JULIEN HOUNKPE

DOCTEUR EN DROIT

FORMATION SUR LE CODE DU NUMERIQUE

+229 **95 88 79 25**

https://julienhounkpe.info

Module 5
LA CYBER-CRIMINALITE

I° LA TYPOLOGIE DES INFRACTIONS NUMERIQUES

II° LA POURSUITE DES INFRACTIONS NUMERIQUES

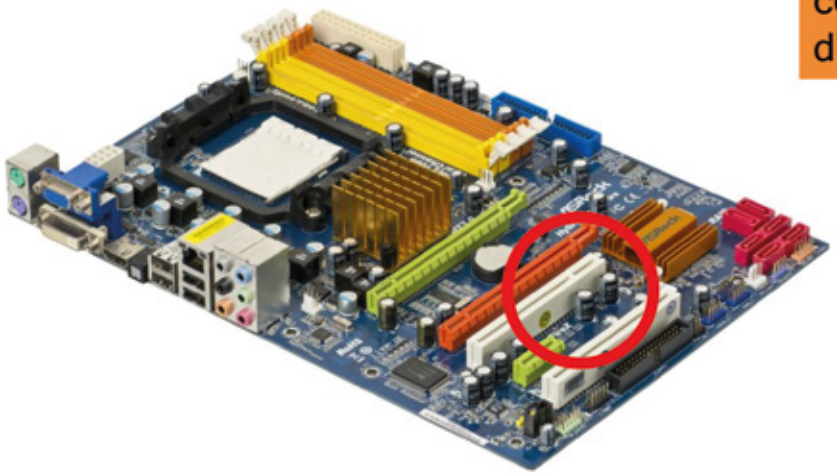
Principales technologies (ordinateurs et internet)

Composantes et principes de fonctionnement des ordinateurs

- Équipements / Hardware
- Logiciels

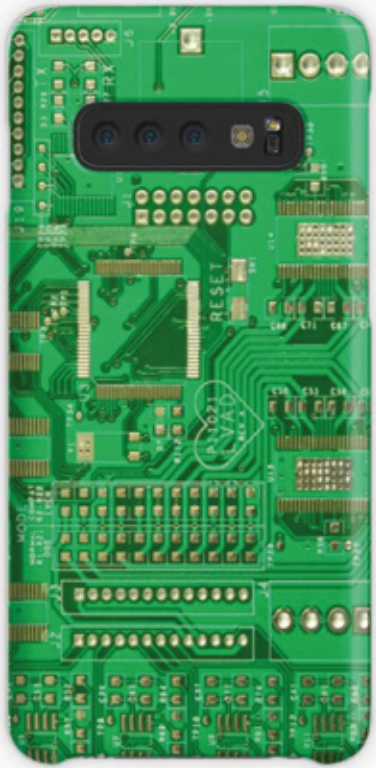
Hardware / Matériels

Carte mère

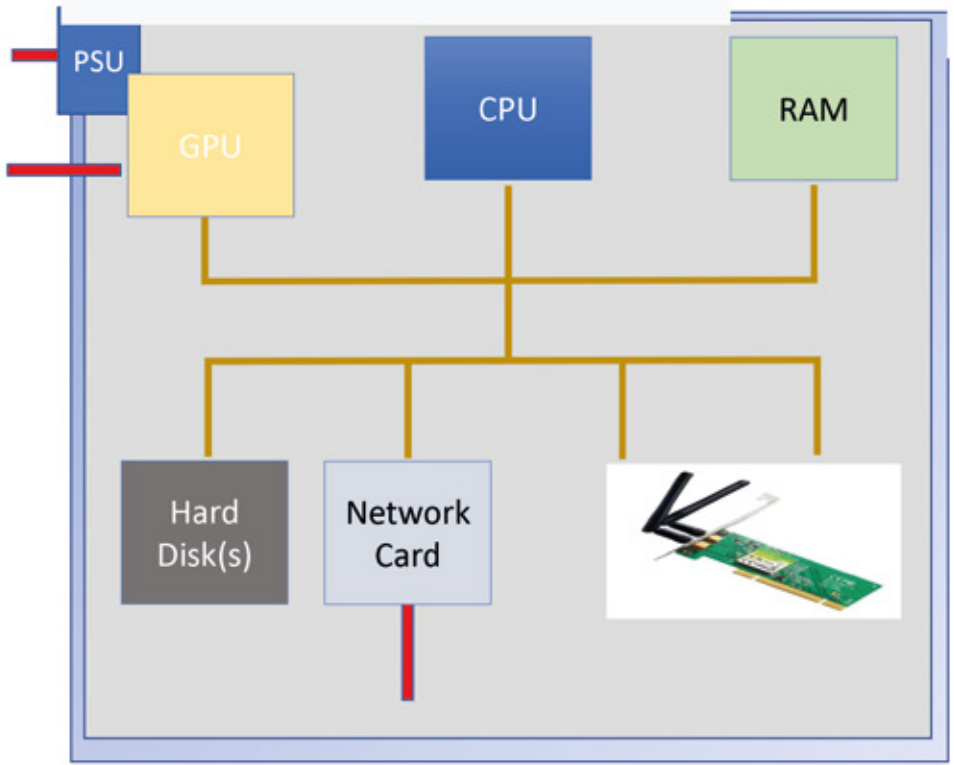


La **carte mère** est le circuit imprimé qui supporte la plupart des composants et des connecteurs nécessaires au fonctionnement d'un compatible PC.

