

Leçon 8 : La cybercriminalité

Avec l'évolution des TIC, il n'est plus rare de voir que l'espace numérique est de plus en plus le lieu pour commettre des agissements répréhensibles de toutes sortes, attentatoires tant aux intérêts des particuliers qu'à l'intérêt général aussi bien sur le plan national qu'à l'échelle internationale. C'est ainsi que les systèmes ou réseaux informatiques tout comme les données informatisées sont la cible d'agissements cybercriminels. De même, les technologies de l'information et de la communication, notamment l'Internet, sont utilisées comme moyens aux fins d'agissements répréhensibles.

Cette délinquance sur internet ou cyberdélinquance est dénommée cybercriminalité. Notons que de manière générale, la cybercriminalité se caractérise par sa transnationalité, son immatérialité, sa volatilité et l'anonymat (hypothétique) de ses acteurs. Ces caractères sont de nature à brouiller les repères du système pénal traditionnel conçu et élaboré pour un environnement matérialisé et national. Ce qui imposait alors un défi d'adaptation du dispositif pénal à l'effet de saisir efficacement cette nouvelle réalité de délinquance numérique aussi bien en droit substantiel qu'en droit processuel. Dès lors, il était nécessaire d'élaborer une cyberstratégie de traitement de cette criminalité numérique, par une adaptation du système pénal, articulée autour de la modernisation des incriminations du droit pénal classique et de l'aménagement des instruments procéduraux traditionnels par rapport aux technologies de l'information et de la communication. C'est ce à quoi répond la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.

I – La consécration d'infractions spécifiques aux TIC

Face à la prolifération des actes de délinquance numérique et dans l'optique d'une dissuasion et/ou répression pénale, le dispositif pénal ivoirien a été revu et reformé pour mieux répondre aux enjeux qu'imposent l'utilisation répréhensible des TIC. En ce sens, le droit pénal substantiel a été reformé et étoffé à travers la consécration d'infractions spécifiques aux technologies de l'information et de la communication.

A – L'atteinte au système informatique

Au terme de la loi 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité en Côte d'Ivoire, le *système informatique* ou *système d'information* s'entend de « tout dispositif isolé ou non, tout ensemble de dispositif interconnecté assurant en tout ou partie, un traitement

automatisé de données en exécution d'un programme ». Selon la loi, système informatique et système d'information ont le même sens.

Aussi, l'atteinte au système informatique peut se manifester de diverses façons. Il peut s'agir d'un accès ou un maintien frauduleux dans le système informatique ; d'une entrave au fonctionnement du système informatique ou encore de l'introduction frauduleux de données dans le système informatique. La loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité appréhende et réprime ces diverses atteintes au système informatique.

1 – L'accès ou le maintien frauduleux dans le système informatique

L'article 4 de la loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité incrimine et punit **l'accès illégal au système informatique**. Ainsi peut-on lire au terme de l'article 4 qu'« *Est puni d'une peine d'emprisonnement de un (01) an à deux (02) ans et d'une amende de 5.000.000 à 10.000.000 francs CFA, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique* ».

Comme l'infraction d'accès illégal au système informatique, la loi ivoirienne de lutte contre la cybercriminalité incrimine et punit **le maintien illégal dans un système informatique**. C'est ce que prévoit l'article 5 de loi n°2013-451 du 19 juin 2013 qui dispose qu'« *Est puni d'une peine d'emprisonnement de un (01) an à deux (02) ans et d'une amende de 5.000.000 à 10.000.000 francs CFA, quiconque accède ou tente d'accéder frauduleusement à tout ou partie d'un système informatique* ».

2 – L'entrave illégale au fonctionnement du système informatique

Le fait d'entraver ou même la tentative d'entraver le fonctionnement normal d'un système informatique est une infraction prévue et punie par la loi relative à la lutte contre la cybercriminalité. En effet, conformément à l'article 6 de la loi 2013-451 du 19 juin 2013, « *Est puni d'un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque entrave, fausse ou tente d'entraver ou de fausser frauduleusement le fonctionnement d'un système d'information* ».

