

REPUBLIQUE DE COTE D'IVOIRE

CONFERENCE REGIONALE AFRICAINE SUR LA CYBERCRIMINALITE

ABIDJAN, COTE D'IVOIRE
DU 17 AU 20 OCTOBRE 2008

DOSSIER DE PRESSE

I- CONTEXTE GENERAL

Le terme « cybercriminalité » a été inventé à la fin des années quatre-vingt-dix, alors qu'Internet se répandait en Amérique du Nord. Un sous-groupe des pays du G8 fut formé suite à une réunion à Lyon, en France, afin d'étudier les nouveaux types de criminalité encouragés par, ou migrant vers, internet. Ce « groupe de Lyon » employait alors « cybercriminalité » pour décrire, de manière relativement vague, tous les types de délits perpétrés sur Internet ou les nouveaux réseaux de télécommunications, dont le coût chutait rapidement.

Dans la même période, et à l'initiative des membres du groupe de Lyon, le Conseil de l'Europe commença à rédiger un projet de *Convention sur la Cybercriminalité* [1]. Celle-ci, rendue publique pour la première fois en 2000, prévoyait un nouvel ensemble de techniques de surveillance que les organismes chargés de l'application de la loi estimaient nécessaires pour combattre cette nouvelle forme de criminalité.

La version finale de la convention susmentionnée, adoptée en novembre 2001 après les événements du 11 septembre de la même année, ne donnait une définition explicite. Cependant, le terme était plutôt utilisé comme une sorte de fourre-tout pour désigner les nouveaux problèmes auxquels se trouvaient confrontés la police et les agences de renseignement, et découlant des performances toujours meilleures des ordinateurs, de la baisse du coût des communications, et du phénomène Internet. La convention énumère les différentes dispositions et les domaines exigeant une nouvelle législation. Ce sont :

- Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ;
- Infractions informatiques [falsification et -fraude] ;
- Infractions se rapportant au contenu [pornographie] ;
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes ;
- Autres formes de responsabilité et de sanctions [aide et complicité, responsabilité des personnes morales].

Comme on peut le noter, la **Cybercriminalité est la boîte de Pandore**. Ce d'autant plus que les dispositions relatives aux crimes, en réalité, sont très brèves, la majeure partie de la Convention traitant de droit procédural et de coopération internationale. Pour que les

poursuites aboutissent, il fallait trouver de nouvelles techniques pour réunir des preuves, assurer leur intégrité, et les partager par delà les frontières. Les injonctions de conservation rapide de données stockées, les mandats électroniques, le recueil de données en temps réel, l'archivage des données relatives au trafic : autant de mesures qui impliquaient une intrusion dans les libertés civiles. Une dépendance croissante des traités mutuels d'assistance légale, même quand il ne s'agissait pas d'un cas de double incrimination, ouvrait une boîte de Pandore d'accusations criminelles possibles selon tous les régimes du monde. Alors que la *Convention sur la Cybercriminalité* énumère clairement les problèmes propres aux enquêtes criminelles au niveau mondial, elle ne propose toujours pas de solution pour protéger la vie privée et les droits humains.

En tout état de cause, la notion de cyber-criminalité était appliquée à de nouveaux types de criminalité, comme la cyberpornographie - c'est-à-dire la diffusion de photographies violant les lois de certains pays (mais pas tous) relatives à la pornographie inacceptable et l'exploitation des personnes. Comme Internet ignore les frontières, il était devenu beaucoup plus facile de diffuser des contenus à l'étranger, parfois de manière complètement anonyme. Pénétrer dans les systèmes informatiques, ou les « pirater », constituait aussi un nouveau crime, alors que de nombreux pays ne le considéraient pas encore comme une infraction criminelle. La *Convention sur la Cybercriminalité* visait entre autres à établir et harmoniser les dispositions qui devaient être intégrées dans la législation des pays signataires, afin de lutter de manière bien coordonnée contre cette nouvelle activité criminelle. Les jeux d'argent en ligne soulevaient un autre problème : des champs de courses virtuels fleurissaient sur Internet, et bien que les pays aient des approches très différentes, suffisamment de pays développés intégraient les revenus tirés des jeux d'argent dans les budgets nationaux et les économies du tourisme, de sorte que l'émergence de concurrents virtuels, opérant depuis des paradis fiscaux, ont fini par susciter une réelle inquiétude. Dans ce contexte devenu complexe à cause notamment de la révolution industrielle, chaque pays se donne les moyens de lutte contre ce que certains spécialistes de la question appréhendent comme une « mafia », celle de la cyber-criminalité.

