pays appartient-il à des organisations relatives à la coopération internationale? | | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Le pays a-t-il signé des accords bilatéraux ou régionaux ou internationaux relatif à l'entraide en matière pénale ou à l'extradition ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des points de contact 24/7 dans le pays ? | | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| **Stratégie nationale** | | | | | | | |
| Existe-t-il une stratégie cybersécurité dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Existe-t-il une stratégie cybercriminalité dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Existe-t-il une stratégie nationale cyberdéfense dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Existe-t-il une autorité nationale dans le pays ? | | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Existe-t-il des CERTS dans le pays ? | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des FASG dans le pays ? | | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |

[Page laissée intentionnellement blanche]

# Cybercriminalité en Europe

*ALLEMAGNE – AUTRICHE – LIECHTENSTEIN – LUXEMBOURG – FRANCE - REPUBLIQUE TCHEQUE – ROUMANIE - UKRAINE*

Plusieurs pays du continent européen ont été sélectionnés afin de présenter l'état du droit sur le cadre juridique du pays, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat du pays et la une du pays en matière de cybercriminalité.

## ALLEMAGNE


**Cadre juridique**. L'Allemagne a signé la convention de Budapest sur la cybercriminalité, le 3 novembre 2001. Elle a ratifié la convention le 9 mars 2009 permettant à la convention de rentrer en vigueur le 1er juillet 2009.

Bien que le droit allemand ne comporte pas de loi spécifique à la cybercriminalité, le code pénal allemand comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale allemand (6/6).

La géolocalisation et les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit allemand.

**Forces judiciaires**. L'Allemagne ne possède pas de cellule cybercriminalité, mais des organisations tel que le BSI, l'Office fédéral pour la sécurité de l'information (BSI), en charge de la gestion de la sécurité informatique et de communication pour le gouvernement allemand.

Les magistrats allemands sont également formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale sont présentes dans le droit allemand grâce à une loi allemande relative à la coopération international en matière pénale ("Act on international cooperation in criminal matters").

L'Allemagne dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Allemagne est membre d'une organisation internationale ITU-IMPACT et de nombreuses organisations européennes telles qu'Eurojust, Europol, Enisa...

**Stratégie nationale**. L'Allemagne s'est dotée d'une stratégie de cybersécurité recouvrant les champs de la cybersécurité, de la cyberdéfense et de la lutte contre la cybercriminalité à partir de 2011 complété par un cadre juridique très complet.

L'Allemagne possède également de nombreux CERT, dont le CERT national, CERT-BUND, et des CERT non gouvernementales.

Concernant les forces armées et services non gouvernementaux, l'Allemagne a notamment le Centre national de cyber protection est chargé d'assister l'Office fédéral pour la sécurité des techniques d'information (BSI). Il coopère directement avec l'Office fédéral pour la protection de la Constitution (BfV) et l'Office fédéral pour la protection civile (BBK). L'Office fédéral de police judiciaire (BKA), la Direction de la police fédérale (BPOL), l'Office de police des douanes (ZKA), les services de renseignement fédéraux, l'armée et les autres autorités supervisant les infrastructures critiques sont représentés au sein du centre national de cyber protection.

**Partenariat**. L'Allemagne a développé des partenariats public-privé, tels que l'Alliance pour la Cybersécurité et le partenariat UP KRITIS.

**AUTRICHE**

**Cadre juridique**.
L'Autriche a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2001. Elle a ratifié la convention le 13 juin 2012 permettant à la convention de rentrer en vigueur le 1er octobre 2012.

Bien que le droit autrichien ne comporte


pas de loi spécifique à la cybercriminalité, le code pénal autrichien comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale autrichien (6/6).

La géolocalisation et les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit autrichien.

**Forces judiciaires**. L'Autriche dispose d'un Office fédéral de police criminelle au rôle analogue à celui du Bundeskriminalamt allemand. Elle dispose également d'une Bundespolizei issue de la Bundesgendarmerie, de l'Office fédéral autrichien de police criminelle et de la police autrichienne.

Sa juridiction couvre toute l'Autriche. Son commandement se situe à Vienne et elle compte 9 directions provinciales.

Plus connu sous le nom de BK, le Bundeskriminalamt est chargé de la coordination des enquêtes criminelles au niveau fédéral et assure la lutte contre le crime organisé.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit autrichien grâce à une loi relative à la coopération international en matière pénale ("Federal law on Extradition and Mutual Assistance in Criminal Matters ") et au Code de procédure pénale autrichien.

L'Autriche dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

L'Autriche est membre d'une organisation internationale ITU-IMPACT et de nombreuses organisations européennes telles qu'Eurojust, Europol, Enisa...

**Stratégie nationale**. L'Autriche s'est dotée d'une stratégie de cybersécurité en 2013. Elle est constitutive d'un ensemble plus vaste concernant les initiatives gouvernementales en matière de sécurité des technologies de l'information et de la communication.

L'Autriche possède également un CERT national, CERT.at dont le périmètre d'action est clairement défini. Le gouvernement dispose également d'un cert dédié (GovCERT.at), de même que le Ministère de la Défense (MilCERT)

L'autorité nationale (la coordination de la lutte contre la cybercriminalité) est partagée en Cyber Crime Competence Center (C4) et le Cybersecurity Steering Group. Les actions de lutte sont partagées entre les secteurs public et privé.