Carte mère d’un telephone portable

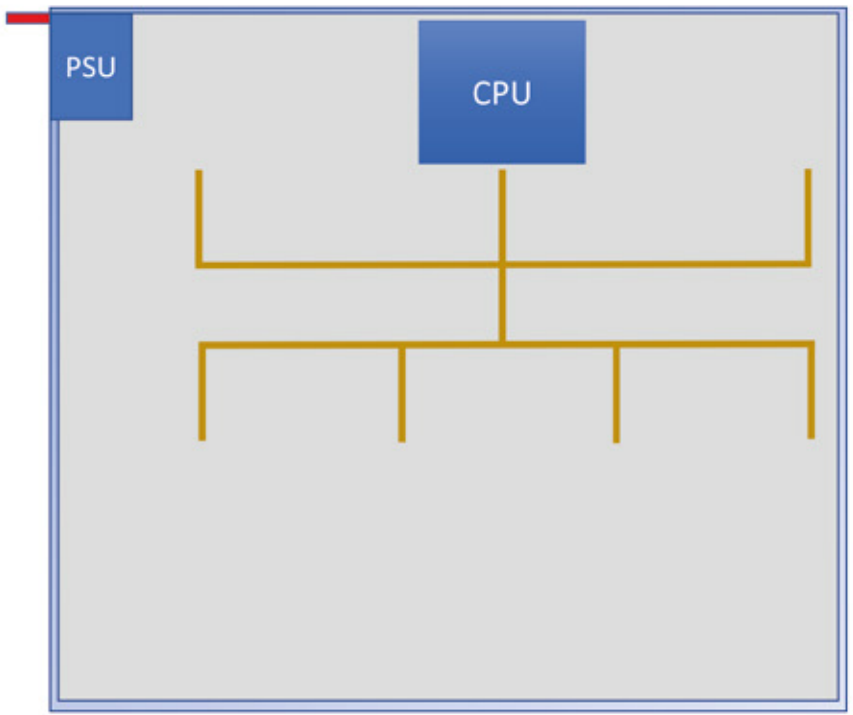


Architecture générale d'un ordinateur

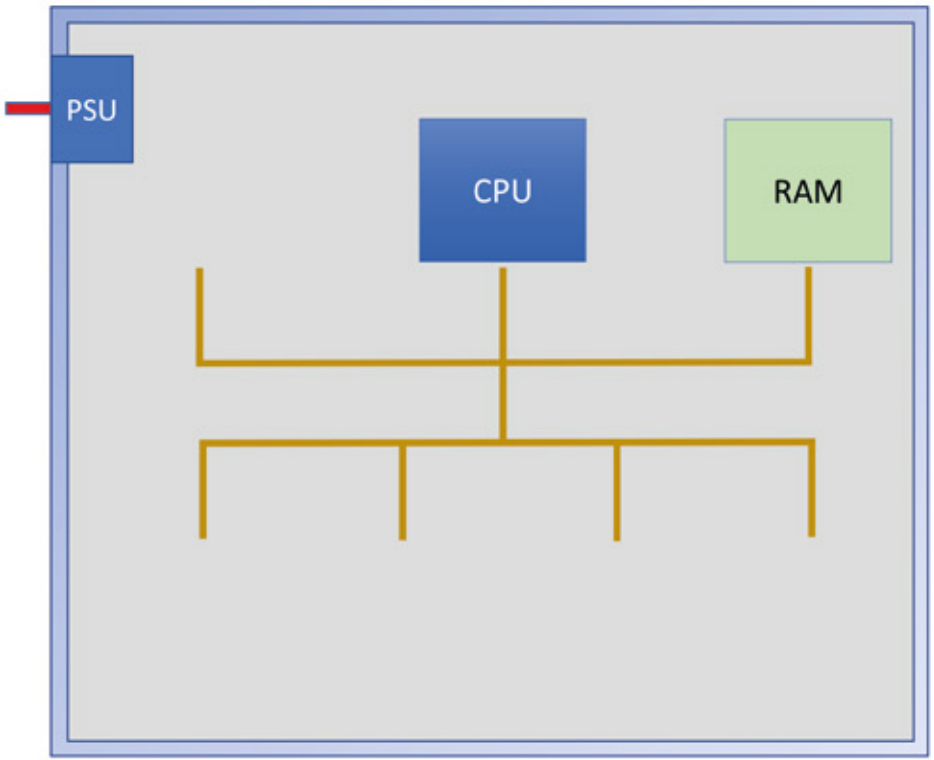


- Permet la connectivité en dehors de l'appareil
- Nécessaire pour l'accès à Internet
- Souvent appelé NIC - Network Interface Cord (ou contrôleur)
- Possède un identifiant unique - adresse MAC