II- LA PROBLEMATIQUE DE LA CYBERCRIMINALITE EN AFRIQUE

Le forum sur la criminalité tenu du 18 au 19 juin 2008, à Abidjan, a permis, à travers des exposés des spécialistes de la question, de faire une analyse économique du phénomène pour en appréhender les conséquences et proposer des solutions idoines. Il en est ressorti que l'économie numérique est une source incontestable de croissance économique (Rapport OCDE, 2003), et contribue à la baisse des coûts de production, à l'émergence des entreprises en réseau, au développement du commerce électronique (e-commerce). En d'autres termes, l'économie numérique favorise une mutation économique. Ce faisant, la diffusion du service Internet se fait de plus en plus à grande échelle aussi bien dans le monde que dans des continents comme l'Afrique où la vitesse d'adoption des Techniques de l'information et de la communication est plus élevée selon un rapport de la CNUCED. En effet, l'Afrique compte 24 millions d'internautes (2,6% du total mondial en 2008). Déjà en 2006, le nombre total d'internautes dans le monde entier était estimé à 1,1 milliards. Cette expansion est aussi à la base de la prolifération d'activités illégales ou criminelles sus indiquées et bien d'autres comme spams, virus, spyware, phishing, etc. qui constituent une réelle menace pour les entreprises et les personnes physiques.

Selon une étude (2007) de l'Union Internationale des Télécommunications (UIT) et de la Conférence des Nations Unies pour le Commerce et le Développement (CNUCED), de 2003 à 2007, le nombre de spams reçus par les entreprises a augmenté de plus de 80%. Par ailleurs, les emails reçus par les internautes sont de 75% de spams. Les sites d'anarques visent, dans 85% des cas, des entreprises opérant dans le secteur de la finance.

Au niveau des pertes causées par la cybercriminalité, les chiffres sont effarants : 20,5 milliards de dollars en 2003, et 198,3 milliards de dollars en 2007 (soit 90% de hausse en quatre ans. En termes de revenus générés par les solutions anti-spams, on en a enregistré 88 millions de dollars en 2002 et 1,740 milliard de dollars en 2008. Au regard de ce qui précède, il s'avère nécessaire de comprendre la rationalité du cybercriminel à travers une analyse de la structure des coûts et des bénéfices afin de lutter efficacement contre le crime opéré via Internet.

III- JUSTIFICATION DE LA CONFERENCE REGIONALE AFRICAINE SUR LA CYBERCRIMINALITE.

Après le Forum sur la cybercriminalité de juin 2008, il est apparu nécessaire de créer un cadre de réflexions périodiques pour combattre le mal qui se propage dans presque tous les pays africains. Au début de l'année 2008, les fournisseurs d'accès Internet ont fait le constat que le volume de spams ou courriers électroniques non sollicités, et dont l'objectif est d'escroquer est devenu considérable. Ces spams ou courriers électroniques non sollicités proviennent, en majorité de la Côte d'Ivoire. Une situation favorisée sans doute par la situation de guerre et de crise que le pays a connue de 2002 à ce jour, et qui focalise les autorités davantage sur la gestion de la crise que la Cybercriminalité. Bien que ce phénomène peut constituer une «*arme de destruction massive*» de l'économie plus que des armes conventionnelles.