3 – L'introduction frauduleuse de données dans un système informatique

Le fait d'introduire ou même de tenter d'introduire frauduleusement des données dans un système informatique est une infraction prévue et punie par la loi relative à la lutte contre la

cybercriminalité en Côte d'Ivoire. En effet, l'article 6 de la loi 2013-451 du 19 juin 2013 dispose qu'« *Est puni d'un à cinq ans d'emprisonnement et de 10.000.000 à 40.000.000 de francs CFA d'amende, quiconque introduit ou tente d'introduire frauduleusement des données dans un système d'information* ».

B – L'atteinte illégale aux données informatiques

Les *données informatiques* ou encore appelées simplement les *données* sont définies par la loi 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité en Côte d'Ivoire à son article premier comme « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information* ». Aussi, l'atteinte illégale aux données informatiques peut prendre plusieurs formes.

1 – L'interception frauduleuse de données informatiques

Le fait d'intercepter ou même de tenter d'intercepter frauduleusement des données informatiques est une infraction prévue et punie par la loi relative à la lutte contre la cybercriminalité. En effet, l'article 8 de la loi 2013-451 du 19 juin 2013 prévoit qu'« *Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque intercepte ou tente d'intercepter frauduleusement par des moyens techniques des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système d'information* ».

2 – L'altération ou la suppression frauduleuse de données informatiques

Le fait d'altérer, modifier ou supprimer frauduleusement des données informatiques est une infraction prévue et punie par la loi. Tout comme la tentative, même non réussie, d'altérer, de modifier ou de supprimer des données informatiques. C'est ce que prévoit l'article 9 de la loi 2013-451 relative à la lutte contre la cybercriminalité. En effet, peut-on y lire que qu'« *Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque altère ou tente d'altérer, modifie ou tente de modifier, supprime ou tente de supprimer frauduleusement des données informatiques* ».

3 – La contrefaçon ou dénaturation de données informatiques

La contrefaçon de données informatiques consiste à produire ou à fabriquer un ensemble de données informatiques contrefaites à travers la manipulation de données informatiques préexistantes dans le but d'utiliser les données contrefaites comme si elles étaient originales. Cette contrefaçon de données informatiques est prévue et punie par l'article 10 de la loi 2013-451 qui dispose qu'« *Est puni de cinq à dix ans d'emprisonnement et de 40.000.000 à 60.000.000 de francs CFA d'amende, quiconque produit ou fabrique un ensemble de données par l'introduction, la modification, l'altération ou la suppression frauduleuse de données informatiques, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales* ».

4 – L'usage frauduleux de données informatiques

La loi sur la cybercriminalité ne sanctionne l'interception frauduleuse de données informatiques, elle criminalise et sanctionne également l'usage de telles données frauduleusement obtenues. C'est ce que prévoit l'article 11 de la loi 2013-451 selon lequel : « *Est puni d'un à cinq ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque fait usage, en connaissance de cause, de données informatiques frauduleusement obtenues* ».

5 – L'obtention frauduleux d'avantages issus de données informatiques

A l'image de l'usage de données informatiques frauduleusement obtenues, il est interdit de tirer un quelconque profit illégitime des données informatiques d'un système informatique. En effet, l'article 12 de la loi sur la cybercriminalité prescrit qu'« *Est puni d'un à cinq ans d'emprisonnement et de 30.000.000 à 50.000.000 de francs CFA d'amende, quiconque obtient frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'utilisation, la modification, l'altération ou la suppression de données informatiques ou par toute forme d'atteinte au système d'information* ».

6 - Le traitement illégal de données ou de dispositif informatique

Il est important aussi de savoir que tout traitement illégal de données ou de dispositif informatique engage la responsabilité pénale de son auteur. En ce sens, l'article 13 dispose qu'« *Est puni d'un an à deux ans d'emprisonnement et de 10.000.000 à 50.000.000 de francs CFA d'amende, quiconque, dans l'intention de commettre l'une des infractions prévues par la*

présente loi produit, vend, importe, détient, diffuse, offre, cède ou met à disposition, en connaissance de cause :

- un équipement, une disposition ou un programme informatique ;*
- un mot de passe, un code d'accès ou des données informatiques similaires ».*

II – L’adaptation des infractions classiques aux TICS

A – L’infraction d’association de cybercriminels

L’association de malfaiteur est une infraction classique prévue et punie par le code pénal. Dans l’environnement numérique, il n’est pas impossible qu’une bande organisée commette des actes répréhensibles. C’est dans ce sens que l’article 14 de la loi 2013-451 sur la cybercriminalité incrimine et punit ce que l’on peut qualifier d’association de cybercriminels. En effet, peut-on lire au terme dudit article 14 qu’« *Est puni de dix à vingt ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque participe à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente loi* ».