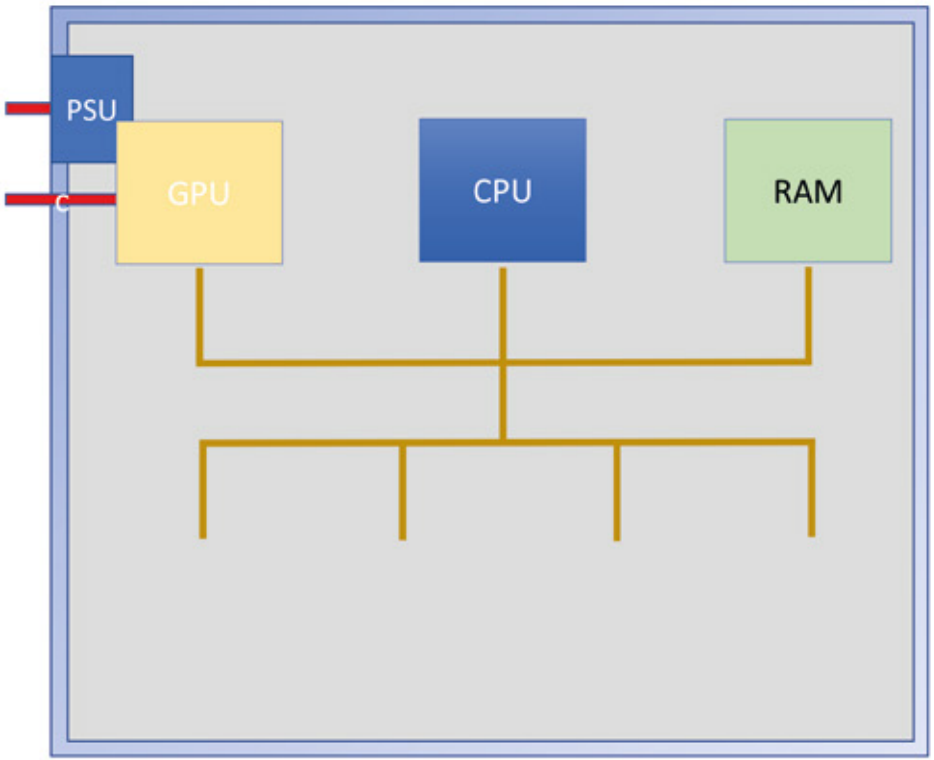
Unité centrale de traitement (CPU)



- Exécute les instructions figurant dans un programme (souvent situé dans la RAM)
- Effectue des calculs
- Traite les données
- Renvoie des données à la mémoire vive (RAM)

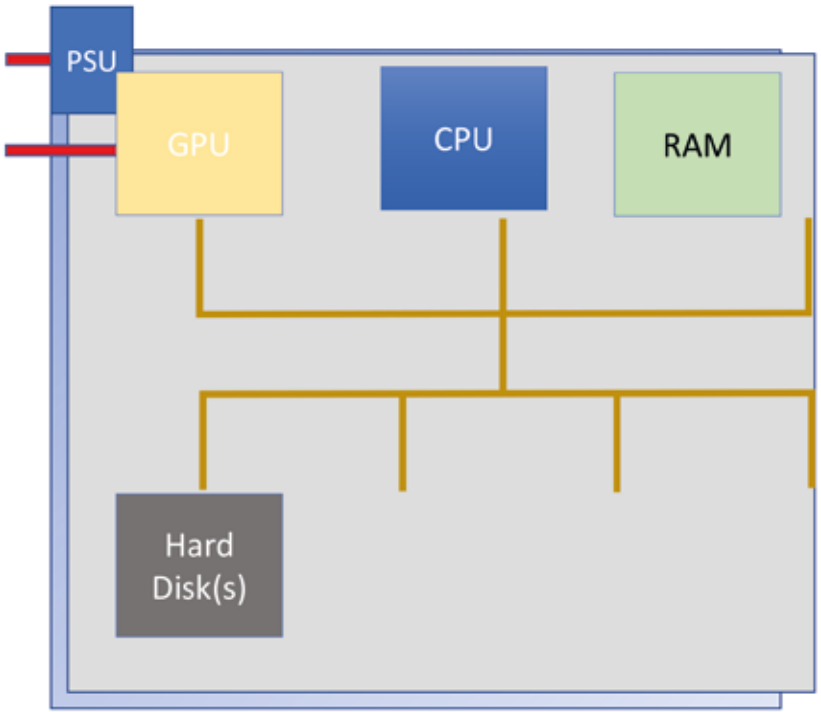


- Stockage volatile
- Le dispositif est en cours d'élaboration
- Stockage très rapide
- Fonctionne parallèlement au CPU
- Peut contenir des données utiles.