**Partenariat**. Plusieurs partenariats existent entre les secteurs public-privé, parmi lesquels l'A-SIT et le Kuratorium Sicheres Österreich.

## LIECHTENSTEIN


**Cadre juridique**. Le Liechtenstein est signataire de la convention de Budapest sur la cybercriminalité mais ne l'a pas encore ratifiée.

Bien que le droit liechtensteinien ne comporte pas de loi spécifique à la cybercriminalité, le code pénal liechtensteinien comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale du Liechtenstein (6/6).

Le Liechtenstein a intégré des moyens procéduraux spécifiques aux nouvelles technologies (ex : surveillance des communications électroniques) au Code de procédure pénale existant. Certains moyens procéduraux prévus par la Convention de Budapest, tels que la surveillance des données relatives au trafic ou la possibilité d'ordonner la conservation rapide de données, n'ont pas été trouvés dans la législation du pays. Il a donc été renvoyé ici aux textes les plus proches.

Les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit du Liechtenstein.

**Forces judiciaires**. L'organisation policière nationale est par conséquent très limitée (120 personnes d'après le site officiel de la Landespolizei).
Les sources officielles de la Landespolizei ne précisent pas l'existence d'une unité dédiée à la lutte contre la cybercriminalité
Au sein de la Landespolizei, un service dédié aux enquêtes liées aux technologies de l'information (au sein de l'Executive Support Division), ainsi qu'une unité Forensic (au sein de la Crime Investigation Division).
Les magistrats liechtensteiniens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas de parallèle dans le droit du Liechtenstein. Seule une loi relative à la coopération internationale en matière pénale ("Gesetz über die internationale Rechtshilfe in Strafsachen " existe dans le droit du Liechtenstein mais elle n'est pas spécifique à la lutte contre la cybercriminalité.
Le Liechtenstein dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Liechtenstein est membre d'organisations européennes telles qu'OSCE, Organisation pour la sécurité et la coopération en Europe.

**Stratégie nationale**. Le Liechtenstein ne s'est pas encore doté d'une stratégie de cybersécurité, de cybercriminalité ou de cyberdéfense.
Le Liechtenstein ne possède pas encore de CERT.

Le Liechtenstein n'a pas encore de forces armées et services non gouvernementaux relatifs à la cybercriminalité, cybersécurité ou cyberdéfense.

**Partenariat**. Le Liechtenstein n'a pas encore développé des partenariats public-privé.

## LUXEMBOURG


**Cadre juridique**. Le Luxembourg a signé la convention de Budapest sur la cybercriminalité, le 28 janvier 2003. Elle a ratifié la convention le 16 octobre 2014 permettant à la convention de rentrer en vigueur le 1er février 2015.

Bien que le droit luxembourgeois ne comporte pas de loi spécifique à la cybercriminalité, le code pénal luxembourgeois comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code d'instruction criminelle luxembourgeois (6/6).

La géolocalisation et les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit luxembourgeois.

**Forces judiciaires**. La Police Grand ducale dispose d'un service de police judiciaire comportant une Section Nouvelles Technologies - mobilisable 24/7 - dont la responsabilité est d'enquêter sur les crimes commis contre les systèmes informatiques et les atteintes aux données.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest ne trouvent pas un parallèle dans le droit luxembourgeois .Seules deux lois relatives à la coopération internationale en matière pénale ("Loi sur l'extradition" et "Loi sur l'entraide judiciaire internationale en matière pénale» existent dans le droit luxembourgeois mais elles ne sont pas spécifiques à la lutte contre la cybercriminalité.

Luxembourg dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Luxembourg est membre d'organisations européennes telles qu'Eurojust, Europol, ENISA…

**Stratégie nationale**. Le Luxembourg a actualisé sa stratégie nationale en matière de cybersécurité en juin 2015.

Luxembourg possède également deux CERT. CIRCL vise à assurer la coordination entre toutes les organisations travaillant à la cybersécurité du Grand-Duché. GOVCERT.LU est dédié à la sécur ité des infrastructures gouvernementales.

Le Luxembourg n'a pas encore de forces armées et services non gouvernementaux relatifs à la cybercriminalité, cybersécurité ou cyberdéfense.

**Partenariat**. Bien que le principe de coopération intersectorielle (public et privé) soit encouragé, il n'est que peu suivi d'effets concrets pour l'instant.

### A LA UNE

**Création en 2017 d'un centre de compétences en cybersécurité.**
**Les objectifs du centre de compétences sont d'accroître à court terme l'avantage concurrentiel actuel du Luxembourg en matière de cybersécurité et à moyen terme, de contribuer au développement des écosystèmes émergeant dans les domaines tels que l'Internet des objets, les technologies spatiales.**

## FRANCE


**Cadre juridique**. La France a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2001. Elle a ratifié la convention le 10 janvier 2006 permettant à la convention de rentrer en vigueur le 1er mai 2006.

