ANSSI

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

CÔTE D'IVOIRE

RAPPORT 2024 SUR L'ETAT DE LA CYBERCRIMINALITE EN CÔTE D'IVOIRE

RÉPUBLIQUE DE CÔTE D'IVOIRE

MINISTÈRE DE L'INTÉRIEUR ET DE LA SÉCURITÉ

MINISTÈRE DE LA TRANSITION NUMERIQUE ET DE LA DIGITALISATION

PLCC Plateforme de Lutte contre la Cybercriminalité ANSSI CÔTE D'IVOIRE

CI-CERT COMPUTER EMERGENCY RESPONSE TEAM ANSSI CÔTE D'IVOIRE

CFAD ANSSI CÔTE D'IVOIRE

SOC - Security Operation Center

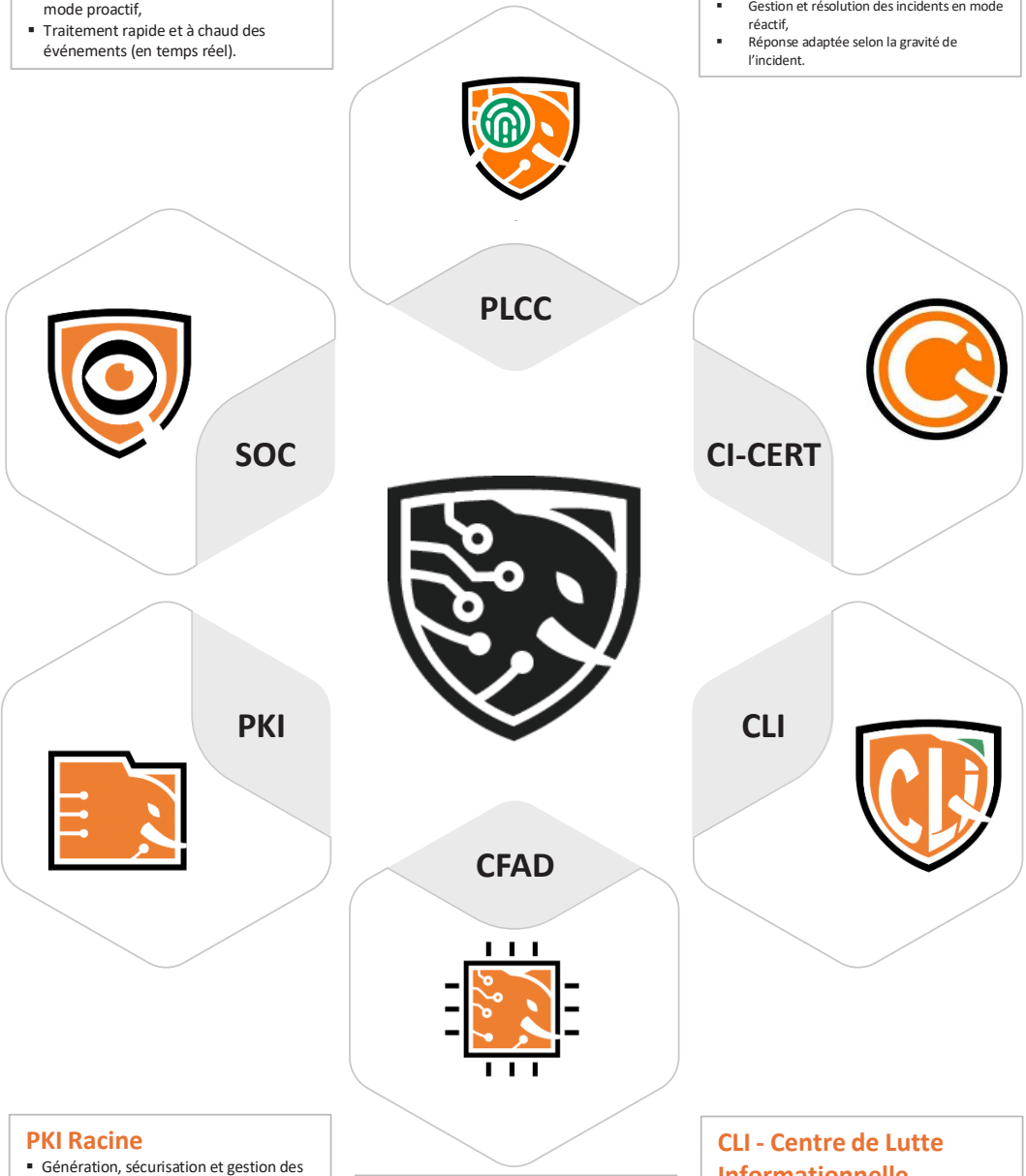
- Surveillance et protection en temps réel des actifs, informatiques de l'ANSSI et d'organismes tiers,
- Surveillance continue et rapidité de réponse,
- Détection et prévention des menaces en mode proactif,
- Traitement rapide et à chaud des événements (en temps réel).

PLCC - Plateforme de Lutte Contre la Cybercriminalité

- Réception de plaintes,
- Assistance aux victimes,
- Enquêtes de cybercriminalité,
- Coopération judiciaire internationale.

CI-CERT - Côte d'Ivoire Computer Emergency Response Team

- Gestion et réponse aux incidents majeurs ou critiques, au national ou sectoriel, pour plusieurs entités,
- Coordination de la réponse, collaboration et analyse approfondie,
- Gestion et résolution des incidents en mode réactif,
- Réponse adaptée selon la gravité de l'incident.



PKI Racine

- Génération, sécurisation et gestion des clés racines,
- Émission et révocation de certificats des autorités de certification subordonnées,
- Conformité aux normes, journalisation et audit des opérations (émission, révocation, etc.),
- Protections (physique et logique),
- Plan de continuité et de reprise.

CFAD - Centre de Fusion et d'Analyse de Données

- Collecte de données d'investigation,
- Laboratoire de digital forensic,
- Analyse et valorisation de données,
- Activités au profit de services requérants (non exclusifs au secteur de la sécurité/défense/renseignement).

CLI - Centre de Lutte Informationnelle

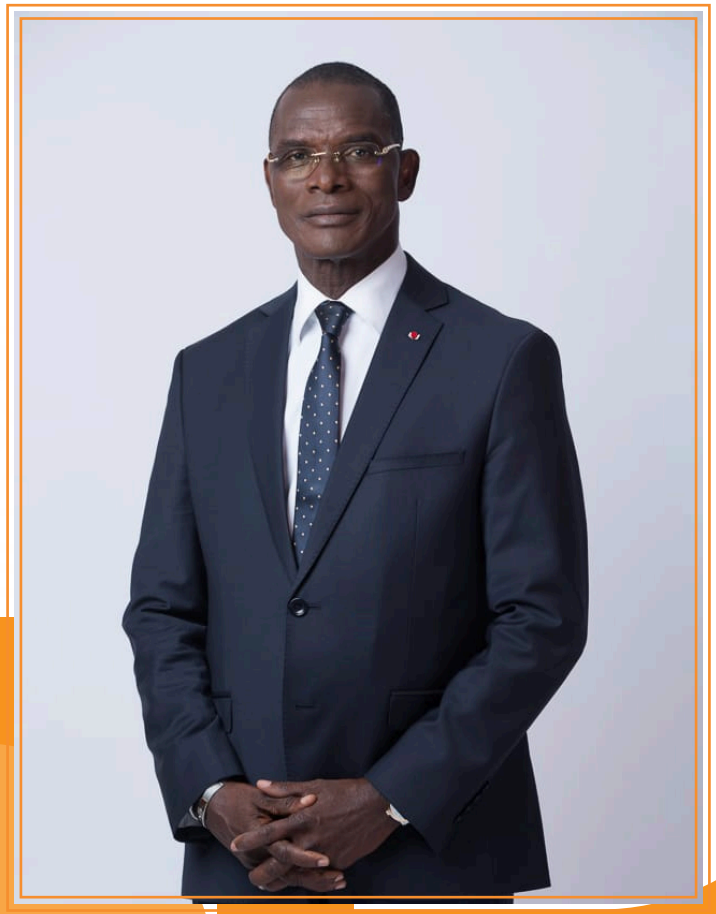
- Surveillance en temps réel des réseaux sociaux,
- Détection de propagandes et autres agressions informationnelles,
- Réponse structurée à aux propagandes et autres agressions informationnelles,
- Communication digitale d'influence.

Alertes 100

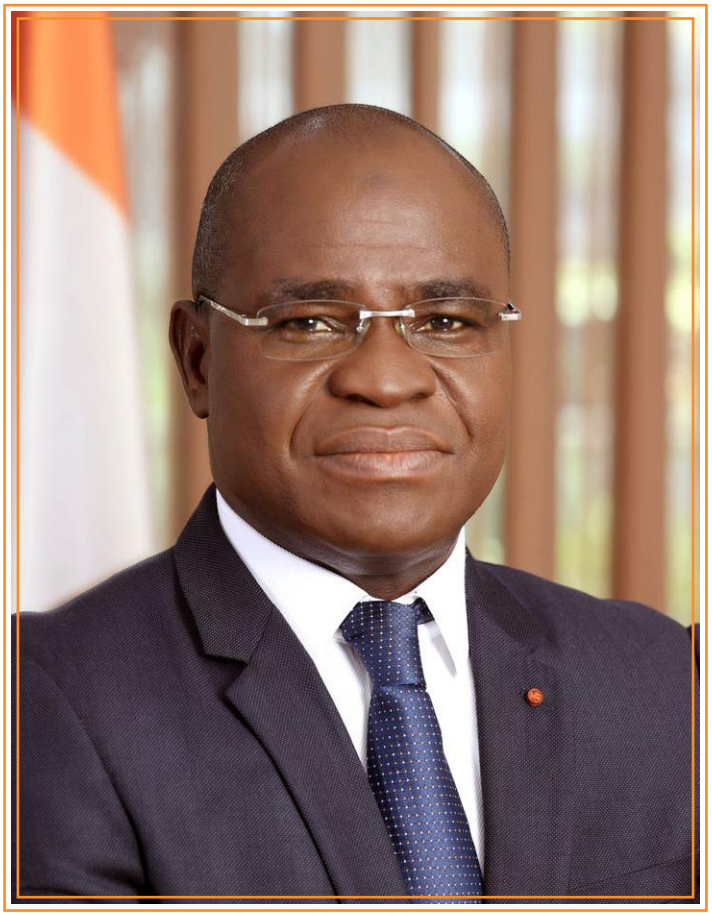
- Centre d'appel d'urgence (100),
- Centre de vidéo protection urbaine,
- Vidéo analytique,
- Monitoring des réseaux sociaux,
- fact checking.

Centre de Formation

- Cadre légal et règlementaire ivoirien,
- Procédures d'agrément et de certification,
- Procédure pénale de la cybercriminalité,
- Connaissance de l'ANSSI,
- Formation RSSI, etc.



Général de Corps d'Armée Vagondo DIOMANDE,
Ministre de l'Intérieur et de la Sécurité



Ibrahim Kalil KONATE,
Ministre de la Transition Numérique et de la Digitalisation

Général de Corps d'Armée Philippe MANGOU,
Président du Conseil de Surveillance de l'ANSSI

Colonel Major Guelpetchin OUATTARA,
Directeur Général ANSSI

Wilfried Elie KONAN,
Directeur Général Adjoint ANSSI

Le Sommet mondial sur la société de l'information (SMSI) ainsi que la Conférence des plénipotentiaires de l'Union Internationale des Télécommunications (UIT) tenue en 2006, ont fortement recommandé à l'UIT, de promouvoir la confiance et la sécurité dans l'utilisation des communications électroniques. En réponse, l'UIT encourage depuis ses États membres à adopter des mesures concrètes en vue de réduire l'impact des cybermenaces et de l'insécurité liée à l'accès et à l'usage des médias numériques, tant pour les populations que pour les entreprises, publiques comme privées.
Face à l'accélération des évolutions technologiques et à leurs corollaires – à savoir les usages illicites, les dysfonctionnements et les vulnérabilités – le gouvernement ivoirien a rapidement pris des mesures pour garantir la sécurité numérique des individus et des organisations.

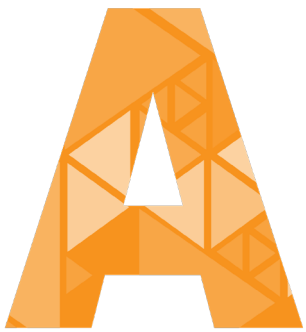
Dès 2007, la Direction de l'Informatique et des Traces Technologiques (DITT) a été créée afin de prendre en charge les enjeux liés aux technologies numériques et à la cybersécurité. Complètement opérationnelle à partir de 2011, la DITT s'est vu confier plusieurs missions majeures, à savoir (1) la lutte contre la cybercriminalité, (2) le conseil et l'assistance en matière de cybersécurité, (3) le soutien aux enquêtes et aux opérations de sécurité, (4) la conduite de projets technologiques à destination du secteur sécuritaire.
Une seconde réponse institutionnelle a été apportée en 2020 avec la mise en place, au sein de l'Autorité de Régulation des Communications électroniques et des TIC (ARTCI), du Centre National de Réponse aux Incidents Informatiques, dénommé CI-CERT (Côte d'Ivoire Computer Emergency Response Team).

Malgré des résultats techniques probants et un cadre juridique qui donne effectivement des outils de prévention, de sécurisation du cyberespace et de répression, les transformations numériques et le développement de services toujours innovants complexifient la donne et font émerger de nouveaux challenges sécuritaires. C'est dans ce contexte que le Gouvernement a adopté, 22 décembre 2021, la Stratégie Nationale de Cybersécurité 2021-2025, prévoyant dans ses principales orientations, la création d'une Agence nationale dédiée à la cybersécurité.

En application de cette mesure stratégique, le Conseil des Ministres du 30 octobre 2024 a adopté par décret n°2024-958 du 30 octobre 2024, la création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). L'ANSSI reprend les missions de la DITT et celles de l'ARTCI en matière de cybersécurité (y compris le CI-CERT) et de confiance numérique en partie. Dès les premières phases de son opérationnalisation, l'Agence a à cœur d'opérer une fusion parfaite des services existants et une communication redynamisée sur l'ensemble de son spectre.

Afin de donner une clarté à son action, l'ANSSI met à la disposition des acteurs impliqués et du grand public, l'état des lieux de la cybercriminalité en 2024. Le cadre légal en Côte d'Ivoire, les infractions et modes opératoires usuels, ainsi que les acteurs institutionnels sont présentés. Les chiffres clés de 2024 sont confrontés aux tendances 2022 et 2023, pour mesurer les transformations qui s'opèrent en matière de cybercriminalité. Nous souhaitons qu'à la fin de la lecture, chacun ait une connaissance des acteurs et une image fidèle du niveau de la cybercriminalité en Côte d'Ivoire en 2024.

COLONEL MAJOR
GUELPETCHIN **OUATTARA**
DIRECTEUR GÉNÉRAL ANSSI



QU'EST-CE QUE LA CYBERCRIMINALITÉ EN CÔTE D'IVOIRE ?

A.1 CADRE JURIDIQUE

A.1.1 CADRE LÉGAL DE LA CYBERCRIMINALITÉ

Le cadre juridique et règlementaire de la cybersécurité et de la lutte contre la cybercriminalité comprend des lois, une ordonnance et des décrets. Ces textes sont accompagnés de Conventions Internationales auxquelles la Côte d'Ivoire a adhéré en matière de coopération internationale, et de la Stratégie Nationale de la Cybersécurité 2021-2025.

A.1.1.1 AU TITRE DES LOIS

Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.
Cette loi fixe le cadre juridique de la protection des données à caractère personnel afin de garantir une protection globale de la confidentialité des données personnelles des utilisateurs, de leurs droits et libertés fondamentaux.

Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, modifiée en ses articles 17, 33, 58, 60, 62 et 66 par la loi n°2023-593 du 07 juin 2023.
Cette loi définit les infractions spécifiques aux communications électroniques, notamment les atteintes aux systèmes informatiques, les atteintes aux systèmes de cryptologie et les atteintes aux systèmes automatisés des données. Elle renforce également les sanctions et peines encourues en cas de violation.

Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques.
Cette loi régit le commerce électronique, notamment la conclusion des contrats par voie électronique. Elle règlemente également l'archivage électronique, la sécurisation des transactions électroniques ainsi que la cryptologie.