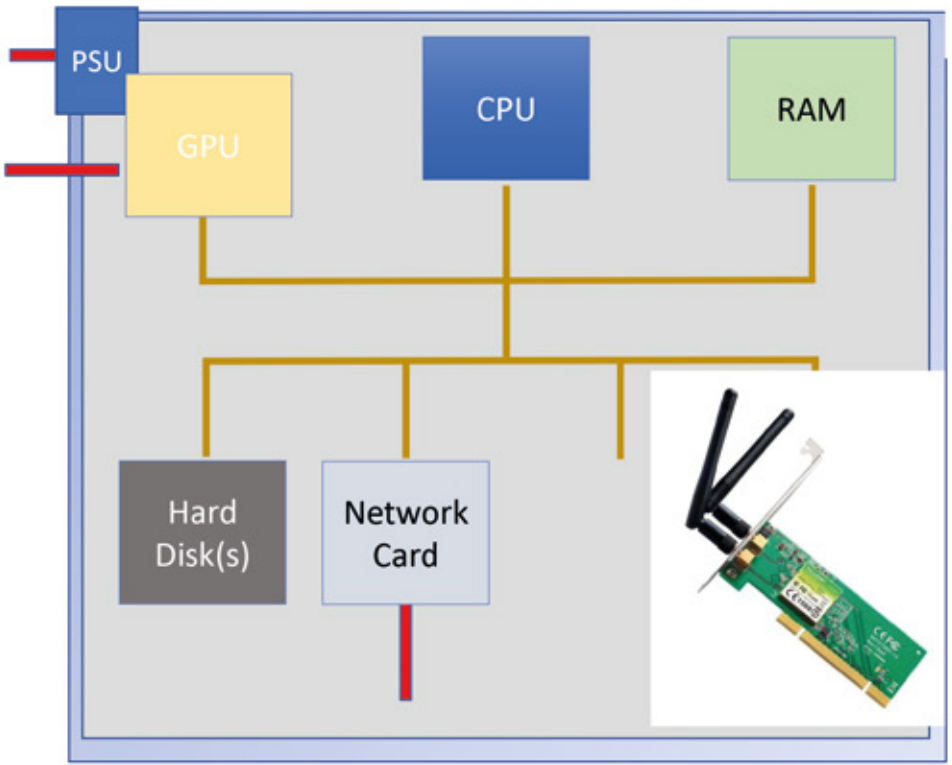
- Permet de voir/lire des informations informatiques
- Peut être intégré à la carte mère ou ajouté en tant que dispositif indépendant conçu sur mesure
- GPU - Unité de traitement des graphiques

GPU: Graphics Processing Unit (unité de traitement graphique)



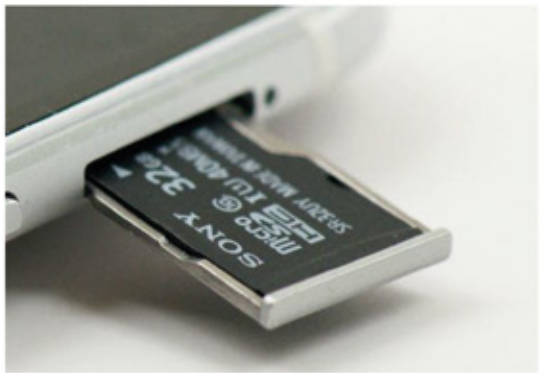
- **est une puce informatique qui effectue des calculs mathématiques rapides, principalement pour le rendu d'images.**

Carte réseau



- Permet la connectivité en dehors de l'appareil
- Nécessaire pour l'accès à Internet
- Souvent appelé NIC - Network Interface Cord (ou contrôleur)
- Possède un identifiant unique - adresse MAC

Disques



Stockage amovible

Mémoire

- La technologie des CD/DVD est toujours présente mais en diminution

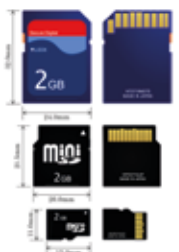
Compact Disk (CD)

Digital Video Disk (DVD)

Blu-ray Disk (BD)

- Dispositifs USB
  - Disques durs externes
  - Les clés USB

- Cartes média SD et MicroSD
  - Probablement des appareils photo et des téléphones



Fax Machine

Scanner

Printer

VR Glasses

Label Printer

Card Reader or Skimmer

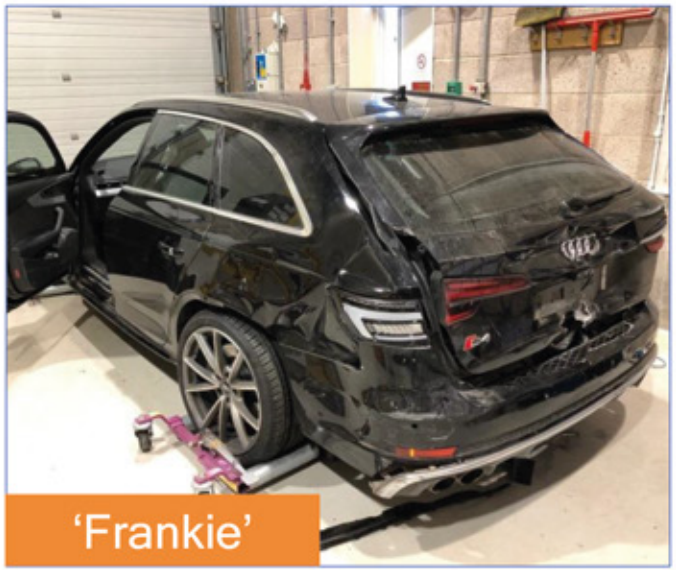
Answering Machine

GPS

Digital Cameras

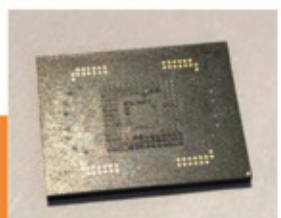
Drones

Wearables



‘Frankie’

Frankie est un système informatique



eMMC Puce Mémoire

Unité télématique qui stocke …..

