Internet Society
Chapitre Malien

**Mali Next Generation Leaders Program**

# LA CYBERCRIMINALITÉ AU MALI ÉTENDUE ET SANCTIONS.


Rejoignez-nous

Tel: (+223) 66 83 44 86 / 66 74 35 72 / 63 46 67 38
Centre UVA/CISCO Sise à l'ENI
410, Av Vollenhoven - BP 242, Bamako Mali
E-mail : info@isoc.ml
www.isoc.ml
@isocml | #ISOCML
www.facebook.com/isocml

**Mentor: Malick Maiga**

**Rédacteurs: Ousmane SIDIBE**
**Soumaila OUOLOGUEM**
**Sali BARRY**


**Novembre 2022**

## Introduction

Avec le développement accéléré de l'IoT (Internet of Things, l'Internet des Objets), la cybercriminalité est l'un des obstacles majeurs de l'avancée des Tics. Elle est aujourd'hui un défi mondial à relever par les pays et les communautés pour garantir la sécurité des utilisateurs et de l'information.

Pour faire face à ce fléau, la communauté technique ne cesse de développer des moyens plus avancés avec des mises correctives pour garantir la sécurité sur le réseau.

En même temps, les états et les organisations intergouvernementales se dotent de lois et recommandations pour prévenir et protéger les citoyens numériques de la cybercriminalité.

En se référant au cas du Mali qui a 27% d'utilisateur d'Internet selon l'Union internationale des télécommunications dans son rapport et Base de données sur le développement des télécommunications/TIC dans le monde pour 2020.

C'est un pays qui prend son envol pour la numérisation et en faire un levier du développement économique. Il est soucié de l'impact de la cybercriminalité sur son développement, et la mise en application de ses programmes et politiques de développement numérique.

Les délits et infractions liés à l'utilisation de ses outils se sont proliféré ses dernières années sous plusieurs aspects notamment avec le développement des médias en ligne qui prennent de plus en plus de place parmi nos moyens de communication et aussi les cyberattaques contre les infrastructures étatiques.

Internet étant un espace de libre échange et de partage d'information, la nécessité d'endiguer la cybercriminalité de son utilisation pour garantir la confiance et la confidentialité des informations qui y véhicule et permet aux utilisateurs d'en tirer le maximum de profit devient impératif.

C'est dans cette optique que le gouvernement de la République du Mali a adopté la loi N°2019-056 du 05 décembre 2019 portant répression de la cybercriminalité.

Cela nous amène à tout d'abord à définir le concept de cybercriminalité et de délimiter son champ d'application dans le cas du Mali.

## Définition de la cybercriminalité :

De manière générale, la cybercriminalité est l'ensemble des crimes et délits commis dans le cyberespace (par où sur un équipement électronique) visant une personne physique ou morale et les infrastructures informatiques.

Les lois applicables à la cybercriminalité sont relatives aux dispositions des pays et des communautés sous régionales, régionales et mondiales :

- La directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, adoptée lors de sa soixante-sixième session du Conseil des Ministres tenus à Abuja (Nigeria), du 17 au 19 août 2011.
- La convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel signée à Malabo le 27 juin 2014, afin d'harmoniser son application et les sanctions dus au caractère transfrontalier de l'Internet.

Le Mali à travers la loi N°2019-056 du 05 décembre 2019 détermine l'étendu, les infractions, ainsi que la procédure à suivre relative à la cybercriminalité.

Elle est la transposition de la directive portant lutte contre la Cybercriminalité dans l'espace CEDEAO d'août 2011.

Au chapitre II des dispositions générales de cette loi, la cybercriminalité est définie comme étant :
-Toute infraction commise au moyen des technologies de l'information et de la communication en tout ou partie sur le territoire de la République du Mali ;
-Toute infraction commise dans le cyberespace et dont les effets se produisent sur le territoire national.
Et en son chapitre III (voir la loi en annexe), elle définit les termes :
Accès dérobé, accès frauduleux, communication électronique, cybercriminalité, cryptographie, données informatiques, données relatives aux abonnés, données relatives au trafic, maintien frauduleux dans un système informatique, matériel raciste et xénophobe, mineur, pornographie infantile, programme informatique, prospection directe, système d'information, système informatique, technologies de l'information et de la communication et réseaux.

## L'étendue de la cybercriminalité au MALI :

Tels définis par la loi, les crimes et délits liés aux technologies de l'information et de la communication au Mali s'étendent aux infractions suivantes :

- Des atteintes à la confidentialité des systèmes d'information ;
- des atteintes à l'intégrité et à la disponibilité des systèmes d'information ;
- des atteintes à l'intégrité des données d'un système d'information ;
- de l'obtention d'avantage frauduleuse ;
- de la disposition d'un équipement pour commettre des infractions ;
- de l'association formelle ou tentative en vue de commettre des infractions informatiques ;
- de la pornographie infantile ;
- des actes racistes, xénophobes, de menaces et d'injures par le biais d'un système d'information ;
- des infractions liées aux activités des prestataires de services de communication au public par voie électronique ;
- des infractions en matière de prospection directe ;
- des infractions en matière de publicité par voie électronique ;
- des infractions en matière de cryptologie ;
- des infractions commises au moyen des technologies de l'information et de la communication ;
- la responsabilité pénale des personnes morales ;
- des peines complémentaires.

Et les procédures en la matière sont :

- de la preuve électronique en matière pénale ;
- de la perquisition et la saisie informatique ;
- de la conservation des données informatisées stockées ;
- de la collecte en temps réel des données relatives au trafic ;
- de l'interception des données informatisées relatives au contenu ;
- de l'utilisation de logiciels à distance

## Les Sanctions :

Au Mali, la cybercriminalité est sanctionnée par la loi et les peines encourues vont :

- D'un emprisonnement de 2 mois à 5 ans,
- D'une réclusion de 5 à 10 ans,
- D'une amande de 100 000 F CFA à 200 000 000 F CFA.

Des personnes morales et des peines complémentaires :

• De la dissolution ;

• interdiction/fermeture/exclusion, à titre définitif ou pour une durée de 5 ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales, d'une ou plusieurs établissements de l'entreprise, des marchés publics, de faire appel public à l'épargne, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès de ceux qui ont certifié ;

• la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est produite ;

• l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public, par voie électronique ;

• interdiction d'émettre des messages de communication électronique ;

• interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction ou l'injonction d'en couper l'accès par tous les moyens techniques disponibles ou même en interdire l'hébergement ;

• la confiscation des outils qui ont servi à commettre l'infraction ou qui en sont produits,

• l'interdiction d'exercer une fonction publique ou une activité liée à la cryptologie pour une durée de 5 ans au plus ;

• la fermeture de l'un ou des établissements de l'entreprise ayant servi à commettre les faits incriminés pour une durée de 5 ans au plus ;

• l'exclusion des marchés publics pour une durée de 5 ans au plus.

## Conclusion

Nous pouvons dire que la cybercriminalité est un fléau auquel les états et les communautés doivent faire face pour garantir la sécurité des utilisateurs et les ressources pour maintenir la confiance dans le cyberespace.

Le Mali, aujourd'hui à l'aide de cette loi, ouvre la voie pour une meilleure utilisation des outils numériques sur son espace géographique, maintenir l'ordre et le respect de la vie privée des utilisateurs et aussi garantir la confiance des internautes.