Loi n°2019-574 du 26 juin 2019 portant code pénal modifié par la loi n°2021-893 du 21 décembre 2021.
L'article premier de la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, définit la cybercriminalité comme l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou un système d'information.
Les modifications de décembre 2021 introduisent des infractions spécifiques au cyberespace.

A.1.1.2 AU TITRE DES ORDONNANCES

Ordonnance n°2024-950 du 30 octobre 2024 portant modification des articles 3 et 17 de l'ordonnance n°2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives et abrogation de l'article 50 de loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques.
Cette ordonnance a remplacé les mentions de l'ARTCI par « l'organisme compétent » en ses articles 3 et 17 et a abrogé l'article 50 de la loi relative aux transactions électroniques, dans le but de renforcer la coordination en matière de cybersécurité, en confiant à un organisme dédié la protection des systèmes d'information et des transactions électroniques. Les changements ainsi opérés par cette ordonnance ont permis la création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) par décret n°2024-958 du 30 octobre 2024.

Ordonnance n° 2017-500 du 02 août 2017 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
Elle qui prévoit la mise en place, par décret, d'un ensemble de référentiels portant notamment sur la sécurité des données échangées par voie électronique ;

A.1.1.3 AU TITRE DES DÉCRETS

Décret n° 2014-105 du 12 mars 2014 portant définition des conditions de fourniture des prestations de cryptologie.

Décret n° 2014-106 du 12 mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique.

Décret n° 2015-78 du 4 février 2015 portant gestion du domaine internet de premier niveau de la Côte d'Ivoire «.ci »

Décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique.

Décret n°2017-193 du 22 mars 2017 portant identification des abonnés des services de télécommunications/TIC ouverts au public et des utilisateurs des cybercafés.

Décret n° 2020-128 du 29 Janvier 2020 portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique (CI-CERT).

Décret n° 2021-911 du 22 décembre 2021 portant adoption du cadre commun d'architecture de référentiel de données.

Décret n° 2021-912 du 22 décembre 2021 portant adoption du Cadre Commun d'Urbanisation des Systèmes d'Information de l'État.

Décret n° 2021-913 du 22 décembre 2021 portant adoption du Référentiel Général d'Interopérabilité des Systèmes d'Information.

Décret n° 2021-914 du 22 décembre 2021 fixant les règles pour la conception, la réalisation et la gouvernance des projets publics d'infrastructures, d'équipements et de plateformes de services numériques. Ce décret comprend deux annexes qui sont :

- Référentiel Général de Sécurité des Systèmes d'Information.
- Plan de Protection des Infrastructures Critiques.

Décret n°2021-918 du 22 décembre 2021 instituant un département en charge des systèmes d'information au sein des ministères.

A.1.2 ACTES COMMUNAUTAIRES

Convention de Malabo du 27 juin 2014 : qui vise à créer un cadre juridique sous-régional, régional et international sur la sécurité et la protection des données à caractère personnel et défini les engagements des États membres de l'Union Africaine, en vue de l'édification de la société de l'information. L'adhésion de la Côte d'Ivoire à cette Convention a été ratifiée le 3 avril 2023.

Acte additionnel relatif à la protection des données à caractère personnel dans l'espace CEDEAO adopté à Abuja le 16 février 2010 : qui vise à encourager les États membres à mettre en place un cadre légal de la protection de la vie privée et professionnelle liée à la collecte, au traitement et à la transmission, au stockage et à l'usage des données à caractère personnel sous réserve de la protection de l'ordre public.

Directive portant lutte contre la cybercriminalité dans l'espace CEDEAO adoptée les 17 et 19 août 2011 à Abuja : qui a pour objet d'adapter le droit pénal de fond et la procédure pénale des États membres de la CEDEAO au phénomène de la Cybercriminalité.

A.1.3 CONVENTIONS INTERNATIONALES

Convention de Budapest du 23 novembre 2001 : vise à établir un cadre de coopération entre les États parties à la Convention dans le but de mener une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale. L'adhésion de la Côte d'Ivoire à cette Convention a été ratifiée le 29 juillet 2024.

A.2 ACTEURS

A.2.1 AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

Compte tenu du contexte national et mondial marqué par l'accroissement des actes de cybercriminalité et la complexification croissante des cybermenaces, le Gouvernement ivoirien a adopté une posture proactive et stratégique. C'est ainsi qu'a été créée, par décret n° 2024-958 du 30 octobre 2024, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), incarnant une réponse structurelle, urgente et coordonnée à ces enjeux critiques Pour accomplir efficacement ses missions, l'ANSSI s'est dotée de plusieurs centres techniques spécialisés, dont certains sont spécifiquement dédiés à la lutte contre la cy bercriminalité, ou y contribuent de manière significative :

La PLCC : Plateforme de Lutte Contre la Cybercriminalité,
Le CI-CERT : Côte d'Ivoire Computer Emergency Response Team,
Le CFAD : Centre de Fusion et d'Analyse de Données ;
Les acteurs de la Procédure Pénale.

A.2.2 PLATEFORME DE LUTTE CONTRE LA CYBERCRIMINALITÉ (PLCC)

En Côte d'Ivoire, les activités de lutte contre la cybercriminalité sont conduites par la PLCC. De 2011 à 2024, la PLCC a été le fruit d'une convention de partenariat entre l'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) et la Direction Générale de la Police Nationale (DGPN). Conformément au décret n°2024-958 du 30 Octobre 2024, l'ANSSI reprend désormais les missions de la DITT. Par conséquent, la PLCC qui était initialement abritée à la DITT, devient un département à part entière de l'ANSSI.

La PLCC mène ses actions sous deux angles à savoir la prévention et la répression

Au niveau de la prévention, la PLCC assiste et conseille le grand public, les entreprises et les victimes.

Au niveau de la répression, la PLCC pose tous les actes de Police Judiciaire en conformité avec le code de procédure pénale, le code pénal, et les textes en vigueur en matière de cybercriminalité et de protection de données à caractère personnel. Elle reçoit des plaintes ou s'auto saisit, constate les infractions, recherche les suspects et les met à la disposition des Parquets.

Pour ses activités d'investigation et de répression, la PLCC travaille en collaboration avec le Centre de Fusion et d'Analyse de Données (CFAD). Quant aux activités préventives elles sont menées en collaboration avec la Direction de la Communication et de la Sensibilisation, et le Centre de Formation de l'ANSSI. Par ailleurs, la PLCC collabore avec des partenaires externes tels que :

- La Police et la Gendarmerie pour les plaintes de cybercriminalité reçues hors de la ville d'Abidjan ;
- Les services étrangers pour d'une part les plaintes reçues hors de la Côte d'Ivoire et ayant un lien avec notre pays et d'autre part les suspects recherchés par la PLCC sur leur territoire ;
- La Cellule Nationale de Traitement des Informations Financières (CENTIF) pour la poursuite des investigations sur le volet blanchiment de capitaux d'origine cybercriminelle.

La PLCC est composée des services de plaintes et d'assistance aux victimes, d'enquêtes spécialisées (atteinte à la dignité, fraude sur transaction électronique, investigations techniques) et de coopération policière internationale.

A.2.3 CÔTE D'IVOIRE COMPUTER EMERGENCY RESPONSE TEAM (CI-CERT)

Créé par le décret n°2020-128 du 29 janvier 2020, le CI-CERT est devenu un département de l'ANSSI depuis octobre 2024. Son rôle est de répondre aux incidents de cybersécurité déclarés par les victimes ou identifiés par le SOC, de coordonner la réponse et proposer des solutions de remédiation. Au quotidien, le CI-CERT documente les vulnérabilités, partage les informations, sensibilise des entreprises et effectue des recherches en matière de cybersécurité. Moins orienté sur la surveillance en temps réel, il intervient donc après la détection d'un incident. Lorsque ces incidents ont un caractère intentionnel ou criminel, le CI-CERT collabore avec la PLCC comme acteur technique d'investigation.

A.2.4 CENTRE DE FUSION ET D'ANALYSE DE DONNÉES (CFAD)

L'article 1er de la loi relative à la lutte contre la cybercriminalité définit la cybercriminalité comme étant « l'ensemble des infractions pénales qui se commettent au moyen ou sur un réseau de télécommunication ou un système d'information ». À l'ère de la généralisation de l'usage des outils numériques au quotidien, il est quasi impossible de trouver des infractions ne faisant pas intervenir les technologies. Se pose la difficulté de faire la part entre les infractions qui sont du ressort exclusif des entités de lutte contre la cybercriminalité, et celles qui relèvent des services d'investigations classiques. C'est pour répondre à cette difficulté qu'il a été mis en place le CFAD. Il a pour rôle de mutualiser les capacités d'investigations cyber permettant de soutenir tant les affaires de cybercriminalité que celles d'ordre général nécessitant des recherches techniques (grand banditisme, trafics de drogue, crimes économiques, trouble à l'ordre public, etc.). Ce choix permet à la Côte d'Ivoire d'impacter positivement l'ensemble du secteur de la sécurité.

Les missions du CFAD sont de collecter et traiter les données, analyser les informations et produire des rapports au profit des services d'investigations : PLCC, Police, Gendarmerie, CENTIF, Parquet, Juges d'instruction, etc. Le CFAD est constitué des services de traitement de données, d'analyse criminelle, de coopération et de gestion des réquisitions judiciaires (relation opérateurs privés du digital) et d'un laboratoire de criminalistique numérique (digital forensic lab).

A.2.5 ACTEURS ET ACTES DE PROCÉDURE PÉNALE

L'ANSSI prend en charge les plaintes en matière de cybercriminalité et enquête dans le respect de code de procédure pénale. Avec ses Officiers et Agents de Police Judiciaire (OPJ et APJ), l'Agence pose l'ensemble des actes de Police Judiciaire pour constater les infractions de cybercriminalité, en rechercher les auteurs, et rassembler les preuves.

Au titre de la phase de constatation et d'enquête, l'ANSSI peut procéder via la PLCC par :

- Enquête de flagrance ou préliminaire,
- Auditions de victimes, de témoins ou des suspects,
- Garde à vue de suspects,
- Interpellations / Arrestations,
- Rédaction de procès-verbaux (PV) et comptes rendu officiels d'actes accomplis, Transmissions de dossier aux autorités judiciaires compétentes (procureur ou juge d'instruction).

Au titre du recueil des preuves numériques, les experts et agents assermentés de l'ANSSI sont compétents pour procéder auprès des personnes morales ou physiques impliquées :

- Saisie de matériel informatique (ordinateurs, serveurs, supports de stockage, etc.),
- Réquisition de données de trafic ou d'identification auprès des fournisseurs de services digitaux et d'accès internet, et des opérateurs de télécommunications,
- Perquisition de systèmes informatiques dans le respect des règles de procédure,
- Exploitation des journaux de logs et autres traces numériques,
- Perquisitions et saisies d'objets utiles à l'enquête (documents, équipements, etc.),
- Etc.

Au titre des activités de police technique et scientifique l'ANSSI peut collaborer avec plusieurs structures de l'État dans la constatation de faits et la collecte de preuves numériques diverses. Dans ce cadre l'Agence apporte son appui aux OPJ, aux auxiliaires, aux services de police judiciaire, et à ceux en charge de la police administrative, pourvu que l'expertise technique de l'ANSSI, notamment en criminalistique numérique et en analyse de données de masse, soit formellement requise. Ces soutiens et interactions se font dans le cadre strict des textes en vigueur.

A.3 TYPES D'AFFAIRES ET REFERENCES LEGALES

ATTEINTE A LA DIGNITE HUMAINE
(FACILITÉ PAR UN SYSTÈME D'INFORMATION)
Code pénal (articles 450-3, 450-4 et 450-5)
6 mois à 5 ans d'emprisonnement et 1.000.000 à 6.000.000 FCFA d'amende

Exemple : Un individu obtient illégalement des photos ou vidéos intimes d'un tiers, par exemple en piratant son téléphone ou en utilisant une technique de manipulation. Cet individu menace ensuite la victime de publier ces images sur les réseaux sociaux ou d'autres plateformes en ligne, à moins que celle-ci ne lui accorde un avantage, tel qu'une somme d'argent ou une faveur.

UNE RELATION AMOUREUSE QUI VIRE AU CHANTAGE

L'obtention frauduleuse d'images intimes d'une personne suivie de menaces de les diffuser en ligne contre de l'argent constitue un chantage à la vidéo. En vertu de l'article 66 de la loi N° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, le coupable risque une peine d'emprisonnement allant de cinq à dix ans et une amende de 5.000.000 à 20.000.000 Francs CFA. La victime a la possibilité de porter plainte auprès de la Plateforme de Lutte Contre la Cybercriminalité (PLCC) pour obtenir un soutien technique et psychologique.

EM a rencontré NH sur le réseau social Badoo, débutant ainsi une relation amoureuse. Après quelques mois, NH a sollicité financièrement EM, qui a répondu favorablement en lui envoyant 500.000 Francs CFA...
suite page 63

ATTEINTE À L'HONNEUR ET À L'IMAGE
(FACILITÉ PAR UN SYSTÈME D'INFORMATION)
Code pénal (article 367) Loi n°2013-451 du 19 Juin 2013
relative à la lutte contre la cybercriminalité (article 60)
1 à 5 ans d'emprisonnement et 5.000.000 à 10.000.000 FCFA d'amende

Exemples :
Injures ou propos outrageants : Un individu poste sur les réseaux sociaux des commentaires méprisants et insultants à l'encontre d'un tiers, par exemple en le qualifiant publiquement de "menteur" ou de "faible" sans qu'aucun fait ne vienne justifier ces propos. Ces injures visent à rabaisser et à nuire à l'honneur de la personne visée.
Diffamation : Un internaute publie sur un forum ou un blog des informations fausses et nuisibles à l'encontre d'une autre personne, l'accusant d'un délit qu'elle n'a pas commis, comme de la fraude ou du harcèlement. Ces accusations, bien qu'infondées, peuvent gravement affecter la réputation de la personne accusée.
Publication de données à caractère personnel : Un individu partage sur internet, sans consentement, des informations privées d'une autre personne, telles que son adresse personnelle, ses informations financières ou des photos privées, dans le but de nuire à sa réputation ou de l'humilier publiquement.

QUAND LA LIBERTÉ D'EXPRESSION DÉPASSE LES LIMITES

La liberté d'expression est un droit fondamental reconnu par la Déclaration universelle des droits de l'homme. Toutefois, elle comporte des limites, notamment lorsqu'elle porte atteinte à la dignité d'autrui. Avec l'essor des réseaux sociaux, on observe une augmentation des propos diffamatoires, souvent justifiés à tort par la liberté d'expression.

L'histoire de DN, une figure culturelle respectée, illustre cette problématique. Victime de fausses accusations sur Facebook, il a vu sa réputation et celle de sa famille mises en péril. En réponse, il a porté plainte auprès de la Plateforme de Lutte Contre la Cybercriminalité (PLCC)...**suite page 65**

ESCROQUERIE SUR INTERNET (FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (article 471)
1 à 5 ans d'emprisonnement et 300.000 à 3.000.000 FCFA d'amende.

Exemples :
Fausse vente en ligne : Un individu crée une fausse annonce de vente en ligne d'un produit populaire, à un prix très attractif. Un internaute intéressé par l'achat paie en avance, mais ne reçoit pas le produit promis. Après avoir effectué le paiement, l'arnaqueur coupe toute communication et disparaît, laissant la victime sans recours.

Fausse bourse en ligne : Un individu met en ligne une fausse annonce de bourse d'études ou de promesse d'emploi, dans laquelle la victime est incitée à verser une somme d'argent pour "finaliser" sa candidature ou "débloquer" des fonds, mais l'arnaqueur disparaît après avoir encaissé l'argent.

QUAND L'ÉPARGNE COLLECTIVE DEVIENT UN PIÈGE.

Là où l'argent circule, la confiance doit être plus précieuse que l'or. »
Cette citation prend tout son sens dans le contexte actuel des tontines en ligne, un système d'épargne collective basé avant tout sur la confiance entre les membres.