B – L’infraction de pornographie infantile au moyen des TIC

La loi ivoirienne 2013-451 relative à la lutte contre la cybercriminalité incrimine et punit sévèrement la communication électronique d’image ou de représentation présentant un caractère de pornographie infantile. Quatre (04) articles ou dispositions de la loi 2013-451 portent sur les aspects pénaux de la pornographie infantile dans l’espace numérique.

C’est ainsi que, tout d’abord, l’article 15 dispose qu’« *Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque produit, enregistre, offre, met à disposition, diffuse, transmet une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques* ». Ensuite, l’article 16 prévoit qu’« *Est puni de deux à cinq ans d'emprisonnement et de 75.000.000 à 100.000.000 de francs CFA d'amende, quiconque se procure ou procure à autrui, importe ou fait importer, exporte ou fait exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système d'information ou d'un moyen de stockage de données informatiques* ». Aussi, l’article 17 prescrit qu’« *Est puni d’un à trois ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque possède intentionnellement une image ou*

une représentation présentant un caractère de pornographie infantile dans un système d'information ou dans un moyen de stockage de données informatiques ». Enfin, l'article 18 dispose qu'« **Est puni d'un à cinq ans d'emprisonnement et de 20.000.000 à 40.000.000 de francs CFA d'amende, quiconque facilite l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur** ».

C – Les infractions relatives à l'identité, la correspondance ou à l'information en ligne

1 – les infractions numériques portant sur l'identité ou les DCP

L'utilisation frauduleuse des éléments d'identification d'une personne physique ou morale via les TICS est une infraction punie par la loi. En effet, l'article 19 prescrit qu'est « **puni de deux à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende, quiconque utilise frauduleusement un ou des éléments d'identification d'une personne physique ou morale par le biais d'un système d'information** ». Il en est de même, en thème de sanction, « *quiconque utilise, possède, offre, vend, met à disposition, transmet en toute connaissance de cause de fausses données d'identification* » (al.2, art.19). De plus, l'alinéa 3 du même article, prévoit que « quiconque réalise ou tente de réaliser de fausses données d'identification est puni de deux à cinq ans d'emprisonnement et de 5.000.000 à 10.000.000 de francs CFA d'amende.

Par ailleurs, le fait d'utiliser « *les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site Internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles* » est puni d'une peine **d'emprisonnement d'un an à cinq ans et d'une amende de 5.000.000 à 100.000.000 de francs CFA**. Mieux, la peine d'emprisonnement ne peut être inférieure à cinq ans et la peine d'amende ne peut être inférieure à 20.000.000 de francs CFA, lorsque les données à caractère personnel ou les informations confidentielles communiquées **ont servi au détournement de fonds publics ou privés**.

En outre, le fait de dissimuler l'identité de la personne pour le compte de laquelle une offre commerciale est émise ou mentionne une offre sans rapport avec la prestation ou le service proposé est une infraction punie d'une peine d'emprisonnement d'un mois à un an et d'une amende de 500.000 à 1.000.000 de francs (art.23, loi 2013-451

Enfin, et relativement aux données à caractère personnel, il est important de relever en vertu de l'article 24 qu'est « puni d'une **peine d'emprisonnement d'un à cinq ans et de 5.000.000 à**

100.000.000 de francs CFA d'amende, quiconque procède au traitement de données à caractère personnel par un moyen frauduleux, déloyal ou illicite ». Et lorsque le traitement frauduleux, déloyal ou illicite des DCP a été faite par une personne morale, autre que l'Etat dans le but d'envoyer des spams, **la peine d'amende ne peut alors être inférieure à 10.000.000 de francs CFA.**

2 – Le spamming ou l'envoi de message électronique non sollicités

Le spamming qui dérive du mot anglo-saxon "spam", peut être défini comme le fait d'utiliser « *des procédés illicites d'envoi de messages électroniques non sollicités sur la base de la collecte de données à caractère personnel* ». Au terme de l'article 22 de la loi sur la cybercriminalité, « *Est puni d'une peine d'emprisonnement d'un à cinq ans et d'une amende de 1.000.000 à 10.000.000 de francs CFA, quiconque utilise des procédés illicites d'envoi de messages électroniques non sollicités sur la base de la collecte de données à caractère personnel* ».