Bien que le droit français ne comporte pas de loi spécifique à la cybercriminalité, le code pénal français comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10) grâce à l'entrée en vigueur de nombreuses lois, la plus récente étant la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale français (6/6).
La géolocalisation et les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit français.

La France possède également un moyen de procédure hors Convention de Budapest l'enquête sous-pseudonyme ou cyberpatrouille.

**Forces judiciaires**. La France possède plusieurs cellules cybercriminalité, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, Cyberdouane, la Direction Centrale de la Police Nationale comprend une Sous-Direction de Lutte contre la Cybercriminalité (SDLC)

Les magistrats français sont également formés dans le domaine de la cybercriminalité. La section F1 du Parquet de Paris est composée de deux magistrats et d'un assistant spécialisé en matière de cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit français grâce à l'entrée en vigueur de plusieurs lois qui ont modifié ou complété le Code de procédure pénale français : la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (1) et la loi n° 2013-711 du 5 août 2013

La France dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La France est membre d'une organisation internationale ITU-IMPACT et de nombreuses organisations européennes telles qu'Eurojust, Europol, Enisa...

**Stratégie nationale**. La France s'est dotée d'une stratégie de cybersécurité/cyberdéfense depuis 2011.

La France dispose d'une autorité nationale (Agence Nationale pour la Sécurité des Systèmes d'Information).
Elle dispose également de nombreux CERT, dont le CERT national, CERT-FR, et des CERT non gouvernementales.

Concernant les forces armées et services non gouvernementaux, la France a notamment le Secrétariat général de la défense et de la sécurité nationale Organisation, le Centre d'analyse en lutte informatique défensive, CALID.

**Partenariat**. La stratégie de cybersécurité française contient des recommandations pour une coopération plus étroite avec le secteur privé, mais cela n'a pas encore été développé.

## REPUBLIQUE TCHEQUE


**Cadre juridique**. La République Tchèque a signé la convention de Budapest sur la cybercriminalité, le 9 février 2005. Elle a ratifié la convention le 22 août 2013 permettant à la convention de rentrer en vigueur le 1er décembre 2013.

Bien que le droit tchèque ne comporte pas de loi spécifique à la cybercriminalité, le code pénal tchèque comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale autrichien (6/6).

Les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit tchèque.

La République Tchèque possède des moyens procéduraux de droit commun ainsi que des dispositions relatives aux communications électroniques adoptées en 2005.

**Forces judiciaires**. La République Tchèque ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.
Les magistrats tchèques ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit tchèque grâce une loi relative à la coopération international en matière pénale ("Zákon o mezinárodní justiční spolupráci ve věcech trestních").

La République Tchèque dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La République Tchèque est membre d'organisations européennes telles qu'Eurojust, Europol, ENISA…

**Stratégie nationale**. La Stratégie de cybersécurité de la République tchèque pour la période 2011-2015 a été publié en 2011. Le 01 janvier 2015, la loi sur la cybersécurité est entrée en vigueur, "Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů".

La République Tchèque possède également un CERT national, CSIRT.CZ, et un CERT, GOVCERT.CZ dédié aux installations et agences gouvernementales.

Un centre national de cybersécurité a été lancé le 01 janvier 2015 dans le promouvoir le rapprochement entre les organisations publiques et privées.

La République Tchèque n'a pas encore de forces armées et services non gouvernementaux relatifs à la cybercriminalité, cybersécurité ou cyberdéfense.

**Partenariat**. La République Tchèque conduit également une évaluation sectorielle des risques sécuritaires en coopération avec les milieux privés et académiques. Le Centre National Cyber Security a été lancé le 1er Janvier 2015 pour promouvoir des partenariats public-privé

## ROUMANIE

**Cadre juridique**. La Roumanie a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2013. Elle a ratifié la convention le 12 mai 2004 permettant à la convention de rentrer en vigueur le 1er septembre 2004.

Le droit roumain comporte une loi spécifique à la cybercriminalité, " Law n°161/2003 - Anti-Corruption Law – Title III - on preventing and fighting cybercrime".
Le code pénal roumain vient compléter cette loi afin que le droit roumain comprenne toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale roumain (6/6).

La Roumanie a intégré plusieurs dispositions législatives relatives aux moyens procéduraux de lutte contre la cybercriminalité au sein d'une loi consacrée à la lutte contre la corruption (Anticorruption law n°161/2003, Title III).

Les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit roumain.

**Forces judiciaires**. La Roumanie ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats roumains ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit roumain dans le chapitre V de la loi, "Law n°161/2003 - Anti-Corruption Law – Chapter V ".

La Roumanie dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La Roumanie est membre d'une organisation internationale ITU-IMPACT et d'organisations européennes telles qu'Eurojust, Europol, Enisa...

**Stratégie nationale**. La Roumanie s'est dotée d'une stratégie de cybersécurité en 2013. La stratégie de cybersécurité prévoit la création de deux nouvelles agences de cybersécurité.

La Roumanie possède un CERT national, CERT-RO, et des CERT non gouvernementales.

En supplément du CERT-RO désormais en place, la stratégie de cybersécurité prévoit la création de deux nouvelles agences de cybersécurité dont les attributions ne sont pour l'heure pas connues.