Bien que ces tontines aient historiquement permis à des communautés de s'entraider financièrement, leur transition vers le numérique a ouvert la porte à une nouvelle vague d'escroqueries. Des plateformes frauduleuses et des organisateurs mal intentionnés profitent de l'anonymat du web pour détourner les fonds collectés et disparaître sans laisser de trace, laissant ainsi derrière eux des victimes dont la confiance a été abusée. L'histoire qui suit en est un témoignage concret...
suite page 69

UTILISATION FRAUDULEUSE D'ÉLÉMENTS D'IDENTIFICATION DE PERSONNE PHYSIQUE / MORALE (USURPATION)

Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (article 19-1) 2 à 5 ans d'emprisonnement et 5.000.000 à 10.000.000 FCFA d'amende.

Exemple : Un individu utilise les informations personnelles volées d'une autre personne, telles que son nom, son adresse et ses coordonnées bancaires, pour créer un faux profil sur un site de vente en ligne. Il utilise ce profil pour réaliser des achats en ligne à l'insu de la victime et se fait livrer les produits à son propre domicile. Ce type d'escroquerie repose sur l'usurpation d'identité dans un but financier et est puni par la loi.

ILS ESCROQUENT LEURS VICTIMES VIA DES FAUSSES ANNONCES D'EMPLOIS

De faux recrutements circulent en ligne, souvent diffusés par des escrocs qui utilisent le nom de prestigieuses entreprises bien connue pour arnaquer des victimes.
Une société de la place a découvert que des individus utilisant sa dénomination, faisaient des annonces de recrutement sur internet. N'ayant pas initié cela, la société saisit la PLCC d'une plainte.

Les enquêtes de la PLCC ont conduit à l'interpellation de FKE et AJH. Leur méthode : publier des annonces attrayantes, puis demander de l'argent sous prétexte de frais médicaux avant de bloquer les victimes. Les deux cyberescrocs ont reconnu les faits et ont été déférés au parquet... **suite page 64**

FRAUDE BANCAIRE EN LIGNE
Règlement n°15 relatif aux systèmes de paiement dans les états membres de l'UEMOA (articles 144 et 147)
1 à 3 ans d'emprisonnement et 100.000 à 2.500.000 francs CFA d'amende

Exemple :
Carte bancaire : Un individu utilise des informations d'une carte bancaire volée ou parvient à contourner les systèmes de sécurité en ligne, grâce à des méthodes comme le phishing pour obtenir des informations sensibles (numéros de carte, codes PIN, etc.) d'une victime. Après avoir récupéré les informations de la carte, il effectue des paiements frauduleux pour son propre compte.
Compte bancaire : Une personne utilise des identifiants de connexion bancaires piratés pour accéder au compte d'un utilisateur et réalise un transfert frauduleux de fonds vers un autre compte qu'il contrôle.

FALSIFICATION ET USAGE FRAUDULEUX DANS LE SECTEUR BANCAIRE.

Dans un monde où les transactions financières reposent sur la confiance mutuelle, la falsification de documents dans le secteur bancaire constitue une menace majeure pour la sécurité et stabilité économique. Cette infraction consiste à modifier illégalement des documents à valeur juridique ou financière, tels que des contrats ou relevés bancaires, afin d'obtenir des avantages. En plus des pertes financières, cela affecte la réputation des banques et la confiance des clients, surtout avec l'augmentation des risques liés à la numérisation. L'histoire suivante nous donnera un meilleur aperçu des méthodes employées par ces faussaires... **suite page 66**

FRAUDE SUR TRANSACTION ÉLECTRONIQUE
(FACILITÉ PAR UN SYSTÈME D'INFORMATION)
Code pénal (articles 471 et 457)
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (articles 4, 6 et 26) 1 à 10 ans d'emprisonnement et 300.000 à 5.000.000 FCFA d'amende

Exemples :
Détournement de transfert : Un individu convainc une victime d'effectuer un transfert d'argent en prétendant qu'il s'agit d'une opération légitime, alors qu'en réalité, l'argent est détourné vers un compte contrôlé par le fraudeur.

SIM Swap (changement frauduleux de carte SIM) : Un individu contacte un opérateur téléphonique en se faisant passer pour une victime, et réussit à obtenir une nouvelle carte SIM, prenant ainsi le contrôle du numéro de téléphone de la victime. Cela lui permet d'accéder à des informations sensibles, comme les codes de validation envoyés par SMS pour les transactions bancaires en ligne, afin de réaliser des paiements frauduleux.

Vol de téléphone portable : Un individu vole un téléphone mobile qui contient des informations sensibles telles que des identifiants bancaires, des applications de paiement mobile, ou des informations de carte bancaire. Grâce à ces données, il peut effectuer des transactions électroniques frauduleuses.

UNE CONFIANCE QUI SE TRANSFORME EN CAUCHEMAR

Madame DM, en difficulté avec son téléphone, fait confiance à un jeune de son quartier pour l'aider à restaurer son WhatsApp. Un mois plus tard, elle découvre que son compte Mobile Money a été vidé. Elle se rend à une agence pour mieux comprendre la situation. Elle est ainsi informée que son argent a été transféré sur plusieurs numéros inconnus.
Dame DM saisit alors d'une plainte la PLCC.

Les enquêtes de la PLCC ont permis d'interpeller EAW. Celui-ci révèle qu'il est membre d'un réseau criminel spécialisé dans le clonage de téléphones.
le rôle de EAW était de recevoir les fonds, les retirer puis les remettre à son complice... **suite page 71**

ACCÈS OU TENTATIVE D'ACCÈS FRAUDULEUX À UN SYSTÈME D'INFORMATION

Loi N°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité (article 4)De 1 à 2 ans d'emprisonnement et une amende de 5.000.000 à 10.000.000 FCFA

Exemple : Utilisation d'un logiciel de contrôle à distance sans autorisation : Un individu utilise un logiciel de prise en main à distance (comme TeamViewer ou AnyDesk) pour accéder secrètement à un ordinateur personnel ou professionnel sans l'accord du propriétaire. L'objectif peut être de voler des informations sensibles, installer des malwares ou espionner les activités de l'utilisateur.

Connexion non autorisée à un serveur : Un hacker se connecte à un serveur ou un réseau privé d'une entreprise, dans le but de voler des données ou de perturber les services en ligne.

Accès à une base de données via une vulnérabilité de sécurité : Un individu exploite une faille dans la sécurité d'un site web ou d'une base de données d'une entreprise pour accéder à des informations confidentielles (par exemple des informations bancaires ou des données personnelles d'utilisateurs), sans une autorisation légale.

Connexion à distance à un système de gestion de réseau : Un individu se connecte sans permission à la ligne de commande d'un système informatique d'une organisation, en utilisant des techniques comme le phishing ou l'exploitation de failles de sécurité pour voler des informations ou perturber les opérations de l'entreprise.

APPROPRIATION DE BIEN D'AUTRUI (FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (articles 471 et 457)
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (articles 4, 6 et 26) 1 à 10 ans d'emprisonnement et 300.000 à 5.000.000 FCFA d'amende

Exemple : Un individu reçoit par erreur une somme d'argent sur son portefeuille électronique (par exemple, un dépôt d'argent, un virement effectué par une banque ou un paiement effectué en ligne). Bien que l'expéditeur prouve, avec des justificatifs, que l'argent a été envoyé par erreur et qu'il demande la restitution des fonds, la personne réceptrice refuse de rendre l'argent et l'utilise à ses propres fins.

DÉTENTION ILLÉGALE DE DONNÉES

Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (article 13).
1 à 2 ans d'emprisonnement et 1.000.000 à 5.000.000 FCFA d'amende.

Exemple : Un individu accède illégalement à un compte bancaire en ligne d'une autre personne, ou à des informations professionnelles sensibles (par exemple, des données d'une entreprise), puis refuse de remettre les identifiants ou de restituer l'accès au propriétaire légitime. Cela peut se produire dans un contexte de conflit, où la personne détentrice des données utilise cette situation pour obtenir un avantage ou pour causer un tort à la victime.

DIFFUSION DE FAUSSES INFORMATIONS
(FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (article 372).
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (article 65).
6 mois à 2 ans d'emprisonnement et 1.000.000 à 5.000.000 FCFA d'amende.

Exemple : Un utilisateur de réseaux sociaux publie une fausse nouvelle concernant un événement, comme la diffusion d'une prétendue déclaration d'une autorité publique annonçant l'introduction d'une loi discriminatoire. Cette information, bien que complètement inventée, est partagée largement, créant une panique parmi les citoyens et affectant la réputation de l'autorité mentionnée. L'individu qui a publié cette fausse information savait qu'elle était erronée, mais l'a partagée dans le but de semer la discorde ou d'obtenir plus d'attention.

ENTRAVE OU TENTATIVE D'ENTRAVE DU FONCTIONNEMENT D'UN SYSTÈME D'INFORMATION

Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (Article 6).
1 à 5 ans d'emprisonnement et 10.000.000 à 40.000.000 FCFA d'amende.

Exemple : Un individu lance une attaque par déni de service distribué (DDoS) contre un site web d'une entreprise, saturant ses serveurs avec un grand nombre de requêtes simultanées, rendant le site inaccessible aux utilisateurs légitimes. Cette attaque perturbe l'activité de l'entreprise et cause une perte financière. Une autre forme d'entrave pourrait être l'utilisation de ransomware, un programme malveillant qui crypte les fichiers d'une organisation, rendant ses systèmes informatiques inaccessibles jusqu'à ce qu'une rançon soit payée.

INCITATION AU TROUBLE À L'ORDRE PUBLIC (FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (article 369).
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (article 62).
6 mois à 5 ans d'emprisonnement et 1.000.000 à 20.000.000 FCFA d'amende.

Exemple : Un individu publie sur un réseau social un message appelant à la violence lors d'une manifestation politique, en incitant les participants à attaquer les forces de l'ordre et à détruire des biens publics. Le message est partagé et repris par de nombreuses personnes, ce qui entraîne des violences pendant la manifestation. L'auteur de ces propos est poursuivi pour incitation au trouble à l'ordre public, car il a encouragé des actions menaçant l'ordre et la sécurité publics.

INCITATION À LA HAINE (FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (articles 365, 367).
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (article 58).
10 à 20 ans d'emprisonnement et 5.000.000 à 10.000.000 FCFA d'amende.

Exemple : Un individu publie sur un réseau social des messages visant à inciter à la violence contre un groupe ethnique ou religieux particulier, en utilisant des propos discriminatoires, menaçant de provoquer des actes violents à l'encontre des membres de ce groupe. Par exemple, la diffusion d'un texte ou d'une vidéo incitant à "chasser" ou à "exterminer" des personnes en raison de leur origine ethnique, de leur religion ou de leur orientation sexuelle serait un acte d'incitation à la haine.

MENACE AU MOYEN D'UN SYSTÈME D'INFORMATION (FACILITÉ PAR UN SYSTÈME D'INFORMATION)

Code pénal (articles 366 et 373).
Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (articles 59 et 66).2 à 10 ans d'emprisonnement et 5.000.000 à 20.000.000 FCFA d'amende.

Exemple : Un individu envoie un message menaçant via un réseau social à une autre personne, en déclarant : «Je vais te tuer si tu ne fais pas ce que je dis» ou «Je vais te faire souffrir». Cette menace, même si elle n'est pas concrétisée, est une infraction puisqu'elle utilise un moyen numérique pour inciter la victime à craindre pour sa vie ou son intégrité physique.

SPOLIATION DE COMPTES RÉSEAUX SOCIAUX

Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (articles 4 et 5).1 à 2 ans d'emprisonnement et 5.000.000 à 10.000.000 FCFA d'amende.

Exemple : Une personne reçoit un message via les réseaux sociaux ou par email, semblant provenir d'un service de support technique de Facebook, l'invitant à "mettre à jour" son mot de passe en cliquant sur un lien. Ce lien redirige la victime vers un faux site Web, où elle entre ses identifiants (adresse email et mot de passe). L'escroc récupère alors ces informations, se connecte au compte de la victime, et en modifie les paramètres, comme l'adresse email et le mot de passe, pour prendre le contrôle total du compte et de ses données. Le fraudeur peut alors publier des messages sous le nom de la victime ou accéder à des informations personnelles sensibles.

VOL D'INFORMATION

Loi n°2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité (articles 26, 27 et 28).
5 à 20 ans d'emprisonnement et 3.000.000 à 10.000.000 FCFA d'amende.

Exemple : Un technicien dans une société accède sans autorisation au serveur interne de l'entreprise. Il copie le fichier de la liste du personnel (Nom, adresses, numéros de téléphone, matricules, numéros comptes bancaires ...). Il transfère ces données sur une Clé USB et les vend à une société concurrente ou les utilise pour envoyer de faux SMS.

CHIFFRES DE LA CYBERCRIMINALITE EN 2024

ACTIVITÉS DE LA PLATEFORME DE LUTTE CONTRE LA CYBERCRIMINALITÉ (PLCC)

Les enquêtes de cybercriminalité sont déclenchées par la réception des plaintes des victimes, la transmission d'affaires par les parquets, ou par voie de coopération policière internationale. Les services d'enquêtes spécialisées conduisent alors leurs investigations conformément au code de procédures pénales.

Parallèlement, les services d'assistance aux victimes se chargent de faire cesser les infractions en cours (suppression de vidéos compromettantes et de faux comptes, restauration de comptes, etc.), d'aider les victimes à recouvrer l'usage normal de leurs équipements et comptes de réseaux sociaux, et de les conseiller à de bonnes pratiques en ligne. Les chiffres présentés ci-dessous, reflètent l'ensemble des activités de la PLCC, département de l'ANSSI en charge de la lutte contre la cybercriminalité au niveau national.

B.1 NOMBRE D'AFFAIRES ET PRÉJUDICES FINANCIERS

TYPES D'AFFAIRES	NOMBRE DE DOSSIERS			PRÉJUDICE FINANCIER CONSOMME (F CFA)		
	2024	2023	2022	2024	2023	2022
ACCES FRAUDULEUX A UN SYSTEME D'INFORMATION	**57**	47	48	**151 845 270**	3 302 428 287	465 866 309
APPROPRIATION DE BIEN D'AUTRUI	**378**	224	221	**86 015 136**	63 368 97554	54 093 860
ATTEINTE A LA DIGNITE HUMAINE	**2822**	2198	1457	**860 151 536**	175 702 659	66 062 466
-MENACE DE PUBLICATION D'IMAGE A CARACTERE SEXUEL	2218			448 847 455		
-PUBLICATION D'IMAGE A CARACTERE SEXUEL	574			20 899 835		
ATTEINTE A L'HONNEUR ET A L'IMAGE	**1577**	720	522	**6 444 000**	39 567 000	260 000
-DIFFAMATION	714			3 080 000		
-PUBLICATION DE DONNEES A CARACTERE PERSONNEL	190			3 320 000		
-HARCELEMENT	544			35 000		
-INJURE	128			9 000		
CHANGEMENT FRAUDULEUX DE CARTE SIM	**15**	9	16	**21 794 281**	8 438 851	6 924 926
DETENTION ILLEGALE DE DONNEES A CARACTERE PERSONNEL	**31**	18	6	**0**	65 000	0
DIFFFUSION DE FAUSSES INFORMATIONS	**28**	39	18	**0**	0	0
ENTRAVE AU FONCTIONNEMENT D'UN SYSTEME D'INFORMATION	**10**	5	0	**0**	0	0
ESCROQUERIE SUR INTERNET	**2326**	802	607	**2 361 374 956**	847 178 774	1 897 384 088
-FAUX ACHAT ET FAUSSE VENTE EN LIGNE	965			326 210 190		
-ESCROQUERIE	457			574 879 493		
-FAUSSE BOURSE D'ETUDE	12			17 264 760		
-FAUSSE BOURSE EN LIGNE	667			1 146 292 139		
-FAUSSE LOCATION DE MAISON	59			36 670 486		
-FAUSSE PROMESSE D'EMPLOI	34			24 525 767		
-FAUSSE TONTINE	21			14 846 850		
-FAUX SENTIMENTS	72			99 483 916		
FRAUDE BANCAIRE	**64**	43	33	**191 127 693**	801 717 094	176 965 439
-SUR CARTE BANCAIRE	31			36 722 045		
-SUR COMPTE BANCAIRE	37			154 405 648		
FRAUDE SUR TRANSACTION ELECTRONIQUE	**1 060**	1 035	1 073	**496 813 497**	411 599 122	1 029 202 714
INCITATION A LA HAINE	**1**	4	4	**0**	0	0
MENACE	**339**	185	185	**1 656 000**	30 000	30 000
-MENACE DE MORT	228			655 000		
-MENACE D'ATTEINTE A UNE PERSONNE	111			1 001 000		
SPOLIATION DE COMPTE MAIL/FACEBOOK	**1205**	711	762	**8 534 320**	4 054 000	0
TROUBLE A L'ORDRE PUBLIC	**28**	3	3	**40 700**	0	0
UTILISATION FRAUDULEUSE D'ELEMENTS D'IDENTIFICATION DE PERSONNE :	**1638**	1520	1226	**1 909 877 375**	2 903 028 953	2 434 736 913
-PHYSIQUE	1534			1 306 185 946		
-MORALE	84			603 691 408		
VOL D'INFORMATION	**374**	368	360	**68 398 716**	490 759	1 814 522 145
AUTRES	**134**	86	38	**647 740 843**	412 579 404	779 404 111
TOTAL	**12 100**	8 132	6 579	**6 960 903 038**	9 206 106 267	6 292 930 058

L'analyse des trois dernières années montre une hausse continue du nombre de plaintes. En effet, les plaintes sont passées de 6579 en 2022 à 8132 en 2023, puis à 12100 en 2024, soit une augmentation de 84% entre 2022 et 2024.