Logiciel (Software)

- **L'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données**

2 principales catégories de logiciels:

- **Système d'exploitation**
- **Logiciels d'application**

- Système d'exploitation: permet au matériel de communiquer avec le logiciel installé

- Exemples: Windows, Mac, Linux, iOS, Android

July 2020

Top 10 Platforms		
1	Windows 10	21.65%
2	iOS 13	12.63%
3	Android 9	11.92%
4	Android 10	9.43%
5	Windows 7	9.19%
6	Android 8	7.76%
7	Mac OS X	6.44%
8	Android 6	4.47%
9	Android 7	4.18%
10	Android 5	2.64%

- **Logiciels d'application**
  - Productivité - suites bureautiques
  - Lecteurs et visionneurs
  - Outils d'archivage

Machine virtuelle:

- Un environnement entièrement virtualisé qui fonctionne sur une machine physique.

- Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau.

Machine virtuelle (suite)

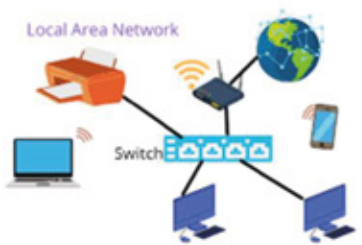
Très utilisée

- Surtout dans le domaine des affaires et du **cybercrime** !

Réseau informatique

- Un ensemble d'équipements reliés entre eux pour échanger des informations.

- Par analogie avec un filet, on appelle nœud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements.



- Chaque ordinateur d'un réseau doit avoir un **identifiant unique** pour envoyer et recevoir des données - une adresse IP
  - **Adresses IPv4**
  - 213.43.112.45
  - **Adresses IPv6**
  - 2600:1403:0002:029c:0000:0000:0000:2add
- Les IPv4 s'épuisent - les IPv6 deviennent donc plus courants

VPN: un réseau privé virtuel ou réseau virtuel privé: est un système permettant d'assurer la confidentialité des données, en créant un tunnel chiffré et en masquant l'adresse IP de l'utilisateur

C'est la méthode la plus simple et efficace pour sécuriser votre trafic internet et pour garder votre identité

Inconvénients

- Il peut, parfois, ralentir la navigation sur Internet
- Il complique le travail des enquêteurs

I- TYPOLOGIE DES INFRACTIONS NUMERIQUES

L’infraction

désigne le comportement d'une personne déterminée contraire à la loi pénale. Dans une seconde acception, plus juridique, l'infraction s'entend du comportement interdit sous la menace d'une peine définie par la loi pénale. En ce sens, l'infraction comporte deux éléments : d'une part l'incrimination, et d'autre part, la peine qui le sanctionne.

Les infractions numériques

sont entendues comme désignant toute infraction qui, d’une manière ou d’une autre, implique l’utilisation des technologies informatiques.

Le système informatique est l’objet de l’infraction : Cette catégorie d’infraction recèle toutes les atteintes contre la confidentialité, l’intégrité et la disponibilité du système informatique.

Le système informatique est le moyen de commission de l'infraction : Cette catégorie concerne les infractions ordinaires qui sont commises au moyen d'un système informatique.

Techniques de cyberattaques :

Cyberattaques reposant sur les vulnérabilités humaines :

ingénierie sociale, hameçonnage (physhing), usurpation d'identité (spoofing), arnaque aux sentiments, sextorsion.

Cyberattaques reposant sur les vulnérabilités technologiques :

exploitation d'une faille de sécurité (ou vulnérabilité), envoi de logiciel malveillant (ramsomwares), fraude à la carte bancaire (skimming)

Spécificités du Code du numérique

Le code numérique est beaucoup plus exhaustif sur les infractions que les conventions de Budapest et de Malabo que le Bénin a ratifiées. Le code ne fait pas distinction entre les délits et les crimes. La tentative de commettre l'une des infractions visées dans le code est puni des mêmes peines que l'infraction. En cas de récidive les peines prévues sont doublées.

Principales catégories d'infractions dans le Code du numérique

Les infractions sont regroupées suivant les titres :

- Atteintes aux réseaux et systèmes d'informations
- Infractions liées à l'utilisation des données à caractère personnel
- Atteinte aux personnes et aux biens
- Infractions sexuelles et prostitution
- De la fraude aux cartes bancaires
- Des autres infractions

- De l'atteinte aux droits de la propriété intellectuelle et industrielle
- Des moyens d'échanges illicites et téléchargement sur internet
- Des infractions relatives à la publicité sur Internet
- Contenus abusifs et Infraction de presse en ligne
- Infractions de droit commun commises en ligne

Les cyber délinquants utilisent le numérique pour porter atteinte soit aux **personnes** (A), soit à leurs **biens** (B).

A. Les infractions contre les personnes

Les infractions à caractère numérique touchent la personne tant dans son intégrité psychique que morale.

1. Les atteintes à l'intégrité psychique

L'intégrité psychique se définit comme un état complet de bien-être mental. Les atteintes psychiques sont des évènements qui altèrent l'intégrité psychique d'un individu.

La provocation de crime ou de délit

Elle est punie par les articles 554 et 555 du Code du numérique. Le législateur retient comme complices, ceux qui au moyen d'un ou sur un réseau de communication électronique ou un système informatique auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet. Il en est de même de l'incitation à la commission d'une infraction contre une personne qui est punie d'un (01) an d'emprisonnement et de cinq millions (5 000 000) de francs CFA d'amende (C. num. art. 555).