**Partenariat**. La Roumanie n'a pas encore développé de partenariats public-privé.

**UKRAINE**


**Cadre juridique**. L'Ukraine a signé la convention de Budapest sur la cybercriminalité, le 23 novembre 2001. Elle a ratifié la convention le 10 mars 2006 permettant à la convention de rentrer en vigueur le 1er juillet 2006.

Le droit ukrainien comporte une loi spécifique à la cybercriminalité, "The Computer Misuse and Cybercrime Act".
Le code pénal ukrainien vient compléter cette loi afin que le droit ukrainien comprenne toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

**Moyens procéduraux**. Les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le Code de procédure pénale ukrainien.

Sur six des moyens procéduraux présents dans la Convention de Budapest, le droit ukrainien couvre un seul moyen procédural (1/6), les perquisitions et saisies.

Les écoutes téléphoniques hors Convention de Budapest sont également des moyens de procédure prévus par le droit ukrainien.

Cependant un projet de loi actuellement à l'étude en Ukraine prévoit de renforcer les moyens procéduraux de lutte contre la cybercriminalité. « Draft law of Ukraine on combating cybercrime. ».

Si l'on prend en compte le « Draft law of Ukraine on combating cybercrime. », le droit ukrainien couvrira probablement l'ensemble des moyens procéduraux présents dans la Convention de Budapest.

**Forces judiciaires**. L'Ukraine ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats ukrainiens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit ukrainien à l'article 10 du Code pénal et au chapitre 44 du Code de procédure pénale.

L'Ukraine dispose de nombreux accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale, à l'extradition, aux commissions rogatoires.

L'Ukraine est membre d'une organisation internationale ITU-IMPACT et d'organisations européennes telles OSCE, Organisation pour la sécurité et la coopération en Europe.

**Stratégie nationale**. L'Ukraine s'est dotée d'une stratégie de cybersécurité en 2014.

L'Ukraine possède également un CERT national, CERT-UA.

**Partenariat**. L'Ukraine n'a pas encore développé de partenariats public-privé.

[Page laissée intentionnellement blanche]

| Questions | ✔ Oui ✘ Non | Allemagne | Autriche | Liechtenstein | Luxembourg | France | Rép. Tchèque | Roumanie | Ukraine |
|---|---|---|---|---|---|---|---|---|---|
| **Cadre juridique** | | | | | | | | | |
| Le pays est-il signataire à la Convention de Budapest ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Exite -t-il des lois nationales spécifiques à la cybercriminalité ? | | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ | ✔ |
| Existe-t-il des dispositions dans le Code pénal ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il des dispositions dans le Code de procédure pénale ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| **Cyber incrimination** | | | | | | | | | |
| L'incrimnation accès illégal existe-t-elle dans législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination interception illégale existe-t-elle dans la législation ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination atteinte intégrité données existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination atteinte intégrité système existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination abus de dispositif existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination falsification informatique existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| L'incrimination fraude informatique existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Des incriminations relatives à la pornorgraphie infantine existe-t-elle dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Des incrimination relatives à la propriété intellectuelle et aux droits connexes existent-elles dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Des autres cyber incriminations hors Convention de Budapest existent-elles dans la législation du pays ? | | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ | ✘ |
| **Moyens de procédure** | | | | | | | | | |
| Des moyens de procédure relatifs à la conservation données existent-ils dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ |
| Des moyens de procédure relatifs à l'injonction de produire existent-ils dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ |
| Des moyens de procédure relatifs à la perquisition et à la saisie existent-ils dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Des moyens de procédure relatifs à l'interception données existent-ils dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ |
| Des moyens de procédure relatifs aux écoutes téléphoniques existent-ils dans la législation du pays? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ |
| Des moyens de procédure relatifs à la géolocalisation existent-ils dans la législation du pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ |

| Questions | ✔ Oui<br>✘ Non | Allemagne | Autriche | Liechtenstein | Luxembourg | France | Rép. Tchèque | Roumanie | Ukraine |
|---|---|---|---|---|---|---|---|---|---|
| **Forces judiciaires** | | | | | | | | | |
| Existe-t-il des organisations liées à la cybercriminalité, cyberdéfense ou cybersécurité dans le pays ? | | ✔ | ✘ | ✔ | ✔ | ✔ | ✘ | ✘ | ✘ |
| Existe-t-il une cellule cybercriminalité dans le pays ? | | ✘ | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✘ |
| Existe-il- des Magistrats spécialisés dans le domaine de la cybercriminalité dans le pays ? | | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ |
| **Coopération internationale** | | | | | | | | | |
| Des dispositions relatives à l'entraide existent-elles dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Des dispositions relatives à l'extradition existent-elles dans la législation du pays ? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Le pays appartient-il à des organisations relatives à la coopération internationale? | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Le pays a-t-il signé des accords bilatéraux ou régionaux ou internationaux relatif à l'entraide en matière pénale ou à | | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il des points de contact 24/7 dans le pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✔ | ✔ |
| **Stratégie nationale** | | | | | | | | | |
| Existe-t-il une stratégie cybersécurité dans le pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il une stratégie cybercriminalité dans le pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il une stratégie nationale cyberdéfense dans le pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il une autorité nationale dans le pays ? | | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ | ✘ |
| Existe-t-il des CERTS dans le pays ? | | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Existe-t-il des FASG dans le pays ? | | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ✔ | ✔ |
| **Partenariat public/privé** | | | | | | | | | |
| Existe-t-il des partenariats public-privé dans le pays ? | | ✔ | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ |

[Page laissée intentionnellement blanche]

# Cybercriminalité au Moyen-Orient

*ARABIE SAOUDITE – EMIRATS ARABES UNIS – IRAN - SYRIE*

Plusieurs pays de la région du Moyen-Orient ont été sélectionnés afin de présenter l'état du droit sur le cadre juridique du pays, les moyens procéduraux, les forces judiciaires, la coopération internationale, la stratégie nationale, le partenariat du pays et la une du pays en matière de cybercriminalité.

## ARABIE SAOUDITE


**Cadre juridique**. L'Arabie Saoudite n'est pas signataire de la convention de Budapest sur la cybercriminalité.

L'Arabie Saoudite a cependant adopté une loi relative à la cybercriminalité en 2007 « Anti-Cyber Crime Law ».

Toutes les incriminations informatiques (10/10) présentes dans la Convention de Budapest trouvent un parallèle dans le droit saoudien.

L'Arabie Saoudite possède également d'autres incriminations issues de la loi « Anti-Cyber Crime Law », le cyber-chantage, la cyber-diffamation, le déphasage, la pornographie et les jeux d'argent, l'atteinte à la vie privé par l'usage de téléphones mobiles équipés de caméras.

**Moyens procéduraux**. Les moyens procéduraux classiques tel que la perquisition, la saisie, l'injonction de produire présents dans la Convention de Budapest trouvent un parallèle dans la loi de procédure pénale saoudien (3/6). Les écoutes téléphoniques hors Convention de Budapest sont également encadrées pas le droit saoudien.

**Forces judiciaires**. L'Arabie Saoudite ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats saoudiens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**.
L'indisponibilité des sources juridiques ne permet pas de connaître si les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit saoudien.

L'Arabie Saoudite a conclu quelques rares accords bilatéraux relatifs à l'entraide en matière pénale, à l'extradition.

L'Arabie Saoudite est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. La stratégie nationale de cybersécurité de l'Arabie Saoudite est toujours en cours d'élaboration. Plusieurs versions de projets (draft) ont cependant été publiées (Developing National Information Security Strategy for the Kingdom of Saudi Arabia) par le Ministry of Communications and Information Technology.

L'Arabie Saoudite possède un CERT national, CERT-SA.

Le CERT-SA est l'autorité de référence en matière de cybersécurité en Arabie Saoudite.

La Communications and Information Technology Commission, de par ses nombreuses compétences, est également une autorité de référence au niveau national. Elle publie un ensemble de guides, de référentiels de sécurité et délivre les labels et les certifications pour les produits et systèmes.

**Partenariat**. L'Arabie Saoudite n'a pas encore développé des partenariats public-privé.

## EMIRATS ARABES UNIS


**Cadre juridique**. Les Emirats arabes Unis ne sont pas signataires de la convention de Budapest sur la cybercriminalité.

Le droit des Emirats arabes Unis comporte une loi spécifique à la cybercriminalité, "Law on combatting cybercrimes de 2012" qui comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

Les Emirats arabes unis possèdent également d'autres incriminations issues de la loi « Law on combatting cybercrimes », la violation de secret professionnel en ligne, le chantage en ligne, la diffamation en ligne, la pornographie et les jeux en ligne.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le droit des Emirats arabes unis (3/6).

Seuls les moyens procéduraux classiques tels que la perquisition, la saisie et l'injonction de produire sont inscrits dans le droit des Emirats arabes unis.

Les écoutes téléphoniques sont des moyens de procédure hors Convention de Budapest non prévus par le droit des Emirats arabes unis.

**Forces judiciaires**. Les Emirats arabes Unis ne possèdent pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats des Emirats arabes Unis ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit des Emirats arabes unis grâce aux articles 6 et suivants et 64 et suivants de la loi fédérale n°39 « Federal law n°39 on international judicial cooperation in criminal matters ».

Les Emirats arabes Unis disposent d'accords régionaux (européens), transnationaux et bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Les Emirats arabes Unis sont membres d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. Les Emirats arabes Unis se sont dotées une politique générale pour le secteur des télécommunications ainsi que la résolution n°21 sur la sécurité de l'information des organismes gouvernementaux.

Les Emirats arabes Unis possèdent un CERT national, aeCERT.

Le déploiement de la stratégie de cybersécurité relève à la fois de la Telecommunications Regulatory Authority (TRA) et de la National Electronic Security Authority (NESA).

Les Emirats arabes Unis ont mis en place une autorité nationale (National Electronic Security Authority) qui héberge le CERT national (aeCERT) et qui conduit également plusieurs projets de sensibilisation.