3 – Le vol d'information

Le vol d'information est une infraction prévue et punie par la loi 2013-451 relative à la lutte contre la cybercriminalité. Le vol d'information peut être appréhendé comme le fait, pour quiconque, de « *prendre frauduleusement connaissance d'une information à l'intérieur d'un système d'information électronique, ou copie frauduleusement une information à partir d'un tel système, ou encore soustrait frauduleusement le support physique sur lequel se trouve une information* » (art.26, al.1). Quiconque s'adonne à une telle pratique est coupable de vol d'information. Le vol d'information est puni, selon l'alinéa 2 de l'article 26, « *d'un emprisonnement de cinq à dix ans et de 3.000.000 à 5.000.000 de francs d'amende* ». Aussi, il est important de relever que la tentative de vol d'information également punissable selon la même disposition.

Le vol d'information ou la tentative de vol d'information est puni « *d'un emprisonnement de dix à vingt ans et d'une amende de 5.000.000 à 10.000.000 de francs CFA* » en vertu de l'article 27 de la loi 2013-451, s'il « *a été commis accompagné d'une au moins des circonstances ci-après : avec des violences ayant entraîné des blessures ; avec effraction, escalade ou usage de fausse clé ; en réunion par au moins deux personnes ; avec usage frauduleux, soit d'un uniforme ou d'un costume d'un fonctionnaire public, civil ou militaire, soit d'un titre d'un fonctionnaire, soit d'un faux ordre d'une autorité civile ou militaire ; dans une maison*

habitée ou servant d'habitation ou dans les locaux professionnels ; avec l'usage d'un masque ; avec l'usage d'un véhicule pour faciliter son entreprise ou sa fuite ; la nuit ».

En revanche, le vol d'information ou la tentative de vol d'information est puni de vingt ans d'emprisonnement et de 10.000.000 de francs CFA d'amende, s'il est accompagné de l'une des circonstances ci-après : lorsque l'auteur ou le complice est porteur d'une arme apparente ou cachée ; lorsque l'auteur ou le complice a fait usage d'une arme ayant entraîné des blessures ou la mort de la victime(art.28). De plus, lorsqu'elle est faite intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission d'un vol d'information, ou l'usage d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information, dans l'intention qu'ils soient utilisées afin de commettre l'une ou l'autre des infractions prévues par la présente loi, est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée d'entre elles.

En outre, observons que lorsque les faits punis par la présente loi portent sur un système d'information ou un programme de traitement de données protégé par un code d'accès secret, la peine encourue ne peut être inférieure à dix ans d'emprisonnement (art.30).

Enfin, l'article 31 de la loi 2013-451 dispose en son alinéa 1^{er} qu'« *Est puni d'un emprisonnement d'un à cinq ans et de 1.000.000 de francs CFA d'amende, quiconque de mauvaise foi, ouvre, supprime, retarde ou détourne des correspondances électroniques arrivées ou non à destination et adressées à un tiers, ou en prend frauduleusement connaissance* ». Est puni des mêmes peines, en vertu de l'alinéa 2 de l'article 31« *quiconque de mauvaise foi, intercepte, détourne, utilise ou divulgue des correspondances électroniques émises, transmises ou reçues par la voie des télécommunications ou procède à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

III – La consécration de sanction complémentaire aux peines principales

L'une des particularités ou caractéristiques du droit pénal numérique ivoirien, c'est qu'au-delà du fait que chaque infraction est nécessairement sanctionnée par une double peine d'emprisonnement et d'amende à titre principal, le législateur ivoirien a également assorti ces mêmes infractions de peine à titre complémentaire. C'est ce qui résulte de l'article 32 de la loi

2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité. On y lit que « *Les personnes condamnées pour les délits prévus au présent chapitre encourent également les peines complémentaires suivantes :*

- *l'interdiction, pour une durée de cinq ans, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;*
- *la confiscation du moyen qui a servi à commettre l'infraction ou qui était destiné à la commission de l'infraction ou du bien qui en est le produit;*
- *la fermeture, pour une durée de cinq ans s'il y a lieu, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;*
- *l'exclusion pour une durée de cinq ans, des marchés publics;*
- *l'interdiction, pour une durée de cinq ans d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés;*

l'affichage ou la diffusion de la décision prononcée, aux frais du condamné ».