La menace de commettre une infraction

La menace est évoquée à l'article 549 du Code du numérique : « Quiconque profère, intentionnellement, une menace par le biais d'un système informatique, de commettre une infraction pénale telle que définie par le Code pénal, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou à un groupe de personnes qui se distingue par une de ces caractéristiques est puni d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA ».

2. Les atteintes à l'intégrité morale

Les atteintes à la vie privée

L'article 575 du Code numérique réprime l'atteinte au secret des correspondances commises sur internet : « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances émises, transmises ou reçues par la voie électronique arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni des mêmes peines que celles prévues dans les dispositions du Code pénal relatives au secret des correspondances. Est puni des mêmes peines, le fait de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions ». (art. 621 à 622). L'emprisonnement est de six (06) mois à cinq (05) ans l'amende de cent mille (100.000) francs CFA à cinq cent mille (500.000) francs

Les atteintes aux mœurs

CYBER HARCÈLEMENT

L'article 550 du Code évoque le « harcèlement par le biais d'une communication électronique ». On peut y lire : « Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement grave, répété et hostile est puni d'une peine d'emprisonnement d'un (01) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de francs CFA, ou de l'une de ces deux peines seulement. (...)

LA PORNOGRAPHIE ET LA PÉDOPORNOGRAPHIE

L'article 518 du Code numérique incrimine la pédopornographie : « Quiconque aura par le biais d'un système informatique, intentionnellement et sans droit, exposé, produit pour lui-même ou pour autrui, vendu, offert, loué, distribué, transmis, diffusé, publié ou mis à la disposition des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, la diffusion, fabriqués, détenus, importés ou fait importer, remis à un agent de transport ou de distribution, est puni de la réclusion de deux (02) ans à sept (7) ans et d'une amende de vingt millions (20 000 000) à cent millions (100 000 000) de francs CFA »

Les atteintes aux mœurs

LA PROSTITUTION DES MINEURS

Elle est incriminée par l'article 522 du Code numérique. Le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution, y compris de façon occasionnelle, est puni de vingt (20) ans d'emprisonnement et cinquante millions (50 000 000) de francs CFA d'amende lorsque la personne a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Les atteintes à l'honneur, à la considération ou à la représentation de la personne.

Art. 551. La diffusion de matériel raciste et xénophobe par le biais d'un système informatique est puni d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende d'un million (1 000 000) à dix millions (10 000 000) de francs CFA (art. 548). La même peine est retenue pour l'injure avec une motivation raciste et xénophobe commise par le biais d'un système informatique.

Art. 576. Aussi, le fait de publier sur internet, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention, est puni de cinq (5) ans d'emprisonnement et de vingt-cinq millions (25 000 000) de francs CFA d'amende

Art. 558. Enfin, une personne qui commet une infraction de presse, notamment une diffamation, une injure publique, une apologie de crime, par le biais d'un moyen de communication électronique public, est punie des mêmes peines que celles prévues par la loi n° 2015-07 du 20 mars 2015 portant Code de l'information et de la communication en vigueur (art. 270 à 273), quel qu'en soit le support.

B. Les infractions contre les biens

Les infractions à caractère numérique touchent la personne tant dans son intégrité psychique que morale.

1. Les atteintes au système numérique

- Du fait que des atteintes non autorisées peuvent causer de graves dommages et menacer la confiance dans le fonctionnement correct du système TIC, le législateur a prévu une sanction pénale pour les **atteintes aux réseaux et systèmes informatiques (C. num. béninois, art. 507 à 513)**.

- La transmission non autorisée et les modifications de données, l'effacement et la destruction de données et de logiciels, de même que le fait d'entraver l'accès au système sont des infractions types de ce que l'on pourrait appeler du « sabotage informatique » **(C. num. béninois, art. 508 et 509)**.

1. Les atteintes au système numérique

Les atteintes aux systèmes informatiques sont de plusieurs ordres :

- l'accès illégal aux données et systèmes d'information (C. num. béninois, art. 507),
- l'interception illégale des données (C. num. béninois, art. 508),
- l'atteinte à l'intégrité des systèmes (C. num. béninois, art. 509),
- l'atteinte à l'intégrité des données (C. num. béninois, art. 510),
- l'abus de dispositif (C. num. béninois, art. 511),
- la falsification informatique (C. num. béninois, art. 512),
- la fraude informatique (C. num. béninois, art. 513).

2. Les atteintes par le système numérique

La méthode usitée par les cyberdélinquants est l'arnaque. Celles-ci sont les techniques d'escroquerie, de tromperie (C. num. béninois, art. 566). Face à cela, le législateur béninois a précisé que « quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se fait remettre ou délivrer des biens et valeurs par le biais d'un système informatique ou d'un réseau de communication électronique et a par un de ces moyens, escroqué tout ou partie de la fortune d'autrui est puni d'un emprisonnement de deux (02) ans à sept (07) ans et d'une amende égale au quintuple de la valeur mise en cause sans qu'elle soit inférieure à un million (1 000 000) de francs CFA.