**Partenariat**. Les Emirats arabes Unis n'ont pas encore développé des partenariats public-privé.

## IRAN


**Cadre juridique**. L'Iran n'est pas signataire de la convention de Budapest sur la cybercriminalité.

Le droit iranien comporte une loi spécifique à la cybercriminalité, " Computer Crimes Law, 2010" qui comprend toutes les incriminations informatiques présentes dans la Convention de Budapest (10/10).

L'Iran possède également d'autres incriminations issues de la loi « Computer crimes law », les atteintes à la chasteté et à la morale et la diffusion de mensonge.

**Moyens procéduraux**. Tous les moyens procéduraux présents dans la Convention de Budapest ne trouvent pas de parallèle dans le Code iranien (2/6)

Seuls les moyens procéduraux classiques tels que la perquisition, la saisie et l'injonction de produire sont inscrits dans le droit iranien.

Les écoutes téléphoniques et la géolocalisation sont des moyens de procédure hors Convention de Budapest non prévus par le droit iranien.

**Forces judiciaires**. L'Iran possède une cellule cybercriminalité, Cyber Defense et une police spécialisée pour la cybercriminalité (FETA Police).

Les magistrats iraniens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**. Les dispositions relatives à la coopération internationale sont présentes dans le droit iranien grâce à une loi relative à l'extradition ("Extradition Law, May 4, 1960").

L'Iran dispose d'accords bilatéraux relatifs à l'entraide en matière pénale, à l'extradition.

L'Iran est membre d'une organisation internationale ITU-IMPACT.

**Stratégie nationale**. L'Iran s'est dotée d'une stratégie de cybersécurité de la cyberdéfense et de la lutte contre la cybercriminalité.
La stratégie de l'Iran en matière de cybersécurité repose sur la nécessité de créer un réseau national (national information network) indépendant de l'internet mondial (= National Internet Project).

L'Iran possède également un CERT national, CERTCC MAHER et est également membre de l'OIC-CERT.

Concernant les forces armées et services non gouvernementaux, l'Iran a notamment une cyber police, un ministère des technologies de l'information et de la communication, une cyber armée, Conseil Suprême du Cyberespace (Shoray-e Aali-e Fazaye Majazi) ; Le CGRI (Corps des Gardiens de la Révolution Islamique ou Pasdarans)

**Partenariat**. L'Iran n'a pas encore développé des partenariats public-privé.

## SYRIE


**Cadre juridique**. La Syrie n'est pas signataire de la convention de Budapest sur la cybercriminalité.

Le droit syrien comporte une loi spécifique sur la cybercriminalité, "Law on the network communication and computer crime control ". Cette loi n'est cependant pas accessible ne permettant pas de savoir si elle comprend toutes les incriminations informatiques présentes dans la Convention de Budapest.
Tout comme cette loi, le code pénal syrien n'est pas accessible.

**Moyens procéduraux**. Le code pénal et le code de procédure pénale n'étant pas accessible il est difficile de savoir si les moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit syrien.

**Forces judiciaires**. La Syrie ne possède pas encore de cellule cybercriminalité ni d'organisations en charge de la gestion de la cybersécurité.

Les magistrats syriens ne sont pas encore formés dans le domaine de la cybercriminalité.

**Coopération internationale**.
L'indisponibilité des sources juridiques ne permet pas de connaître si les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit syrien.

La Syrie dispose d'un accord régional d'extradition grâce à la ligue arabe, et d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

La Syrie est membre d'une organisation internationale ITU-IMPACT et de l'organisation de la coopération islamique (OIC-CERT).

**Stratégie nationale**. La Syrie ne s'est pas encore dotée d'une stratégie de cybersécurité, de cybercriminalité ou de cyberdéfense.

La Syrie possède un CERT national qui fait parti du NANS, National Agency for Network Service.

La Syrie n'a pas encore de forces armées et services non gouvernementaux relatifs à la cybercriminalité, cybersécurité ou cyberdéfense.

**Partenariat**. La Syrie n'a pas encore développé des partenariats public-privé.

[Page laissée intentionnellement blanche]

| Questions | ✓ Oui<br>✗ Non | Arabie Saoudite | Emirats arabes Unis | Iran | Syrie |
|---|---|---|---|---|---|
| **Cadre juridique** | | | | | |
| Le pays est-il signataire à la Convention de Budapest ? | | ✗ | ✗ | ✗ | ✗ |
| Exite -t-il des lois nationales spécifiques à la cybercriminalité ? | | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des dispositions dans le Code pénal ? | | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il des dispositions dans le Code de procédure pénale ? | | ✗ | ✗ | ✗ | ✗ |
| **Cyber incrimination** | | | | | |
| L'incrimnation accès illégal existe-t-elle dans législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| L'incrimination interception illégale existe-t-elle dans la législation ? | | ✗ | ✓ | ✓ | ✗ |
| L'incrimination atteinte intégrité données existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| L'incrimination atteinte intégrité système existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| L'incrimination abus de dispositif existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| L'incrimination falsification informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| L'incrimination fraude informatique existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✗ |
| Des incriminations relatives à la pornorgraphie infantine existe-t-elle dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ |
| Des incrimination relatives à la propriété intellectuelle et aux droits connexes existent-elles dans la législation du pays ? | | ✓ | ✗ | ✗ | ✓ |
| Des autres cyber incriminations hors Convention de Budapest existent-elles dans la législation du pays ? | | ✓ | ✓ | ✓ | ✓ |
| **Moyens de procédure** | | | | | |
| Des moyens de procédure relatifs à la conservation données existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à l'injonction de produire existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à la perquisition et à la saisie existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à l'interception données existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs aux écoutes téléphoniques existent-ils dans la législation du pays? | | ✗ | ✗ | ✗ | ✗ |
| Des moyens de procédure relatifs à la géolocalisation existent-ils dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |

| Questions | ✓ Oui<br>✗ Non | Arabie Saoudite | Emirats arabes Unis | Iran | Syrie |
|---|---|---|---|---|---|
| **Forces judiciaires** | | | | | |
| Existe-t-il des organisations liées à la cybercriminalité, cyberdéfense ou cybersécurité dans le pays ? | | ✗ | ✗ | ✗ | ✗ |
| Existe-t-il une cellule cybercriminalité dans le pays ? | | ✗ | ✗ | ✓ | ✗ |
| Existe-il- des Magistrats spécialisés dans le domaine de la cybercriminalité dans le pays ? | | ✗ | ✗ | ✗ | ✗ |
| **Coopération internationale** | | | | | |
| Des dispositions relatives à l'entraide existent-elles dans la législation du pays ? | | ✗ | ✗ | ✗ | ✗ |
| Des dispositions relatives à l'extradition existent-elles dans la législation du pays ? | | ✗ | ✗ | ✓ | ✗ |
| Le pays appartient-il à des organisations relatives à la coopération internationale? | | ✓ | ✓ | ✓ | ✓ |
| Le pays a-t-il signé des accords bilatéraux ou régionaux ou internationaux relatif à l'entraide en matière pénale ou à l'extradition ? | | ✗ | ✓ | ✓ | ✓ |
| Existe-t-il des points de contact 24/7 dans le pays ? | | ✗ | ✗ | ✗ | ✗ |
| **Stratégie nationale** | | | | | |
| Existe-t-il une stratégie cybersécurité dans le pays ? | | ✗ | ✓ | ✓ | ✗ |
| Existe-t-il une stratégie cybercriminalité dans le pays ? | | ✗ | ✓ | ✓ | ✗ |
| Existe-t-il une stratégie nationale cyberdéfense dans le pays ? | | ✗ | ✓ | ✓ | ✗ |
| Existe-t-il une autorité nationale dans le pays ? | | ✗ | ✓ | ✓ | ✗ |
| Existe-t-il des CERTS dans le pays ? | | ✓ | ✓ | ✓ | ✓ |
| Existe-t-il des FASG dans le pays ? | | ✗ | ✓ | ✓ | ✗ |

[Page laissée intentionnellement blanche]


internet
e-mail
attack
cybersecurity
protection
computer

## 4. GLOSSAIRE

# A –

**ABUS DE DISPOSITIFS** : désigne (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 précisées dans la convention de Budapest;
(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 dans la convention de Budapest; 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 dans la convention Budapest. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

**ACCES** : désigne toute mise à disposition de moyens, matériels ou logiciels, ou de services, en vue de permettre au bénéficiaire de fournir des services de communications électroniques.

**ACCES ILLEGAL** : désigne l'accès intentionnel et sans droit à tout ou partie d'un système informatique, 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.

**ATTAQUE INFORMATIQUE** : terme générique désignant une action malveillante dont la cible ou le moyen est l'informatique et qui génère un dommage ou un préjudice. Le plus souvent, l'intrusion est facilitée par une vulnérabilité dans le logiciel ou le système de sécurité, qu'exploite l'agresseur aux fins d'installer un programme malware, qui soit récupère et transmet les données pour lesquelles il a été programmé (mots de passe, données personnelles, éléments de propriété littéraire et artistique, secret des affaires, analyse du réseau ou du système, écoute des communications) ou développe une autre attaque interne, à des fins par exemple, de blocage ou de sabotage. Le point d'attaque se situe ordinairement dans le terminal (ordinateur, téléphone portable, objet connecté), mais il peut aussi être dans le centre de données lui-même, ou dans le réseau.

**ATTEINTE A L'INTEGRITE DES DONNEES** : désigne le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

**ATTEINTE A L'INTEGRITE DU SYSTEME** : désigne 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.

# C –

**COMMUNICATION AU PUBLIC EN LIGNE** : désigne toute transmission, sur demande individuelle, de données

numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'information entre l'émetteur et le récepteur.

**COMMUNICATION ELECTROMAGNETIQUE** : désigne toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée.

**CYBERDEFENSE** : désigne l'ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels.

**CYBERESPACE** : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

**CYBERSECURITE** : état recherché pour un système d'information lui permettant résister à des évènements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'il rendent accessibles.

## D –

**DONNEES INFORMATIQUES** : désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.

**DONNEES RELATIVES AU TRAFIC** : désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

## F –

**FALSIFICATION INFORMATIQUE** : désigne 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.

**FOURNISSEUR DE SERVICE** : (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.

**FRAUDE INFORMATIQUE** : désigne 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.

## I –

**INFRACTIONS SE RAPPORTANT A LA PORNOGRAPHIE ENFANTINE** : désignent 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.