L'augmentation durable du nombre de cas traités se justifie par plusieurs facteurs. Nous observons une évolution de la criminalité traditionnelle vers un usage accru du numérique comme outil de commission des infractions. Cette mutation tend à estomper la distinction claire qui existait auparavant entre les infractions classiques et celles relevant de la cybercriminalité (infractions facilitées par les technologies numériques). Les magistrats privilégient les qualifications de cybercriminalité car leur traitement repose sur des preuves plus scientifiques.

L'augmentation du nombre d'utilisateurs des technologies numériques, ainsi que la diversification des services en ligne, expliquent par ailleurs cette progression du nombre d'affaires. Enfin, la hausse se justifie par les sensibilisations actives de la PLCC qui touchent de plus en plus de personnes désormais convaincues de déposer plainte. De plus la qualité de l'assistance apportée aux victimes est un facteur de rapprochement des justiciables.

Relativement aux préjudices, les atteintes à la dignité humaine connaissent une hausse en nombre et en préjudice de 2022 à 2024, passant de 1457 à 2822 plaintes et de 66.062.466 FCFA à 860.151.536 FCFA de préjudice en 2024.

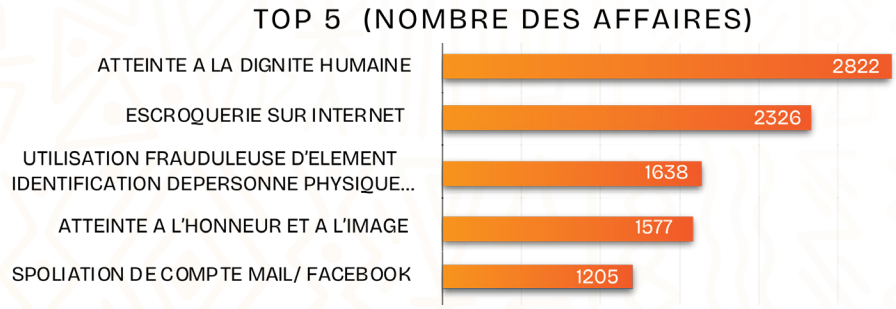
Les escroqueries, en particulier celles liées aux faux investissements en ligne, ont connu une explosion en 2024, avec des affaires médiatisées telles que GLOBAL INVESTISSEMENT, INDEX TECHNOLOGIES, MINNINGORACLES, COCA COLA, et SUNPOWER. Cette catégorie d'escroqueries a enregistré une hausse de 178,7% en préjudice (passant de 847.178.774 FCFA en 2023 à 2.361.374.956 FCFA en 2024) et une augmentation de 190% en nombre de plaintes (de 802 plaintes à 2326 plaintes).

En revanche, concernant les accès frauduleux aux systèmes d'information, on note une forte baisse de préjudice de 3.302.428.287 FCFA en 2023 à 151.845.270 FCFA en 2024. Cette baisse a eu un impact sur les pertes globales de l'année, qui sont passées de 9.206.106.267 FCFA en 2023 à 6.960.903.038 FCFA en 2024, soit une diminution de 24,4%.

B.1.1 TOP 5 DES TYPES D'AFFAIRES

B.1.1.1 EN FONCTION DU NOMBRE D'AFFAIRES

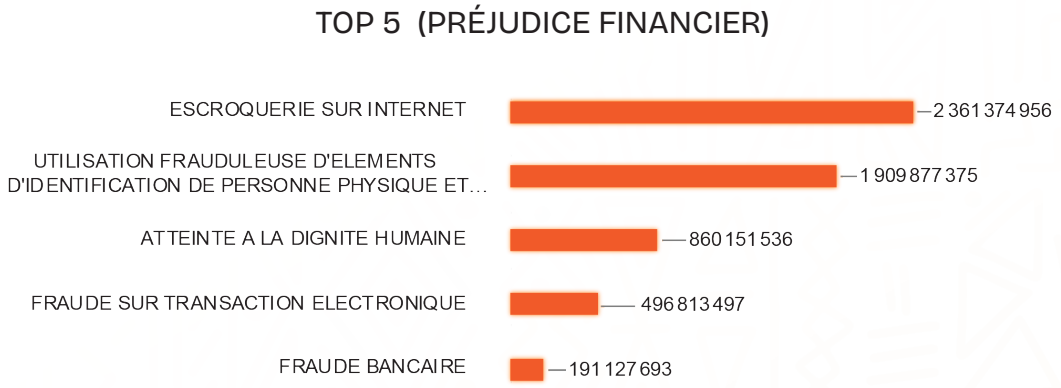
N°	TOP 5 DES TYPES D'AFFAIRES 2024	NBRE AFFAIRE	%	Rang 2023	Rang 2022
1	ATTEINTE A LA DIGNITE HUMAINE	2822	23,32	1	1
2	ESCROQUERIE SUR INTERNET	2326	19,22	4	5
3	UTILISATION FRAUDULEUSE D'ELEMENT D'IDENTIFICATION DE PERSONNE PHYSIQUE ET MORALE (USURPATION)	1638	13,54	2	2
4	ATTEINTE A L'HONNEUR ET A L'IMAGE	1577	13,03	5	6
5	SPOLIATION DE COMPTE MAIL/ FACEBOOK	1205	9,96	6	4
...	AUTRES	...	...		
	TOTAL	12100			



Sur les trois dernières années, les atteintes à la dignité humaine occupent la première place du top 5 des infractions les plus signalées. En parallèle, les escroqueries connaissent un regain, tandis que les usurpations d'identité reculent d'une place dans le classement.
Le maintien en tête des atteintes à la dignité humaine et la progression continue des atteintes à l'honneur et à l'image, qui passent de la 6ème place en 2022 à la 4ème place en 2024, témoignent de la difficulté de la coopération opérationnelle avec les plateformes de réseaux sociaux. En effet, ces deux types d'infractions se commettent exclusivement sur ces plateformes, qui continuent de faire des difficultés à répondre aux réquisitions judiciaires et aux demandes d'informations d'investigation.

B.1.1.2 EN FONCTION DU PRÉJUDICE FINANCIER

N°	TOP 5 INFRACTIONS 2024	PREJUDICE FINANCIER	%	Rang 2023	Rang 2022
1	ESCROQUERIE SUR INTERNET	2 361 374 956	33,92	3	2
2	UTILISATION FRAUDULEUSE D'ELEMENTS D'IDENTIFICATION DE PERSONNE PHYSIQUE ET MORALE (USURPATION)	1 909 877 375	27,44	2	1
3	ATTEINTE A LA DIGNITE HUMAINE	860 151 536	11,58	6	7
4	FRAUDE SUR TRANSACTION ELECTRONIQUE	496 813 497	7,14	5	4
5	FRAUDE BANCAIRE	191 127 693	2,75	4	6
...	AUTRES	...	...		
	TOTAL	6 960 903 038			

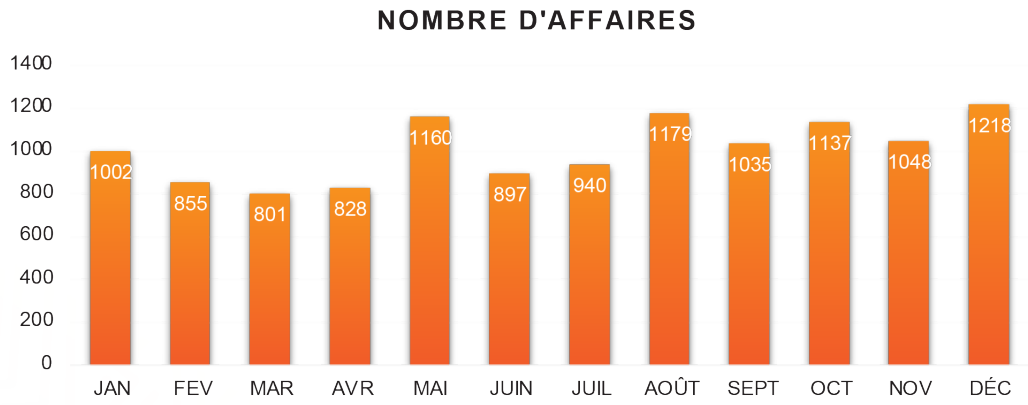


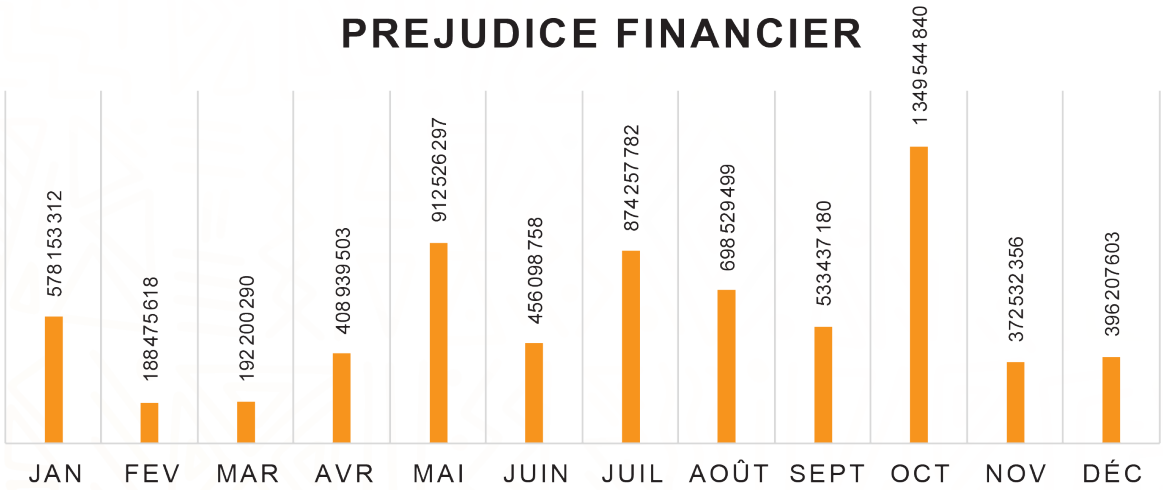
La croissance des escroqueries sur internet telle qu'indiquée plus haut, place ce type d'affaires en tête du top 5 des préjudices, de la 3ème place à la 1ère.

Bien que les usurpations d'identité connaissent une baisse significative de 34,2%, passant de 2.903.028.953 FCFA à 1.909.877.375 FCFA, elles gagnent néanmoins une place dans ce top 5.Les atteintes à la dignité humaine qui causaient principalement des préjudices moraux rentrent dans ce top 5 des préjudices financiers. Ce type d'affaires constitue en 2024 une source de revenu substantielle pour les cybers délinquants.

Les accès frauduleux à un système d'information, qui occupaient la 1ère place en 2023, ne figurent plus dans le top 5 en 2024. Cependant, il convient de noter que l'Association Professionnelle des Banques et Établissements Financiers (APBEF) de Côte d'Ivoire a pris des mesures proactives en mettant en place un cadre d'échange avec la DITT. Cette collaboration a permis d'anticiper de nombreuses attaques et d'atténuer les risques.

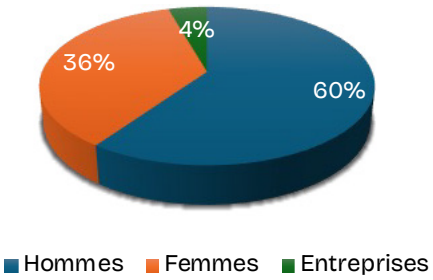
B.1.2 NOMBRE D'AFFAIRES ET PRÉJUDICES FINANCIERS PAR MOIS



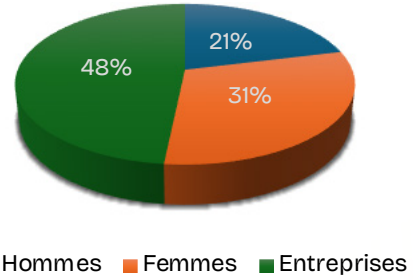


B.2 TYPES DES VICTIMES

Nombre des affaires



Préjudice financier



En 2024, 11 563 personnes physiques ont été victimes de cybercriminalité, contre 7 677 en 2023, soit une hausse de 50,62 %. En revanche, le préjudice financier reste relativement constant, passant de 3 577 103 925 FCFA en 2023 à 3 595 286 419 FCFA en 2024. Concernant les personnes morales, 537 entreprises ont été victimes en 2024, contre 458 en 2023, enregistrant une augmentation de 17,25 %. Toutefois, le préjudice financier subi par ces entreprises a diminué, passant de 5 629 002 342 FCFA en 2023 à 3 365 616 619 FCFA en 2024, soit une baisse de 40,21%. Ces constats mettent en évidence l'impact positif des actions de sensibilisation menées par la PLCC, notamment à l'attention des entreprises. Les établissements financiers et leurs clients entreprises ont été formés sur les modes opératoires des cybercriminels et les mesures de cybersécurité à adopter pour réduire les risques.

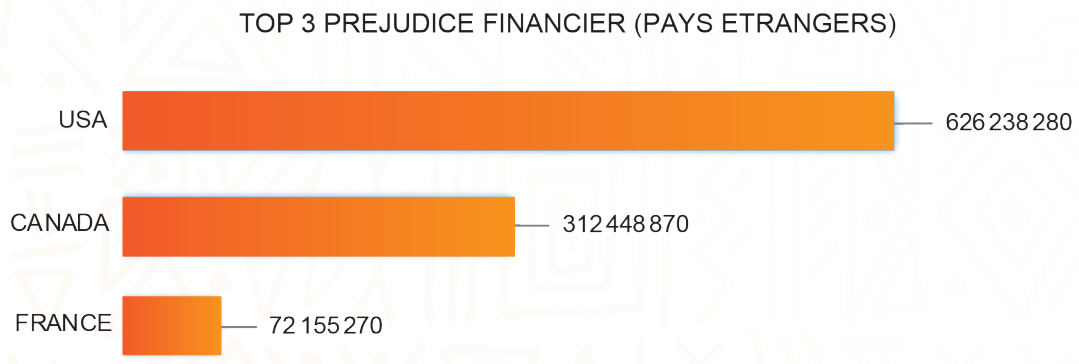
B.3 PAYS D'ORIGINE DES VICTIMES

Contrairement à 2023 qui a enregistré 37 affaires de coopération internationale représentant 0.45 % des dossiers totaux, 13 dossiers de coopération ont été enregistrés en 2024 soit 0,11 % du nombre total d'affaires. Bien qu'il apparaisse que de nombreux incidents aient un lien avec la Côte d'Ivoire, très peu d'entre eux sont judiciarisés et formellement portés à la connaissance de nos services. Ces chiffres reflètent uniquement les affaires transmises par voie de coopération judiciaire ou policière.