Face à la prolifération de ces emails indésirables disséminés à partir de la Côte d'Ivoire, de nombreux pays africains ont demandé aux Autorités ivoiriennes de prendre des mesures susceptibles d'aider à endiguer ou à défaut à maîtriser le phénomène. Faute de quoi, ces pays menacent d'interdire l'accès de leurs sites aux internautes naviguant à partir de la Côte d'Ivoire.

Ces pratiques répréhensibles posent le problème général de la cybercriminalité qui, avec le développement de l'Internet s'est amplifié pour atteindre aujourd'hui des proportions inquiétantes.

Face à l'ampleur de ces actes cybercriminels dont les conséquences sont désastreuses pour l'économie et l'image du pays, l'Agence des télécommunications de Côte d'Ivoire (ATCI) a décidé de porter une attention particulière à la question en faisant de la cybersécurité, son cheval de bataille. A cet effet, l'Agence a entrepris une série d'actions relatives aux aspects techniques et à la sensibilisation globale des internautes.

- créer un cadre de concertation avec les fournisseurs d'accès Internet en vue de déterminer les mesures techniques immédiates à mettre en œuvre ;
- susciter l'émergence de discussions entre les acteurs nationaux à travers forum et conférences afin d'éveiller la conscience nationale sur le sujet.

C'est dans ce cadre qu'en juin 2008, en partenariat avec l'Internet Society chapitre de la Côte d'Ivoire, l'ATCI a organisé (18 et 19 juin 2008) **un forum national sur la cybersécurité**, pour sensibiliser la communauté nationale sur le phénomène.

Ce forum, faut-il le rappeler, visait trois objectifs spécifiques suivants :

- sensibiliser les acteurs nationaux, le gouvernement, le secteur privé et la société civile sur les enjeux liés à la cybersécurité ;

- faire un état des lieux et identifier les tendances fortes en matière de protection de l'information et des réseaux d'information au plan national ;
- réunir les spécialistes et les parties prenantes pour proposer des solutions en vue de définir une stratégie nationale en matière de cybersécurité,
- sensibiliser les acteurs nationaux, le gouvernement, le secteur privé et la société civile sur les enjeux liés à la cybersécurité ;
- faire un état des lieux et identifier les tendances fortes en matière de protection de l'information et des réseaux d'information au plan national ;
- réunir les spécialistes et les parties prenantes pour proposer des solutions en vue de définir une stratégie nationale en matière de cybersécurité.

La Conférence régionale africaine sur la cybersécurité qui se tient du **08 au 10 octobre 2008**, à la salle de **Conférence de la CGRAE**, au Plateau (Côte d'Ivoire) se situe dans le prolongement des réflexions et recommandations du Forum sus indiqué. Elle est co-organisée par la Côte d'Ivoire et l'**Organisation internationale de la francophonie (OIF)**, en relation avec l'**Union africaine**.

IV- RESULTATS ATTENDUS

- Elaboration d'un code de surveillance de l'utilisation de l'Internet ;
- La lutte contre la cybersécurité engage tous les acteurs en Côte d'Ivoire ;
- L'image de la Côte d'Ivoire réhabilitée ;
- La cybercriminalité drastiquement réduite et les sites Internet crédibilisés
- La législation ivoirienne réprime à des peines lourdes les cybercriminels (sanctions surtout pénales)

V- PARTICIPANTS

- les opérateurs du secteur des télécommunications dont les fournisseurs d'accès Internet ;
- les gestionnaires des cybercafés, lieux par excellence de l'utilisation de l'Internet ;
- les différents services de police (police économique, police judiciaire et police scientifique) qui sont au quotidien charges de lutter contre la cybercriminalité ;
- la société civile : les associations de promotion de l'utilisation des tic, les associations de consommateurs et le grand public ;
- experts nationaux et internationaux en matière de cybersécurité.

GOORE-BI HUE
 Journaliste - Economiste - Experts consultant -
 Rédacteur en chef : Indice Africaine -
 Chef de rédacteur économique du groupe Fraternité Matin