**INTERCEPTION ILLEGALE** : désigne 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.

## P –

**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;
(c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

## R –

**RESEAU DE COMMUNICATION ELECTRONIQUE** : toute installation ou tout ensemble d'installation de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de communications et de routage (les réseaux satellitaires, les réseaux terrestres, les systèmes utilisant le réseau électrique pour autant qu'ils servent à l'acheminement de communication électronique, les réseaux assurant la diffusion ou utilisés pour la distribution de service de communication audiovisuelle).

## S –

**SYSTEME INFORMATIQUE** : Désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

[Page laissée intentionnellement blanche]


Ransomware

## 5. A PROPOS DE LA BUSINESS UNIT DEFENSE ET SECURITE AU SEIN DE LEXING ALAIN BENSOUSSAN AVOCATS

Notre expertise et nos compétences nous permettent d'anticiper, d'analyser et d'évaluer les risques, afin de vous permettre de pérenniser et renforcer votre stratégie de cybersécurité mais aussi de défendre contre les conséquences dommageables sur les patrimoines et l'image de votre entreprise, en cas de dommages portés aux réseaux et systèmes d'information de votre entreprise.

### PRESTATIONS AVOCAT CYBERSECURITE CYBERDEFENSE

#### ANTICIPER

Les missions réalisées poursuivent l'objectif de vous permettre de développer une action d'anticipation et d'analyse des risques :

- définition de plan de veille et d'anticipation des menaces cyber ;
- identification des modes opératoires de collecte, d'analyse, de valorisation, de diffusion et de protection de l'information économique stratégique.

En fonction de votre domaine d'activité et de votre plan de veille stratégique et de vos besoins, nous travaillons avec un réseau de correspondants spécialisés en matière d'intelligence économique.

#### ANALYSER ET EVALUER

L'évaluation des risques a pour objectif de vous permettre de définir ou d'adapter votre stratégie globale de cybersécurité aux risques et aux vulnérabilités relatives au patrimoine technologique, scientifique, économique de votre entreprise, aux données stratégiques de votre entreprise mais aussi à l'image de votre entreprise.

Elle comprend les prestations suivantes :

- audit flash des risques de sécurité globale ;
- audit flash des risques et menaces Cyber ;
- cartographie des risques avec validation préalable des enjeux de sécurité globale pour l'entreprise ;
- notes d'alertes et de notes de recommandations sectorielles ;
- note de ciblage des risques cyber ;
- mise en place et tenue d'un registre des failles de sécurité.

#### PERENNISER ET RENFORCER

Les missions comprennent :

- la définition de la politique d'intelligence économique d'une entreprise ;
- la définition de la charte de gouvernance des systèmes d'information ;
- la définition de la politique globale de sécurité de l'entreprise ;
- l'analyse, l'identification des faits générateurs de risques de sécurité et la hiérarchisation des risques ;

- la définition, la mise en place de politique de formation et de sensibilisation aux risques cyber de l'ensemble des acteurs de l'entreprise à la cybersécurité ;
- l'audit des contrats avec les concepteurs de produits informatiques et de systèmes d'information afin de s'assurer qu'ils ont pris en compte les questions de sécurité dès l'origine de leurs développements.

**DEFENDRE**

Il s'agit de la réalisation de toutes actions contentieuses en cas d'atteintes ou d'infractions commises via les réseaux et systèmes d'informations de l'entreprise aux patrimoines technologique, scientifique, économique de l'entreprise.

Nous intervenons pour assister les entreprises de tous secteurs d'activités, souhaitant obtenir réparations pour les atteintes ou infractions portées via leurs systèmes d'informations de toutes natures, technologiques, de gouvernance, de management, de conformité, ainsi que pour tirer parti de la montée en puissance de la norme internationale et européenne.

# L'EQUIPE


## Didier GAZAGNE

**Avocat, Directeur de la Business Unit Défense & Sécurité - Systèmes autonomes - Risques**

**T:**+33 (0)1 82 73 05 05

**M:**+33 (0)6 47 34 16 63

**Email:** didier-gazagne@lexing.law


Expertise

- Droit de la défense et de la sécurité
- Droit de renseignement
- Droit de la cybersécurité et cyberdéfense
- Droit de la robotique et des systèmes autonomes
- Droit de l'informatique et des communications électroniques
- Droit du numérique et des technologies avancées


## Audrey Jouhanet

**Avocat - Business Unit Défense & Sécurité – Systèmes autonomes - Risques**

**T:**+33 (0)1 82 73 05 05

**M:**+33 (0)6 47 34 72 76

**Email:** audrey-jouhanet@lexing.law


Expertise

- Droit de la défense et de la sécurité
- Droit de renseignement
- Droit de la cybersécurité et cyberdéfense
- Droit de la robotique et des systèmes autonomes
- Droit de l'informatique et des communications électroniques
- Droit du numérique et des technologies avancées

[Page laissée intentionnellement blanche]