› B.3.1 EN FONCTION DU NOMBRE D'AFFAIRES

N°	PAYS	2024	2023	2022
1	COTE D'IVOIRE	12087	8095	6537
2	USA	4	14	24
3	CANADA	4	7	12
4	FRANCE	1	5	2
5	SINGAPOUR	1	2	0
6	AUTRICHE	1	0	1
7	POLOGNE	1	0	0
8	SUISSE	1	1	2
9	ARRABIE SAOUDITE	0	1	0
10	MEXIQUE	0	1	0
11	SLOVAQUIE	0	1	0
12	TURQUIE	0	1	0
13	BULGARIE	0	1	0
14	BIELORUSSIE	0	1	0
15	LIBAN	0	1	1
16	ESPAGNE	0	1	0
	TOTAL	12100	8132	6579

› B.3.2 EN FONCTION DU PRÉJUDICE FINANCIER

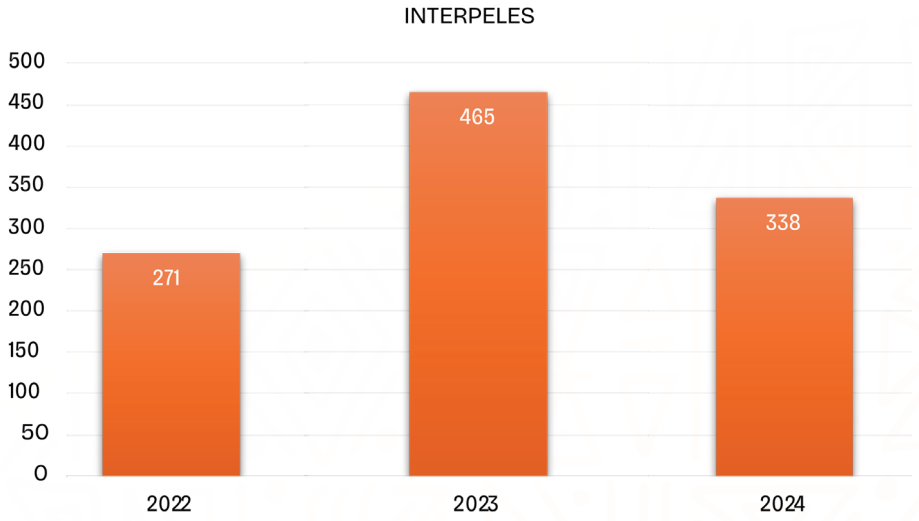


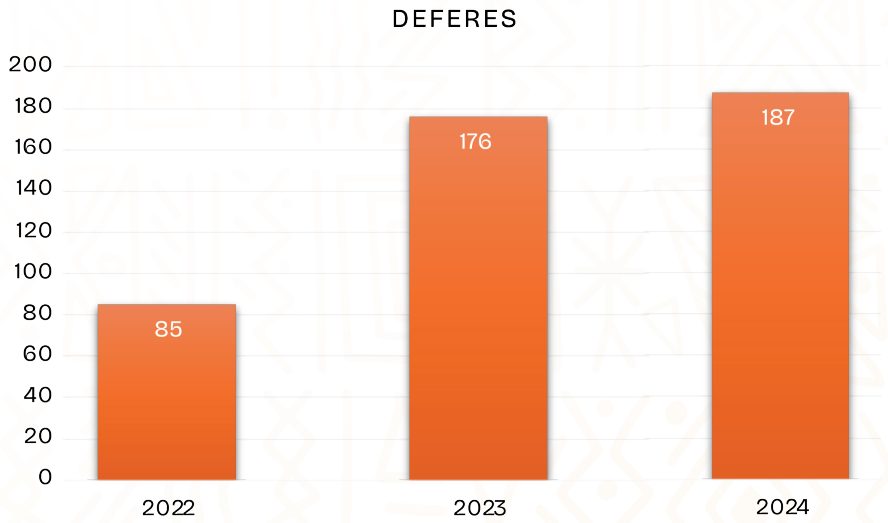
B.4 TRAITEMENT DES DOSSIERS

› B.4.1 INTERPELLÉS ET DÉFÉRÉS

En 2024, 338 personnes ont été interpellées, contre 465 en 2023, marquant ainsi une baisse de 27,31 % des interpellations. En revanche, 187 personnes ont été déférées devant les tribunaux en 2024, contre 176 en 2023, ce qui représente une augmentation de 6,25 % des déferrements.
On observe également une baisse du nombre de mineurs impliqués, ainsi qu'une réduction du nombre de non-nationaux concernés par les affaires.

Certaines infractions, telles que les atteintes à la dignité humaine et les atteintes à l'honneur et à l'image, impliquent souvent des suspects résidant hors de notre juridiction. Bien que leur identification permette d'élucider certaines affaires, les interpellations et les extraditions demeurent des défis majeurs. Par ailleurs, les escroqueries sur internet génèrent de nombreuses plaintes, souvent liées à des petits groupes de suspects. Sans ces particularités, le nombre d'interpellations et de déférés aurait pu être plus élevé.





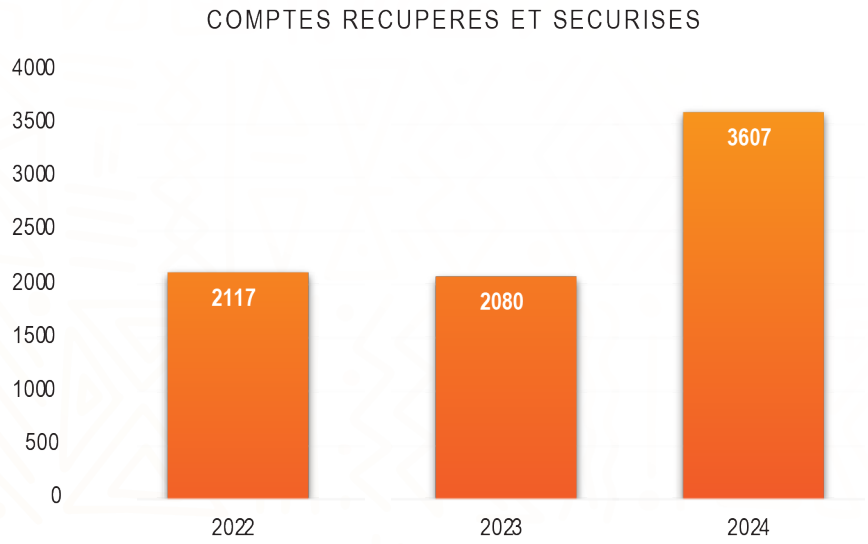
B.5 ASSISTANCE TECHNIQUE AUX VICTIMES

L'assistance aux victimes a pour objectif de faire cesser les infractions en cours lors du dépôt de plainte. Cette assistance permet également d'aider à l'implémentation de bonnes pratiques de sécurisation et d'hygiène numérique. Contrairement à l'assistance apportée par le CI-CERT aux entreprises, cette activité s'adresse principalement aux particuliers.

› B.5.1 RÉCUPÉRATION ET SÉCURISATION DE COMPTES

La récupération et la sécurisation de compte, consiste à redonner l'accès à une victime qui en a perdu le contrôle.

N°	RECUPERATION ET SECURISATION DE COMPTES	2024	2023	2022
1	FACEBOOK	3604	2065	2056
2	GMAIL	1	3	37
3	YAHOO	1	2	5
4	WHATSAPP	1	0	0
5	TIK TOK	0	2	6
6	INSTAGRAM	0	7	12
7	SNAPCHAT	0	1	1
	TOTAL	**3607**	**2080**	**2117**



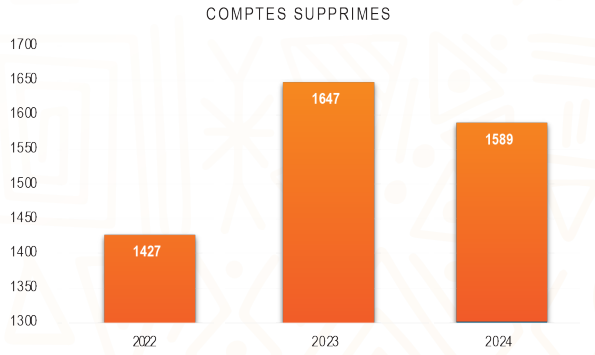
De 2023 à 2024, les récupérations et sécurisations de comptes ont connu une hausse de 73,4%. Cette augmentation est principalement liée aux spoliations de compte Facebook qui précèdent généralement des infractions telles que les usurpations d'identité, les escroqueries et les atteintes à la dignité humaine. Pour rappel, ces infractions ont connu un fort accroissement (B.1 NOMBRE AFFAIRES ET PRÉJUDICES FINANCIERS, page 30).

B.5.2 SUPPRESSION DE COMPTES

Il s'agit du signalement et de la suppression de comptes impliqués dans la perpétration d'infractions. Ces comptes sont généralement des avatars (faux comptes), ou des comptes usurpateurs d'identité.

N°	SUPPRESSION DE COMPTES	2024	2023	2022
1	FACEBOOK	1501	1566	1399
2	TIK TOK	12	7	5
3	INSTAGRAM	9	4	19
4	SWEET MEET	13	26	1
5	WHATSAPP	20	37	1
6	XVIDEO	0	6	0
7	BADOO	2	0	0
8	EVERMATCH	3	0	0
v9	MAYBE YOU	1	0	0
10	YHAPPI	12	1	2
11	CHAT YAMO	3	0	0
12	WANNA	1	0	0
13	AFRO-INTRODUCTION	1	0	0
14	AFROYAMO	1	0	0
15	YOU LOVE	1	0	0
16	APPLICATION	1	0	0
17	LIKERRO	1	0	0
18	LOVETOR	1	0	0
19	ONLYORK	2	0	0
20	NOUS 2	1	0	0
21	PHEROMANCE	2	0	0
22	BUNPLAY	1	0	0
	TOTAL	**1589**	**1647**	**1427**

La majorité des comptes incriminés supprimés sont du réseau social Facebook. L'usurpation d'identité des autorités ivoiriennes demeure un véritable facteur influençant les chiffres.

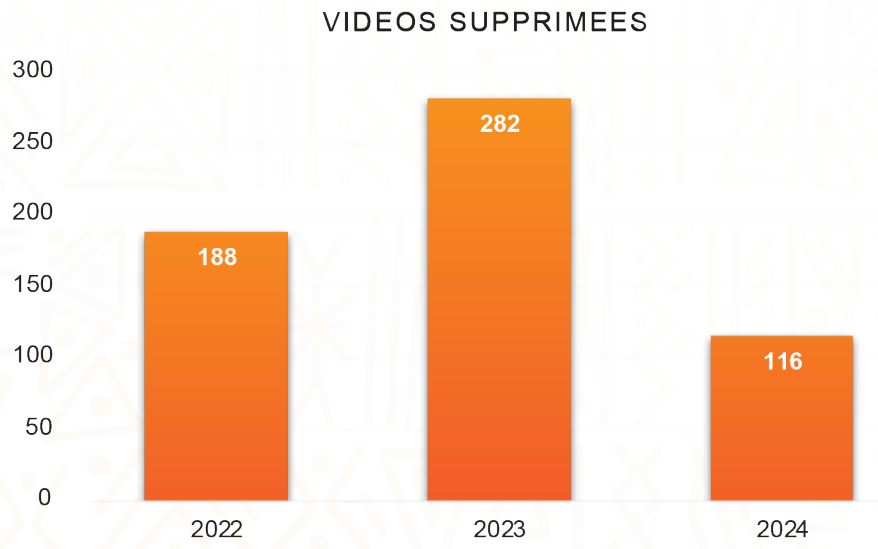


B.5.3 SUPPRESSION DE VIDÉOS

Il s'agit du retrait de vidéos compromettantes ou illicites, postées sur des plateformes d'accès public. Cela inclut des vidéos telles que de la nudité, des deepfakes, des profanations, l'exposition de mineurs, la pornographie infantile, etc.

N°	SUPPRESSION DE VIDÉOS	2024	2023	2022
1	FACEBOOK	89	233	144
2	TIK TOK	1	3	7
3	INSTAGRAM	0	1	12
4	SWEET MEET	3	10	1
5	WHATSAPP	1	0	0
6	XVIDEO	10	7	23
7	YHAPPI	0	1	0
8	MESSENGER	4	0	0
9	VIMEO	7	25	0
10	AFROMAYO	0	0	1
11	MAYBE YOU	0	1	0
12	SNAPCHAT	0	1	0
13	XNXX	1	0	0
	TOTAL	116	282	188

En 2024, 116 vidéos compromettantes ont été supprimées contre 282 en 2023, soit une baisse de 58,87%. Cette baisse s'explique par un changement de stratégie des cyber délinquants, qui se détournent progressivement des sites web et réseaux sociaux non cryptés pour utiliser de plus en plus des messageries et plateformes chiffrées telles que Signal ou Telegram afin de diffuser leurs contenus illicites.

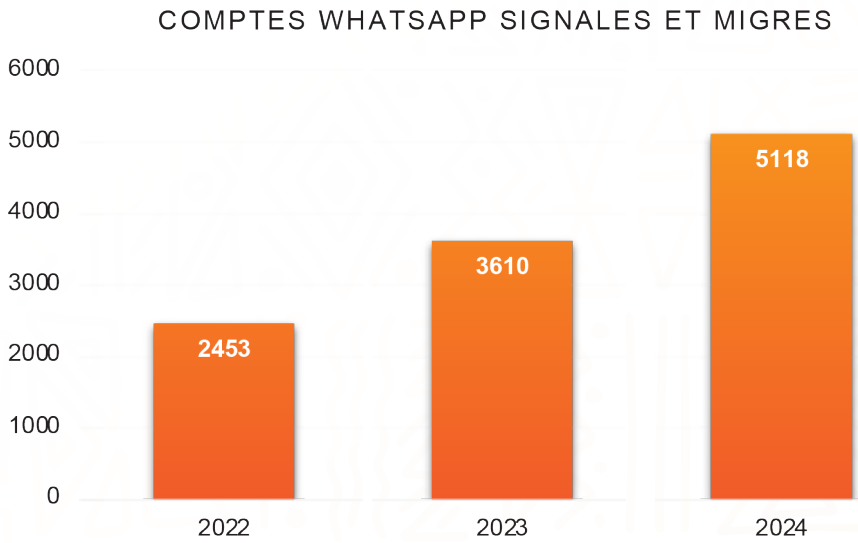


B.5.4 COMPTES WHATSAPP

Il s'agit d'une part, de signaler et d'obtenir la suppression de comptes WhatsApp impliqués dans des infractions, et d'autre part d'assister les victimes dans la migration et la sécurisation de leurs comptes. Dans ce second cas, l'objectif est de soustraire les victimes du harcèlement ou de la pression morale exercée par les suspects.

N°	COMPTES WHATSAPP	2024	2023	2022
1	COMPTES INCRIMINES SIGNALÉS	2203	2420	1342
2	MIGRATION DE COMPTE	2915	1190	1111
	TOTAL	5118	3610	2453

En 2024, 5118 comptes WhatsApp ont été traités, contre 3610 comptes en 2023. Cette forte croissance est due à une augmentation du nombre de victimes choisissant de changer de compte afin d'échapper aux pressions psychologiques exercées par les auteurs d'infractions.



APPORT DES TECHNOLOGIES AUX INVESTIGATIONS

ACTIVITÉS DU CENTRE DE FUSION ET D'ANALYSE DE DONNÉES (CFAD)

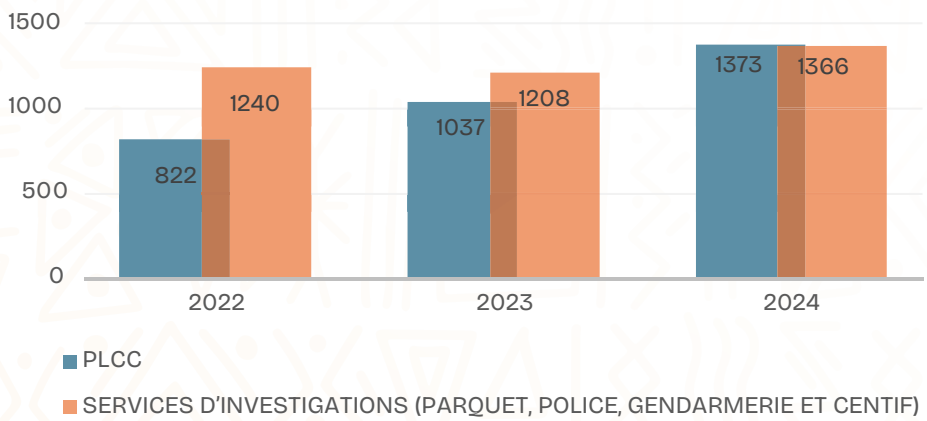
Les missions du CFAD sont de collecter et traiter les données, analyser les informations et produire des rapports au profit des services d'investigations : PLCC, Police, Gendarmerie, CENTIF, Parquet, Juges d'instruction, etc. La collecte de données se fait soit par voie de réquisition judiciaire à l'endroit des opérateurs privés (nationaux et internationaux) détenant des logs en lien avec des affaires, soit par extraction forensique légale d'information sur tous les types d'équipement stockant des preuves numériques utiles à la manifestation de la vérité. L'analyse est le processus de valorisation des données pour fournir des informations stratégiques et tactiques, qui aident à résoudre des affaires, et à identifier des tendances criminelles. Les analystes produisent des rapports d'analyse au profit des services requérants.