Des circonstances aggravantes y ont été prévues (lorsque l'escroquerie est réalisée :

- par un dépositaire de l'autorité publique ou un chargé de service public, dans l'exercice ou à l'occasion de ses fonctions ;
- par une personne qui prend indûment la qualité de dépositaire de l'autorité publique ou chargé de service public ;
- par une personne ayant fait appel au public en vue de l'émission d'actions, obligations, bons, parts ou titres quelconques soit d'une société, soit d'une entreprise commerciale ou industrielle ;
- au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits » (C. num, art. 566).

2. Les atteintes par le système numérique

Parmi les autres atteintes à la propriété, on peut citer :

le recel portant sur des données informatiques

est sanctionné par l'article 565. Il s'agit pour une personne de garder, retenir ou détenir intentionnellement en tout ou en partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit prévu par les dispositions du Code sur le numérique. Les peines sont prévues à l'article 563 du Code du numérique. Il s'agit d'un emprisonnement de cinq ans à 10 ans d'emprisonnement et d'une amende pouvant aller jusqu'à dix millions ;

le blanchiment de capitaux (C. num. , art. 573) :

le blanchiment de capitaux commis au moyen d'un ou sur un réseau de communication électronique ou un système informatique est puni conformément aux textes en vigueur. Le blanchiment de capitaux est « Un acte illégal perpétré sans le recours à la contrainte physique usant de la dissimulation ou l'artifice, afin d'obtenir de l'argent ou des propriétés, éviter un paiement ou de perte de l'argent ou pour obtenir des affaires ou des avantages personnels ».

A. Les moyens d'investigation

La spécificité des cyber infractions conduit à la mise en œuvre des techniques particulières d'investigation et à la participation d'experts dans le cadre des perquisitions (locaux, systèmes) et des saisies. Les interpellations et les auditions subséquentes quant à elles se font de manière classique.

Il convient en outre d'ajouter ici des particularités en matière de prescription, d'administration de la preuve (preuve électronique, interception de données informatiques) et d'établissement des procès-verbaux électroniques.

L'infraction

Le législateur a progressivement renforcé les moyens d'investigation particulièrement adaptés à l'univers numérique avec notamment l'autorisation d'infiltration pour tout enquêteur qui découvre des agissements susceptibles de recevoir une qualification pénale sur Internet. L'autorisation d'infiltration permet par exemple d'intervenir, de façon dissimulée, sur un forum de discussion ou sur des sites.

Régime

La mesure d'infiltration doit être préalablement autorisée par l'autorité judiciaire par écrit et spécialement motivée, mentionnant ainsi les infractions recherchées et l'identité de l'officier de police judiciaire responsable de l'opération. C'est le même régime qu'on applique en matière d'interception de communication

Renforcement du pouvoir d'investigation au profit des autorités policières et judiciaires (art 586, 587, 588, 591 594 et 635 CdN)

- Pouvoir d'injonction de produire des documents (article 586)
- Pouvoir de perquisition sans consentement (articles 587, 588)
- Pouvoir d'injonction de conserver et de protéger (article 591)
- Pouvoir d'interception de données informatisées (article 594)
- Pouvoir d'injonction de coopérer (article 635)

B. Les structures d'investigation

1) L'Office central de lutte contre la cybercriminalité (OCRC)

OCRC OFFICE CENTRAL DE RÉPRESSION DE LA CYBERCRIMINALITÉ

POLICE RÉPUBLICAINE

Le Code du numérique a créé une structure de lutte contre les infractions cybernétiques (C. num. béninois, art. 608). Cette structure est dénommée Office central de répression de la cybercriminalité (OCRC). Elle est placée sous la tutelle du ministère en charge de la sécurité publique, a une compétence nationale.

Sont associés aux activités de cet Office, le ministère en charge de la défense nationale, le ministère en charge des finances et le ministère en charge des communications électroniques. L'Office a pour domaine de compétences les infractions spécifiques à la criminalité liées aux technologies de l'information et de la communication (C. num. béninois, art. 609)

2) L'Agence nationale de la sécurité des systèmes d'information (ANSSI)

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

Dans le domaine de la cryptologie, il est créé une Agence nationale de la sécurité des systèmes d'information **« ANSSI »** (C. num. béninois, art. 604). L'Agence est en charge des missions suivantes : apporter son concours aux services de l'État en matière de sécurité des systèmes d'information et des réseaux ; effectuer un contrôle général de la sécurité des systèmes d'information et des réseaux relevant des divers organismes publics et privés identifiés par voie règlementaire ; assurer la veille technologique dans le domaine de la sécurité des systèmes d'information et des réseaux ; établir et maintenir une base de données des vulnérabilités ; diffuser des informations sur les précautions à prendre pour prévenir ou minimiser les risques d'incident ou leurs conséquences ; etc.

3) L’Agence des Systèmes d'Information et du Numérique (ASIN)

ASIN AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

L’Agence des Systèmes d'Information et du Numérique en abrégé ASIN est un établissement public à caractère social et scientifique créé par décret No 2022-324 du 1er juin 2022 portant la fusion de l'Agence de Développement du Numérique (ADN), de l'Agence des Services et Systèmes d'Information (ASSI), de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et de l'Agence Béninoise du Service Universel des Communications Électroniques et de la Poste (ABSUCEP) et approbation de ses statuts.