Le CFAD est constitué de services de traitement de données, d'analyse criminelle, d'analyse réseaux sociaux et d'un laboratoire de criminalistique numérique (digital forensic lab.). L'acquisition des données d'investigation détenues par le secteur privé du digital est assurée par une gestion centralisée de réquisitions judiciaires en relation avec les bureaux des Procureurs. Le CFAD est l'interface, tiers de confiance entre les fournisseurs de services digitaux (nationaux et internationaux) et les services d'investigations. La collecte de données et de signalement en ligne est dévolue au service réseaux sociaux qui effectue de nombreuses patrouilles virtuelles.

Véritable lien entre les enquêteurs et les traces numériques, l'objectif du centre est de guider, à l'aide de données numériques, les activités des Officiers de Police Judiciaire.

C.1 ANALYSES JUDICIAIRES

Initialement dévolus qu'à la PLCC, depuis 2018 les analystes du service Analyse Judiciaire ont pour mission de mettre à la disposition de l'ensemble des services de l'État effectuant des enquêtes judiciaires, toutes les capacités technologiques d'analyse ainsi que l'expérience acquise dans le domaine.



Les enquêteurs sont de plus en plus convaincus de l'apport du CFAD dans la résolution de leurs affaires. Cela s'explique par des résultats probants mais aussi par une grande tournée de sensibilisation, conduite en 2024 par l'ANSSI, auprès des services d'investigations. Le CFAD a aussi travaillé à l'accroissement de ses capacités de prise en charge des affaires. En dehors des affaires de cybercriminalité soumises par la PLCC au CFAD, ce centre traite d'une grande diversité de sujets criminels : grand banditisme, trafic illicite de drogue, blanchiment de capitaux, lutte contre le terrorisme, orpaillage clandestin, etc.

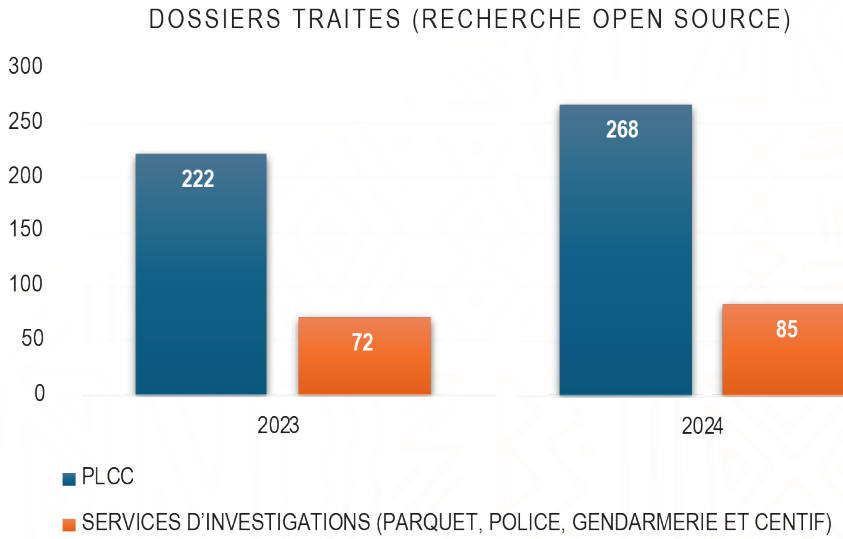
De 2022 à 2024 on assiste à une augmentation de 32,8% du nombre de sollicitations des services.

C.2 ANALYSES RÉSEAUX SOCIAUX

C.2.1 RECHERCHE OPEN SOURCE

Les recherches sur les sources ouvertes effectuées par le CFAD au profit des enquêteurs dans le cadre des affaires soumises.

ACTIVITES	2024	2023
RAPPORTS D'ANALYSE	162	133
ACTIONS RESEAUX SOCIAUX	190	130
TOTAL	**352**	**263**



Le service analyse réseaux sociaux a reçu 353 dossiers en 2024 contre 294 en 2023, soit une augmentation de 20,1%. Cela est dû à une meilleure prise en compte des infractions liées aux réseaux sociaux et aux résultats probants dans le traitement des requêtes.

C.2.2 RENSEIGNEMENT OPEN SOURCE

Le renseignement open source est constitué d'informations collectées sur les réseaux sociaux ayant fait l'objet de note de renseignement au profit des autres services judiciaires.

ACTIVITES	2024	2023
RAPPORTS D'ANALYSE	162	133
ACTIONS RESEAUX SOCIAUX	190	130
TOTAL	**352**	**263**

L'augmentation des chiffres s'expliquent par :

- L'intensification des patrouilles virtuelles due à la détection de nombreuses campagnes de propagande.
- L'organisation de la CAN 2023 nécessitant des rapports de suivi réguliers.

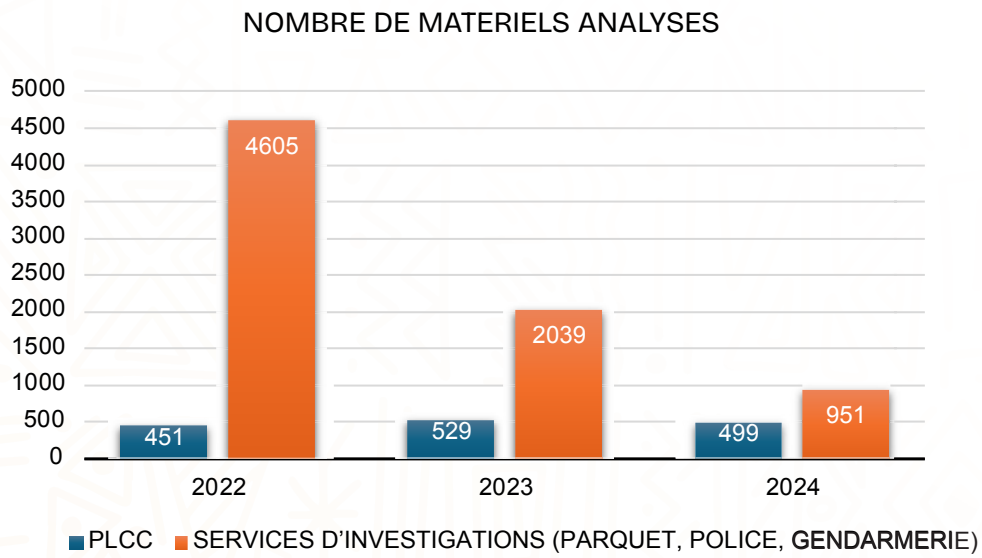
C.3 TRAITEMENTS NUMÉRIQUES

Le service Traitements Numériques a pour rôle de fournir aux analystes du CFAD les données numériques dont ils ont besoin. La collecte de ces preuves numériques s'opère par plusieurs canaux que sont l'extraction forensic sur les équipements, la gestion des réquisitions judiciaires des OPJ, et les sources de données ouvertes (open source) produites par le service analyse réseaux sociaux.

C.3.1 LABORATOIRE DE CRIMINALISTIQUE NUMÉRIQUE

Le Laboratoire de Criminalistique Numérique (LCN) a pour mission d'extraire les données des équipements numériques qu'il reçoit des enquêteurs. Ses requérants sont constitués de services de police judiciaire ainsi que l'administration pénitentiaire.

C.3.1.1 MATÉRIELS ANALYSÉS PAR TYPE DE SERVICE

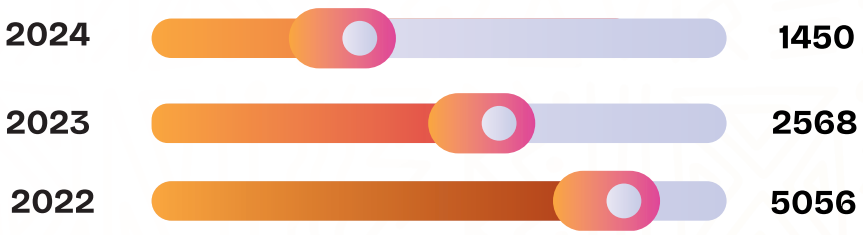


C.3.1.2 TYPES DE MATÉRIELS ANALYSÉS

N°	TYPES DE MATERIELS	2024	2023	2022
1	TÉLÉPHONES PORTABLES	646	1953	4105
2	CARTES ET SUPPORT SIM	678	493	786
3	ORDINATEURS PORTABLES	44	42	26
4	CARTES MÉMOIRES	31	38	63
5	ENTÊTE MAIL	17	10	24
6	DISQUES DURS EXTERNES	10	8	13
7	UNITÉS CENTRALES	3	7	6
8	CLÉ USB	9	4	17
9	PORTATIF + CHARGEUR	0	3	1
10	ENREGISTREURS NUMÉRIQUES	2	2	12
11	POCKET WIFI	0	2	0
12	SERVEURS	0	2	0
13	GPS	0	2	0
14	TABLETTE	0	1	2
15	DRONE	10	1	0
16	I MACHINE	0	0	1
	TOTAL	1450	2568	5056

En 2022 et 2023 d'importantes saisies de téléphones usagers ont été opérées. En 2024 ces opérations n'ont pas eu lieu d'où le chiffre en forte baisse.

TYPES DE MATÉRIELS ANALYSÉS



C.3.2 RÉQUISITIONS JUDICIAIRES

Une réquisition judiciaire est un acte par lequel une autorité judiciaire (Juge, Procureur ou Officier de Police Judiciaire) demande officiellement à une personne, une entreprise ou une organisation de fournir des informations ou d'effectuer une action dans le cadre d'une enquête. Dans notre cas, ces réquisitions peuvent concerner des adresses IP, des numéros de téléphone, des profils de réseaux sociaux, des adresses mails, ou des transactions entre ces éléments.

Les réquisitions judicaires à l'endroit des acteurs privés du numérique sont centralisées et gérées au niveau national par l'ANSSI. Les échanges avec ces acteurs font l'objet de suivi car l'efficacité des réponses impacte directement les résultats des enquêtes.

C.3.2.1 OPÉRATEURS DE TÉLÉCOMS & FAI

	TAUX TRAITÉ (%)			DELAI DE REPONSE (JOURS)		
OPÉRATEUR	2024	2023	2022	2024	2023	2022
ORANGE	84,8	80,8	84,9	10	16	7
MTN	75,5	68,1	72,6	3	7	6,2
MOOV AFRICA	84,6	65,9	57,3	7	6	14

Le nombre total d'éléments numériques ayant fait l'objet de réquisitions judicaires soumises par les OPJ et validées par les parquets est en baisse.

Sur la totalité des réquisitions judiciaires transmises aux opérateurs télécoms et FAI en 2024, 50% ont été adressées à ORANGE. Le reste est reparti pour 28% à MTN et 22% à MOOV-AFRICA.

Les taux de traitement ont augmenté de 2023 à 2024 de 80,8% à 84,8% pour ORANGE, 68,1% à 75,5% pour MTN et de 65,9 à 84,6% pour MOOV AFRICA.

La durée moyenne de traitement est passée de 16 à 10 jours pour ORANGE. Quant à l'opérateur MTN, la durée moyenne est passée de 7 à 3 jours et enfin MOOV-AFRICA la durée moyenne est de 6 à 7 jours.

La bonne collaboration avec tous les opérateurs et l'utilisation de la plateforme d'échange électronique mise en place par l'ANSSI permettent le traitement accéléré d'un plus grand nombre de demandes. Malgré ces efforts, les délais moyens de traitement de l'ordre d'une semaine restent encore trop longs pour satisfaire les besoins de célérité des procédures judiciaires.

C.3.2.2 OPÉRATEURS DE TRANSFERTS D'ARGENT

En dehors des opérateurs télécoms et ISP dont les performances des services mobile-money sont incluses au point précédent, le tableau ci-dessous reprend les réquisitions adressées aux structures dont l'activité n'est limitée qu'aux transferts d'argent.

	TAUX TRAITE (%)			DUREE MOYENNE (JOURS)		
OPÉRATEUR	**2024**	**2023**	**2022**	**2024**	**2023**	**2022**
WESTERN UNION	100	100	92,8	2	3	3
MONEY GRAM	50	33,3	0,1	4	15	-
WAVE	96,4	96,8	93,6	3	1	7

Le nombre de réquisitions adressées aux opérateurs de transfert d'argent a augmenté de 32% de 2023 à 2024.

Sur la totalité des réquisitions judiciaires relatives aux opérateurs de transferts d'argent en 2024, 84% ont été adressées à WAVE. Les autres se répartissent entre 14% à WESTERN UNION et 2% à MONEYGRAM.

96,4 % des requêtes adressées à l'opérateur WAVE ont été traitées pour une durée moyenne de 3 jours pour l'année 2024.

100% des requêtes WU ont été traitées pour une durée moyenne de 2 jours.

FORMATIONS ET SENSIBILISATIONS

D.1 FORMATIONS ET CONFÉRENCES ANIMÉES PAR L'ANSSI

N°	DATE	THEME	BENEFICIAIRES	NBR PARTICITANTS
1	FEVRIER	Analyse des données téléphoniques et exploitation des sources ouvertes	Togo, Benin, Bureau régional Interpol	20
2	FEVRIER	Premiers intervenants sur la preuve électronique	Autorités de justice pénale du Sénégal	30
3	MARS	Lutte contre la cybercriminalité en milieu ONG	Responsables SOS villages d'enfants ci	20
4	MARS	Droits de l'homme à l'épreuve du phénomène des influenceurs en côte d'ivoire	Comité national des droits de l'homme et groupe d'influenceurs	105
5	AOUT	Retour d'expérience sur la lutte contre la cybercriminalité	CRIET du Benin	35
6	SEPTEMBRE	Vulgarisation des lois et textes ivoiriens en matière de lutte contre la cybercriminalité	Responsables et membres des clubs UA	50
7	SEPTEMBRE	Exploitation des sources ouvertes	Force de Défense et de Sécurité	25
8	OCTOBRE	Les méthodes d'investigation et d'exploitation de la preuve numérique	Unité des services d'enquêtes	18
9	OCTOBRE	Sûreté et protection face au chantage sur les réseaux sociaux et à la cybercriminalité	Grand public	80
10	NOVEMBRE	Investigation sur les crimes sexuels en ligne	Fonctionnaire de police du district de Divo	20
11	NOVEMBRE	Investigation sur les crimes sexuels en ligne	Fonctionnaire de police de la Préfecture de police de San-Pedro	20
12	DECEMBRE	La transformation numérique : innover tout en protégeant les données personnelles	Grand public	110
13	DECEMBRE	Etat des lieux de la cybercriminalité en Côte d'Ivoire et soutien aux investigations	Magistrats du Pôle Pénal Economique et Financier	30
14	DECEMBRE	Sécurité et éthique en ligne : règles et bonnes pratiques pour un espace digital responsable	Grand public	105
TOTAL				**668**

D.2 SENSIBILISATIONS ANIMÉES PAR L'ANSSI

N°	DATE	THÈME	ORGANISATEUR	LIEU	BENEFICIAIRE	NBR PARTICITANTS
1	MARS	Les risques liés à l'utilisation d'internet pour les élèves	École internationale Léonard de Vinci	Abidjan Cocody	Elevés et encadreurs	204
2	MARS	Avoir de bonnes pratiques dans l'utilisation d'internet	Association des usagers d'internet en côte d'ivoire (AUICI)	Grand-Lahou	Chefs d'entreprises et usagers de l'internet	364
3	MARS	Lutte contre la cybercriminalité en milieu ONG	Direction ONG SOS	Abidjan	Grand public	300
4	AVRIL	Eglise évangélique rédemption	Bureau des jeunes	Abidjan	Fidèles	150
5	AVRIL	Les bonnes pratiques internet en milieu professionnel	CRIHD	Abidjan	Grand public	350
6	AVRIL	La cybercriminalité en Côte d'Ivoire	Cyber Africa Forum	Abidjan	Grand public	325
7	AVRIL	Network Security	Talentys	Abidjan	Grand public	310
8	AVRIL	Cybercriminalité en milieu scolaire	Genesis com	Dabou	Elèves	400
9	AVRIL	Cybercriminalité en milieu scolaire et rôle des parents	Ecole Daniélou	Abidjan	Parents d'élèves	200
10	AVRIL	Lutte contre la cybercriminalité en milieu scolaire	Collège Sainte Camille	Abidjan	Elèves	200
11	MAI	Risques lies a l'utilisation d'internet	Ecole ENKO	Abidjan	Elèves	84
12	MAI	Police nationale : je m'engage avec la jeunesse dans la lutte contre la cybercriminalité	Direction DPSD	Man	Grand public	420
13	MAI	Risques liés à l'utilisation d'internet pour les enfants	École N'gatadolikro	N'gatadolikro	Elèves	250
14	MAI	Lutte contre la cybercriminalité en milieu universitaire	Université Al Fourcan	Abidjan	Etudiants	100
15	JUIN	La cybercriminalité en Côte d'Ivoire état des lieux	7eme cour d'Etat-Major Gendarmerie Nationale	Ecole de gendarmerie	Officiers du 7eme cours d'Etat-Major	133
16	JUIN	Intelligence artificielle	SIADE	Abidjan	Grand public	300
17	JUIN	Les données à caractère personnel	Forum sur la protection des données à caractère personnel	Abidjan	Grand public	370
18	JUIN	Risques liés à l'utilisation d'internet	La municipalité d'Adiaké	Adiaké	Grand public	200
19	AOUT	Utilisation responsable des réseaux sociaux	Réseau d'action sur les armes légères en Afrique de l'Ouest (RASALAO-CI)	Bonoua	Grand public	25
20	AOUT	Le musulman et les réseaux sociaux	Association des scouts musulmans	Bingerville lycée Mami Fetai	Grand public	200
21	SEPTEMBRE	Les lois et textes en matière de cybercriminalité	Réseau d'action sur les armes légères en Afrique de l'Ouest (RASALAO-CI)	Abidjan	Grand public	70
22	SEPTEMBRE	A quoi s'expose l'auteur ou le relayeur d'une fausse information	Association population solidaire (APS)	Abidjan Cocody hotel Sofitel Ivoire	Grand public	300
23	OCTOBRE	La citoyenneté numérique	Unesco cote d'ivoire	Cocody	Grand public	100
24	NOVEMBRE	Risques liés à l'utilisation d'internet	PNUD	Divo, San-Pedro	Elèves et responsable des comités consultatifs	805
25	DECEMBRE	Le chrétien et les réseaux sociaux	Eglise du seigneur Jésus Christ	Yopougon	Fidèles	170
26	DECEMBRE	Risques liés à l'utilisation d'internet	Structure de communication police secours	Abengourou	Grand public	110
27	DECEMBRE	Le chrétien et les réseaux sociaux	Paroisse Saint Bernadette	Bingerville	Fidèles	255
28	2024	En ligne tous responsables	Ministère de la communication	Côte d'ivoire	Grand public	22 206
TOTAL						**29105**

CONCLUSION

Globalement, les chiffres 2024 expriment des menaces et risques informationnels croissants liés à des transformations numériques en l'occurence l'usage d'IA, des algorithmes de ciblage, et des techniques d'amplification. La recrudescence en Côte d'Ivoire comme ailleurs dans le monde, de la diffusion de fausses informations, des campagnes de propagande, des atteintes à l'image, à l'honneur et à la dignité, constitue à la fois les conséquences et les moteurs de la radicalisation de nos sociétés.

Pour notre pays, 2025 étant une année particulière en raison des élections au dernier trimestre, le renforcement du dispositif de l'ANSSI s'avère indispensable pour maintenir un niveau de performance élevé, garantir la résilience des infrastructures numériques de l'État, et surtout contribuer efficacement à la paix sociale. En plus des actions déjà engagées, l'efficacité des interventions de l'ANSSI reposera sur la mise à niveau de son dispositif de réponse, fondé sur des technologies innovantes et sur le renforcement de ses ressources humaines en charge de conduire des opérations en ligne.

ANSSI

AGENCE NATIONALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

Créée par le décret **N° 2024-958 du 30 octobre 2024**, l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI) est une agence d'exécution placée sous la tutelle d'une part, du Ministre de la Transition Numérique et de la Digitalisation, pour les matières administratives et techniques propres à la gouvernance et aux missions générales de cybersécurité. Et d'autre part, sous celle du Ministre chargé de la Sécurité, pour les activités et faits de cybersécurité, susceptibles de qualification pénale ou touchant à la sûreté de l'Etat.

A ce titre, elle est chargée de l'exécution des missions suivantes:

- Concevoir et mettre en œuvre les stratégies nationales de sécurité des systèmes d'information.
- Protéger les infrastructures numériques critiques publiques et privées.
- Coordonner la gestion des crises de cybersécurité.
- Surveiller, détecter et répondre efficacement aux menaces.
- Appuyer, avec ses capacités cyber, l'action des forces de sécurité.
- Lutter contre la cybercriminalité.

L'ANSSI en intégrant les missions anciennement dévolues à la DITT ainsi que les activités de cybersécurité et de confiance numérique que gérait l'ARTCI, devient la force unifiée qui oeuvre à travers ses différents centres techniques:

- **PLCC : Plateforme de Lutte Contre la Cybercriminalité**
- **CI-CERT : Côte d'Ivoire Computer Emergency Response Team**
- **SOC : Centre d'Operation de Sécurité Cyber**
- **PKI Racine : Centre de Gestion de la PKI Racine Nationale**
- **CFAD : Centre de Fusion et Analyse de Données**
- **ALERTES 100 : Centre d'alerte**

En combinant expertises et ressources pour apporter une réponse plus rapide et plus efficace, elle incarne la vision de la Côte d'Ivoire de bâtir une Côte d'Ivoire plus résiliente face aux cybermenaces.
Avec l'ANSSI, la Côte d'Ivoire ambitionne de se positionner parmi les leaders africains en matière de cybersécurité et s'engage à garantir la sécurité numérique des citoyens, des entreprises et des institutions.

cybercrime@anssi.gouv.ci

+225 27 22 48 97 77
Abidjan Cocody Danga
Impasse Ablaha Pokou

PLCC

CI-CERT
COMPUTER EMERGENCY RESPONSE TEAM
ANSSI CÔTE D'IVOIRE

ALERTES 100

ATELIERS POUR UNE UTILISATION RESPONSABLE DES RÉSEAUX SOCIAUX À SINÉMATIALI, FERKESSÉDOUGOU ET KONG

03 et le 06 décembre 2024

RENFORCEMENT DES CAPACITÉS DES OFFICIERS DE POLICE JUDICIAIRE SUR LES CRIMES SEXUELS EN LIGNE À SAN PEDRO

29 novembre 2024

SENSIBILISATION À L'USAGE RESPONSABLE DES RÉSEAUX SOCIAUX À BOUNDIALI ET KOUTO

29 novembre 2024

SENSIBILISATION À L'USAGE RESPONSABLE DES RÉSEAUX SOCIAUX À ODIENNÉ

27 et 28 novembre 2024

RENFORCEMENT DES CAPACITÉS DES OFFICIERS DE POLICE JUDICIAIRE À DIVO

CAMPAGNE DE SENSIBILISATION À L'USAGE RESPONSABLE DES RÉSEAUX SOCIAUX À BONDOUKOU

02 OCTOBRE 2024

ENVIRON 200 STAGIAIRES VOLONTAIRES DE L'OFFICE DU SERVICE CIVIQUE NATIONAL DE BIMBRINSSO SENSIBILISÉS À L'UTILISATION RESPONSABLE DES RÉSEAUX SOCIAUX.

25 JUILLET 2024

ANNEXE

UNE RELATION AMOUREUSE QUI VIRE AU CHANTAGE

Menacer de publier ou de relayer des informations portant atteinte à l'image et à l'honneur d'autrui est une infraction sévèrement punie par la loi.
Cependant certains individus, bien que conscients, choisissent de l'ignorer. Ils le font généralement à des fins d'escroquerie ou de vengeance. C'est dans ce contexte de vengeance que JMH s'est retrouvé à la PLCC.

Dame KDC, vivant à Abidjan, fait la connaissance de JMH, résidant dans un pays de l'occident, sur le réseau social Tiktok. Leurs multiples échanges ont conduit à une relation amoureuse virtuelle.
Après quelques mois de relation à distance, JMH décide de se rendre à Abidjan pour officialiser la relation. Chose faite, JMH et KDC procèdent à un mariage coutumier. Tout va bien jusqu'à ce que, JMH à plusieurs reprises, confronté à un refus, décide de rompre. En effet, il exigeait des pratiques que KDC trouvait peu commodes, et a donc refusé catégoriquement et à plusieurs reprises. C'est alors que JMH, mécontent, met un terme à la relation et retourne dans son pays. Ce retour marque la fin de leur relation amoureuse.

Plusieurs jours passent, KDC continue ses activités, et contre toute attente elle est confrontée à une situation angoissante. En effet, elle est contactée un soir, par son amie ALV qui dit avoir reçu des extraits de conversation vidéo montrant sa nudité. Elle affirme que ces images ont été envoyées par JMH, qui aurait menacé de les publier sur les réseaux sociaux. KDC constate qu'il s'agit de vidéos enregistrées à son insu lors des appels vidéos torrides qu'ils faisaient pour pimenter leur amour.
Prise de peur, KDC se rend à la Plateforme de Lutte Contre la Cybercriminalité (PLCC) pour porter plainte.

Les investigations menées par la PLCC appuyée par le Laboratoire de Criminalistique Numérique (LCN) ont permis d'interpeller JMH alors qu'il était de retour à Abidjan. Soumis à une audition, il a reconnu sans grande difficulté les faits. Il dit avoir agi ainsi parce qu'il était en colère. Il dit avoir beaucoup investi de son temps et de son argent dans cette relation. Il ajoute qu'il avait pour but de convaincre KDC de se remettre à nouveau avec lui afin de repartir sur de bons termes. Il affirme également ne pas savoir que le fait de menacer de publier et de publier les images intimes d'une personne soit une infraction.

Pour finir, JMH a été conduit au parquet pour enregistrement illégal, menace de publication et publication d'images à caractère sexuel au moyen d'un système d'information tel que prévu par les articles 62 et 66 de la loi numéro 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.

ILS ESCROQUENT LEURS VICTIMES VIA DES FAUSSES ANNONCES D'EMPLOIS

« Le travail est nécessaire pour l'homme. Il en a inventé le réveil-matin. » Pablo Picasso.
Le travail est indéniablement un pilier de la vie humaine. Avoir un emploi ou une activité afin de subvenir à ses besoins est la volonté de tous. Pour ce faire, il faut s'informer sur les offres d'emploi, postuler et espérer être par la suite retenu au poste voulu. C'est là que les réseaux sociaux entrent en jeu. Ils sont des puissants canaux de communication et favorisent la recherche d'emploi. Les offres d'emploi et recrutements y sont régulièrement publiés.

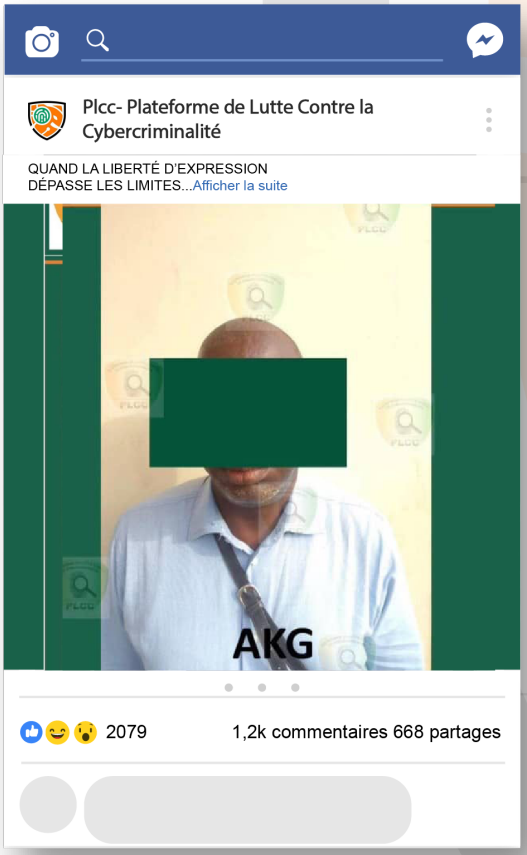
Cependant, il est regrettable de constater que certains individus exploitent cette quête de travail pour commettre des actes répréhensibles. Les cyberescrocs ciblent les chercheurs d'emploi, exploitant souvent la vulnérabilité et le désir légitime de ceux-ci pour les escroquer. Pour atteindre leur but ils utilisent parfois des enseignes d'entreprises sérieuses. C'est le cas de FKE et AJH qui se livraient à ces activités frauduleuses.

Une société de la place (qu'on nommera X) découvre sur Internet des individus utilisant sa dénomination, publiant ceci : « Urgent urgent urgent... Programme de recrutement de la société X, 543 nouveaux postes vacants, logements gratuits pour tous les travailleurs... Contactez-nous vite pour l'ouverture de votre dossier... ». N'ayant jamais initié ce recrutement, la société X saisit la Plateforme de Lutte Contre la Cybercriminalité (PLCC) d'une plainte.

Les enquêtes menées par la PLCC soutenue par le Laboratoire de Criminalistique Numérique (LCN) ont conduit à l'interpellation de FKE. Soumis à une audition, FKE reconnaît être l'auteur de ces fausses annonces de recrutement et avoue qu'il les fait à des fins d'escroquerie. Il ajoute qu'il n'est pas seul à faire cela et dénonce alors AJH, son ami et complice, qui est aussitôt interpellé. Interrogés tous deux, ils avouent pratiquer la cyberescroquerie depuis 2022. Leur technique consiste à faire des publications concernant de faux recrutements et, par la suite, demander un montant pour les frais de visites médicales. Après réception des fonds via des dépôts sur différents numéros, ils bloquent la victime.

Pour finir, FKE et AJH ont été conduits au parquet pour utilisation frauduleuse d'éléments d'identification de personne morale et escroquerie sur Internet.

QUAND LA LIBERTÉ D'EXPRESSION DÉPASSE LES LIMITES



La déclaration universelle des droits de l'homme reconnaît la liberté d'expression comme un droit fondamental, offrant à chaque individu la possibilité d'exprimer ses opinions sur divers sujets, y compris des personnes. Cependant, ce droit comporte des restrictions. En effet, il ne doit pas être exercé au détriment de la dignité d'autrui, et chaque avis formulé doit respecter l'autre. Mais avec l'essor des réseaux sociaux, nous observons malheureusement une prolifération inquiétante de propos diffamatoires, où la liberté d'expression devient parfois un prétexte pour des attaques injustifiées et malveillantes. Pour mieux comprendre les conséquences de ces dérives, nous vous proposons de découvrir l'histoire suivante.

DN, figure influente du monde culturel, mène une vie bien remplie, partagée entre ses responsabilités professionnelles et son attachement aux valeurs familiales. Connu pour son intégrité et son professionnalisme, il utilise activement les réseaux sociaux pour promouvoir ses activités. Cependant, il ne se doutait pas qu'une simple publication sur Facebook deviendrait le point de départ d'un événement qui allait perturber son quotidien. Un matin, DN découvre avec stupéfaction un commentaire hostile sous l'un de ses posts. L'auteur y formule de graves accusations, affirmant que DN aurait expulsé ses propres parents de la maison familiale pour la vendre tout en le traitant de «faux type». Ces propos, empreints de malveillance, mettent en péril non seulement sa réputation, bâtie avec soin, mais aussi l'honneur de sa famille. Refusant que ces allégations infondées restent impunies, il se rend à la Plateforme de Lutte Contre la Cybercriminalité (PLCC) pour porter une plainte.