L’Agence des Systèmes d’Information et du Numérique a pour mission la mise en œuvre opérationnelle des projets relatifs au secteur du numérique.

4) Le Centre national d'Investigations numériques (CNIN)

CNIN CENTRE NATIONAL D'INVESTIGATIONS NUMÉRIQUES

PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

Le Conseil des Ministres en sa séance du 29 novembre 2023 a décidé de la création du Centre national d'Investigations numériques (CNIN). En effet, la nécessité impérieuse de poursuivre la lutte contre la cybercriminalité a conduit à la redéfinition des axes stratégiques implémentés jusqu'ici en vue de consolider les efforts des entités impliquées pour de meilleurs résultats.

Cette détermination s'est traduite par le recours à des technologies plus modernes, le renforcement en ressources humaines et la coordination des activités opérationnelles. En décidant de créer une structure unique constituée de multiples compétences, le gouvernement se fixe comme objectif l'efficacité plus affichée dans toutes les investigations liées à l'usage des nouvelles technologies.

Ainsi, le Centre national d'Investigations numériques (CNIN) reprendra les attributions les attributions de l'Office central de Répression de la Cybercriminalité (OCRC) et disposera de missions plus élargies absorbant partiellement celles de l'Agence des Systèmes d'Information et du Numérique (ASIN) relatives à la cybercriminalité.

C. La responsabilité des acteurs de l'internet

Article 497: Responsabilité des Fournisseurs de Service en Ligne

Les fournisseurs de services en ligne ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de leurs services, s'ils n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

Art. 495: Obligation de conservation de données

Les fournisseurs de services en ligne détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires.

Article 500 : Obligation de coopération à la lutte contre la cybercriminalité

Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, les opérateurs fournissant un accès à internet et les fournisseurs de services en ligne doivent concourir à la lutte contre les infractions visées au présent Livre.

Article 499 : Absence d'obligation générale de surveillance

Les opérateurs fournissant un accès à internet et les fournisseurs de services en ligne ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites. Ils sont toutefois tenus à l'obligation de vigilance prévue à l'article 377 du présent code.

Art. 495: Obligation de conservation de données

Les fournisseurs de services en ligne détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires.

D. Les difficultés techniques

1) Anonymat

L' identification de l'auteur d'infraction sur les réseaux sociaux peut être difficile dans la mesure où les réseaux sociaux offre à leurs utilisateurs, la possibilité de s'inscrire sous un pseudonyme. Dans certains cas, rien ne garantit que l'identité associée au compte à l'origine du contenu litigieux soit réellement celle de la personne à l'origine du contenu.

2) Localisation

L'utilisation d'un ordinateur en accès public, avec des connexions « Wi Fi » ou celle d'un « Anomyser » rendent toute localisation de preuve difficile, incertaine ou impossible. La localisation de la preuve devient difficile lorsque l'auteur de l'atteinte se retrouve sur le territoire d'un autre Etat que celui où le préjudice a été subi, ou lorsqu'elle se situe dans le "cloud computing", c'est-à-dire dans le nuage.

3) Volatilité

Il existe sur les réseaux sociaux un risque constant de voir disparaître l'élément incriminé quelque temps seulement après sa publication. Lorsque la preuve n'est pas recueillie avant cette suppression, il peut être difficile pour la victime ou l'enquêteur de rapporter la preuve de l'infraction. La sauvegarde de la preuve est donc une question d'urgence

4) Fiabilité

Des contestations peuvent être élevées relativement aux preuves numériques lorsqu'elles ne sont pas recueillies dans des conditions garantissant la fiabilité. C'est la raison pour laquelle les seules preuves fiables sont celles administrées par un agent assermenté.

5) Cryptographie

La cryptographie encore appelée le chiffrement, est une opération de transformation des données visant à les rendre inintelligibles à toute personne autre que le possesseur de la clé de chiffrement. Dans une enquête pénale, lorsque les enquêteurs sont confrontés à des appareils cryptés par les suspects qui refusent de leur communiquer le code de décryptage, cela devient un défi pour l'enquête.

6) Volume des données

Le nombre de documents numériques croit constamment du fait de leur faible cout de stockage. L'augmentation de la taille maximale des disques durs entraînent parallèlement l'augmentation du nombre de fichiers à décortiquer. Ainsi, les preuves des actes délictuels se retrouvent dans un grand flux de données qui rende l'obtention et la recherche de la preuve très difficile.

7) Dépendance des algorithmes

La preuve numérique repose sur des algorithmes complexes et sensibles aux erreurs. Si ces algorithmes contiennent des bugs ou sont manipulés, la fiabilité de l'ensemble de la preuve est compromise.

8) Recours aux tiers

Les opérateurs de réseaux sociaux n'ont pas de représentation légale sur le territoire béninois, ce qui pose des difficultés en termes d'échange avec eux. Les plateformes de services et serveurs sont généralement situés à l'étranger et dans des endroits gardés confidentiels. Ainsi, les données sauvegardées sont détenues en tout ou partie dans différents pays du monde. Or, lorsqu'il est avéré que le système informatique en cause est situé à l'étranger, la perquisition s'avère impossible.

JULIEN HOUNKPE
DOCTEUR EN DROIT

+229 95 88 79 25

julien coomlan hounkpe

julienhounkpe@gmail.com

www.julienhounkpe.com