La PLCC, en collaboration avec le Laboratoire de Criminalistique Numérique (LCN), ouvre une enquête qui conduit rapidement à l'interpellation de AKG. Auditionné, il reconnaît les faits qui lui sont reprochés. AKG explique avoir agi sous l'influence d'une information relayée dans un «grin» du quartier. Selon cette source, DN aurait expulsé ses parents de la maison familiale. Pour exprimer sa solidarité vis-à-vis de la famille, AKG choisit d'utiliser les réseaux sociaux.

Il est important de souligner que le cyberespace ne doit pas être utilisé comme un exutoire pour exprimer ses émotions de manière impulsive. Cet espace est soumis à des règles juridiques qui exigent une conduite responsable de la part de chacun.

Pour conclure, AKG a été conduit au parquet pour atteinte à l'honneur et à l'image, tel que prévu par l'article 60 de la loi N° 2013-451 dU 19 juin 2013 relative à la lutte contre la cybercriminalité.

FALSIFICATION ET USAGE FRAUDULEUX DANS LE SECTEUR BANCAIRE

Dans un monde où les transactions financières reposent sur la confiance mutuelle, la falsification de documents dans le secteur bancaire constitue une menace majeure pour la sécurité et la stabilité économique. Cette infraction consiste à modifier illégalement des documents à valeur juridique ou financière, tels que des contrats ou des relevés bancaires, afin d'obtenir des avantages. En plus des pertes financières, cela affecte la réputation des banques et la confiance des clients, surtout avec l'augmentation des risques liés à la digitalisation. L'histoire suivante nous donnera un meilleur aperçu des méthodes employées par ces faussaires.

Historiquement, les banques sont perçues comme des institutions de confiance pour la gestion des finances des citoyens. Une banque de renom, fidèle à cette tradition, parvient à instaurer un climat de confiance avec ses partenaires et à se forger une solide réputation dans son secteur. Cependant, elle se retrouve confrontée à un cas de falsification de documents compromettant sa stabilité. Après une enquête interne infructueuse, l'institution fait appel à la Plateforme de Lutte Contre la Cybercriminalité (PLCC). Le représentant de la banque, dépose une plainte.

Les investigations menées conjointement par la PLCC et le Laboratoire de Criminalistique Numérique (LCN) conduisent à l'interpellation de GKB. Lors de son audition, GKB minimise son rôle, accusant son ami DL d'être le véritable auteur de la fraude. Il explique qu'au cours d'une soirée bien arrosée, il a révélé à DL qu'il détenait un compte dans une banque réputée. En difficulté financière, DL saisit cette opportunité pour proposer un plan de fraude bancaire. Séduit par la promesse d'une généreuse commission et convaincu de l'absence de risque, GKB accepte de lui fournir un chèque de sa banque. DL tente alors d'organiser un transfert entre deux entreprises, dont il contrôle l'une d'elles. Mais quelques jours plus tard, DL lui annonce que le plan a échoué. Il lui verse tout de même la somme de 300 000 FCFA en guise de dédommagement pour les chèques fournis. GKB ajoute que DL prépare un nouveau coup avec l'aide d'un complice, employé de banque, considéré comme la pièce maîtresse de cette nouvelle arnaque.

DL et ses autres complices ont réussi à extorquer la somme de 50 495 150 francs CFA, tout en dissimulant à GKB le succès de leur escroquerie.
En conclusion, GKB a été conduit au parquet pour complicité de faux et usage de faux en écriture privée de banque. DL et ses autres complices sont toujours recherchés, et leur interpellation sera communiquée ultérieurement.

QUAND LES PRÊTS EN LIGNE DEVIENNENT UN PIÈGE

Les prêts usuraires, connus pour leurs taux d'intérêt abusifs, se caractérisent par des conditions financières particulièrement dévastatrices. Ces pratiques qui sont illégales et immorales, plongent les emprunteurs dans un cycle de dettes insurmontables, tirant profit de leur vulnérabilité. Malgré des régulations mises en place dans de nombreuses juridictions pour atténuer les effets, ces méthodes persistent et s'infiltrent dans diverses sphères économiques

L'histoire qui suit éclaire sur cette pratique inquiétante. Dans l'urgence et en précarité financière, un nombre croissant de personnes se tournent vers des solutions digitales non conventionnelles, appelées "PRÊT EN LIGNE", pour satisfaire leurs besoins immédiats. Malheureusement, ces emprunteurs se retrouvent souvent piégés dans une spirale infernale par des taux d'intérêt exorbitants et des intimidations constantes de la part des prêteurs. Refusant de rester impuissantes face à cette injustice, de nombreuses victimes décident de porter plainte.

La Plateforme de Lutte Contre la Cybercriminalité (PLCC), alertée par 492 plaintes relatives aux pratiques de prêts usuraires en ligne, mène une enquête en collaboration avec le Laboratoire de Criminalistique Numérique (LCN). Ces investigations aboutissent à l'interpellation de plusieurs individus, parmi lesquels ZJM, TR, SAL, ASA, EBE, BEM, CLH, AGH, AMC, BM, YME, YKJ, KMM, BGA, TAG, ACE, PMP, ACN et HAO.

Au cours de leurs auditions, les suspects reconnaissent les faits. ZJM explique que le cerveau de l'opération a créé une plateforme permettant d'octroyer des prêts via des applications mobiles telles que «OZZYMONEY», «CASHARROW», «CRÉDIT CORNET», «JUJUMONEY», «BOMPRÊT», «NANACRÉD», «OCEAN», et «MUMUARGENT».

Il a ensuite constitué plusieurs équipes, chacune se voyant attribuer un rôle précis. La première équipe se charge de la promotion des services sur les réseaux sociaux, vantant des prêts sans engagement, à taux d'intérêt très bas et avec des conditions de remboursement flexibles. Cette approche séduit ainsi de nombreux emprunteurs, attirés par la simplicité d'un prêt sans lourdeurs administratives. Une autre équipe assiste les clients potentiels dans le remplissage du formulaire après le téléchargement de l'application, et une fois le formulaire complété, les fonds sont transférés directement au client par mobile money.

Peu de temps après la contraction du prêt, une troisième équipe d'agents de recouvrement dont ZJM fait partie commence à passer des appels incessants aux clients pour réclamer le remboursement. Ceux qui ne parviennent pas à rembourser dans les délais subissent des hausses de taux d'intérêt quotidiennes. Les prêteurs harcèlent tellement les emprunteurs que certains se retrouvent à rembourser le double, voire le triple du montant initial. Pour ceux qui tentent de résister, une équipe accède à leurs répertoires téléphoniques via une interface, harcelant et menaçant leurs proches pour exercer une pression supplémentaire en vue d'obtenir un remboursement.

Dans le cadre de sa mission régalienne visant à assainir le cyberespace ivoirien, la PLCC a déployé des efforts considérables pour démanteler un autre réseau de prêts en ligne utilisant les mêmes méthodes avec les applications «PRÊT CI» et» BLAZELOAN»
Grâce à un travail acharné et méthodique, la PLCC s'engage à lutter contre ces pratiques frauduleuses qui exploitent la vulnérabilité des emprunteurs. En collaborant étroitement avec des institutions spécialisées et en mobilisant des ressources adéquates, elle vise non seulement à protéger les consommateurs, mais également à restaurer la confiance dans un environnement numérique devenu trop souvent le théâtre d'abus. Cette action déterminée témoigne de la volonté des autorités de garantir un cyberespace sécurisé et respectueux des droits de tous.

En conclusion, ils ont été transférés au Pôle pour prêts usuraires sur internet, de vol de données à caractère personnel et de menaces via un système d'information.

QUAND L'ÉPARGNE COLLECTIVE DEVIENT UN PIÈGE

« Là où l'argent circule, la confiance doit être plus précieuse que l'or. »

Cette citation prend tout son sens dans le contexte actuel des tontines en ligne, un système d'épargne collective basé avant tout sur la confiance entre les membres.
Bien que ces tontines aient historiquement permis à des communautés de s'entraider financièrement, leur transition vers le numérique a ouvert la porte à une nouvelle vague d'escroqueries. Des plateformes frauduleuses et des organisateurs mal intentionnés profitent de l'anonymat du web pour détourner les fonds collectés et disparaître sans laisser de trace, laissant ainsi derrière eux des victimes dont la confiance a été abusée. L'histoire qui suit en est un témoignage concret.

Madame TEM, une jeune femme ambitieuse menant une vie paisible, partage le rêve de nombreux jeunes du 21e siècle : bâtir son propre empire. Elle aspire à l'indépendance financière et pour concrétiser cette vision, elle décide de se constituer une épargne. Cherchant des moyens pratiques d'y parvenir, TEM entend parler des tontines, ces groupes d'épargne collective très populaires dans la société. Curieuse, elle explore les options disponibles et découvre un groupe de tontine en ligne. À sa grande surprise, l'une de ses amies proches en fait déjà partie. Confortée par cette connexion de confiance, elle recueille les informations nécessaires auprès de cette amie et s'inscrit sans hésitation.

Les premiers mois se déroulent à merveille. Madame TEM verse ses cotisations mensuelles avec rigueur et voit ses projets prendre forme. Elle commence à rêver à tout ce qu'elle pourrait accomplir grâce à cette épargne collective. Cependant, un événement familial imprévu vient chambouler ses plans. Elle se retrouve en difficulté financière, incapable d'honorer sa cotisation du mois. Consciente de l'importance de maintenir sa participation, elle contacte rapidement la gérante du groupe espérant obtenir un délai pour régulariser sa situation.

Mais, à sa stupéfaction, la réponse est brutale et inattendue. Sans explication ni avertissement, TEM est exclue du groupe. Confuse, elle tente à plusieurs reprises de joindre la gérante : appels, messages, rien n'y fait. Son inquiétude grandit lorsqu'elle remarque que le groupe en ligne a tout simplement disparu, rompant le lien virtuel et emportant avec lui les fonds qu'elle avait patiemment épargnés. Désemparée, TEM se tourne vers son amie, espérant y trouver des réponses et du réconfort. Mais le choc est encore plus grand lorsque cette dernière lui révèle qu'elle aussi a été dupée par la même arnaque. TEM comprend alors que le groupe de tontine n'était en réalité qu'une vaste escroquerie habilement conçue.

Refusant de rester impuissante face à cette injustice, elle contacte immédiatement la Plateforme de Lutte Contre la Cybercriminalité (PLCC) et expose sa situation dans les moindres détails. Les agents de l'unité, réceptifs à son récit, l'accompagnent dans sa procédure de porter plainte.

Les investigations menées par la PLCC, avec l'appui du Laboratoire de Criminalistique Numérique (LCN) ont conduit à l'interpellation de ZDM. Lors de son audition, acculée par les preuves, cette dernière avoue être l'architecte de cette arnaque. Elle révèle avoir monté un faux groupe de tontine avec des participants fictifs dans l'unique but d'arnaquer son amie TEM et d'autres victimes. Elle admet également avoir usurpé l'identité d'une autre personne pour commettre d'autres fraudes similaires par le passé.
Le montant reçu par ZDM suite à cette escroquerie s'élève à un million quatre-vingt-quatre mille trois cent dix francs CFA (1 084 310 F CFA).

Grâce à la détermination de TEM à obtenir justice et au travail acharné de la PLCC, plus personne ne tombera dans les pièges tendus par ZDM. Cette affaire met en lumière les dangers du monde numérique
et souligne l'importance de rester prudent face à la prolifération des escroqueries en ligne.

Pour conclure, ZDM a été conduit au parquet pour escroquerie sur Internet.

IL ESCROQUE LES VICTIMES EN VIDANT LEUR COMPTE MOBILE MONEY

Avec l'évolution rapide des technologies et la généralisation des services financiers numériques, les plateformes de Mobile Money ont modifié la manière dont des millions de personnes gèrent leur finance. Ces services offrent la possibilité d'effectuer des transferts d'argent et de recevoir des fonds de manière instantanée via un téléphone portable, rendant les opérations financières plus accessibles et pratiques. Cependant, cette adoption massive a également attiré la curiosité des cybercriminels et des escrocs, qui exploitent les vulnérabilités de sécurité et le manque d'information des utilisateurs pour mettre en place des arnaques de plus en plus sophistiquées. Malheureusement, TLI a été victime de ce type de mésaventure.

Madame TLI, gérante d'un point de services Mobile Money, mène une vie bien organisée, marquée par ses responsabilités professionnelles. Chaque matin, avec discipline et rigueur, elle se prépare pour une nouvelle journée de travail. Une fois arrivée sur son lieu d'activité, elle accueille ses clients avec professionnalisme en répondant à leurs différents besoins. Un soir, après une journée bien remplie, alors qu'elle s'apprête à clôturer ses comptes, son téléphone sonne. À l'autre bout du fil, une voix inconnue se présente comme un émissaire de son employeur DZ. L'interlocuteur, au ton rassurant, explique que son patron se trouve à ses côtés et demande à TLI d'effectuer en urgence un dépôt de 2 000 000 FCFA sur un compte créditaire.

Convaincue par ce récit bien structuré et par l'assurance de l'appelant, TLI sans la moindre méfiance réalise la transaction. Ce n'est qu'après avoir exécuté l'opération qu'elle décide d'appeler son employeur pour lui confirmer que la demande a bien été honorée. À sa grande surprise, ce dernier lui répond qu'il n'a jamais mandaté quiconque pour une telle opération.

La réalité s'impose brutalement à Madame TLI : elle vient de se faire escroquer.
Choqué par cette fraude, l'employeur de TLI saisit immédiatement la Plateforme de Lutte Contre la Cybercriminalité (PLCC) et rapporte les faits dans les moindres détails.
Les agents de la PLCC, attentifs et professionnels, assistent DZ dans sa procédure de porter plainte et initient des investigations en collaboration avec le Laboratoire de Criminalistique Numérique (LCN). Ces investigations ont conduit à l'interpellation de KT. Lors de son audition, il reconnaît sans difficulté les faits et détaille plusieurs stratagèmes bien rodés pour extorquer de l'argent.

La première consiste à se rendre dans une agence Mobile Money pour effectuer un dépôt. Plus tard, il contacte la caissière en utilisant le numéro marchand figurant dans le message de dépôt, prétendant appeler au nom du responsable de l'agence pour recharger les comptes marchands. Il communique les informations nécessaires pour effectuer des transactions et s'approprie les fonds.

La deuxième méthode se résume à appeler des numéros de téléphone consécutifs en se faisant passer pour un agent du ministère de la Santé, chargé de l'indemnisation des populations dans le cadre de la COVID-19.

Il informe ses victimes qu'elles sont éligibles à un pack alimentaire et à une somme d'argent, puis leur demande leurs coordonnées personnelles. Il leur fait utiliser un code reçu par message, qui lui permet ensuite de vider leurs comptes.

La troisième stratégie repose sur l'envoi de faux messages de dépôt. KT appelle ensuite ses victimes pour leur demander de renvoyer l'argent, prétendant qu'il s'agit d'une erreur. Pour les convaincre, il propose même un dédommagement. Une fois la transaction effectuée, il dépouille les victimes de leur argent.
Enfin, KT utilise une quatrième méthode en prétendant que ses victimes ont gagné un bonus offert par une compagnie de téléphonie mobile. Il les incite à se rendre dans une agence et leur demande de le présenter à la gérante comme un parent. Il demande ensuite à cette dernière d'effectuer des dépôts, promettant que les victimes régleront les montants. Mais une fois l'opération effectuée, il disparaît, laissant les victimes dans l'incompréhension et endettées.
Les fonds issus de ces arnaques sont transférés directement sur les comptes de ses complices. De cette activité criminelle, KT et ses complices ont soutiré à leurs victimes la somme de 16 000 000 CFA (seize millions de francs CFA).
Il est important de noter que KT et ses acolytes sont liés à 18 plaintes, témoignant de l'ampleur de leur arnaque.

Pour conclure, KT est conduit au parquet pour escroquerie en bande organisée sur Internet. Ses complices sont toujours recherchés par les autorités. Leur arrestation fera l'objet d'une communication ultérieure.

cybercrime@anssi.gouv.ci

+ 225 27 22 48 97 777

Abidjan Cocody Danga, Impasse Ablaha Pokou

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

PLCC
Plateforme de Lutte contre la Cybercriminalité
ANSSI CÔTE D'IVOIRE

CI-CERT
COMPUTER EMERGENCY RESPONSE TEAM
ANSSI CÔTE D'IVOIRE

ALERTES 100