Cybercriminalité en RD Congo :
Faire du vieux avec du neuf, pour un renouveau sans révolution

La cybercriminalité est un fait de la société postmoderne. Il est le fléau du « tout numérique » et du « tout connecté » pour notre époque contemporaine.

L'accroissement des cyber-attaques est lié au développement des réseaux de communications électroniques, à la généralisation d'Internet dans les entreprises et dans notre quotidien, de même qu'à l'accès facilité et continu aux informations sensibles, aux données personnelles ou autres au sein des organisations. La RD Congo compte plus de 35 millions d'abonnés téléphoniques et un peu moins de 16 millions d'internautes mobiles, avec un taux modeste mais significatif de pénétration des TIC dans les ménages.

Si le minerai informationnel attire des convoitises, les prouesses de contournement des pare-feux stimulent un nouveau profil de Lombroso.

I. Un profil cybercriminel très varié

Des jeunes surdoués de l'art informatique agissent, sans histoire et sans casier judiciaire, souvent paradoxalement sans intention de nuire, avec la puissance du code informatique pour des intrusions dans des systèmes d'information, des manipulations des données, des blocages et détournements des dispositifs informatiques. Des cyber-soldats, des cyber-espions, des hactivistes ou des opportunistes jouent les saltimbanques, flibustiers et corsaires face à tous ceux qui naviguent sur Internet ou y surfent. Le cyber-terroristes de Daesh, l'état islamique, a fait usage de la peur, du recrutement des djihadistes, de la radicalisation des blasés du mode de vie occidentale ou de épris d'un nouveau exotisme politique. Internet a été le terreau fertile de Daesh dans ses objectifs… Que dire des pédocriminels et de la maffia ayant intégré le web dans leurs approches lubriques ou lucratives !

En Afrique de l'ouest, les « brouteurs » hameçonnent des pigeons qu'ils font chanter en échange de la compromission sexuelle de leurs victimes devant une webcam contre de fortes sommes d'argent pour payer leur silence. L'« escroquerie à la nigériane » porte encore la nationalité des spécialistes qui vous envoient un email de notification de gain à une loterie à laquelle vous n'avez jamais misée ou d'un héritage confisqué dans une banque qui requiert votre aide pour un partage de la bonne fortune…

Pris dans les méandres du cybercriminels, la victime est dans une très mauvaise fortune.

II. Une variété d'infractions dans le seul vocable cybercriminalité

La cybercriminalité ne correspond pas à une infraction précise. Elle n'est ni futuriste ni surréaliste à l'envie. Elle n'est pas aussi récente dans son analyse que l'intellection profane entend le faire croire. Déjà en 1975, l'Institut de recherche Stanford donnait de la cybercriminalité une déclinaison bipartite de droit pénal général. Aujourd'hui, avec les travaux de la magistrate française, Myriam Quéméner notamment, l'approche générique, en la matière, englobe trois catégories d'activités répréhensibles dans la cybercriminalité.

1. Ce sont d'abord les *infractions anciennes de droit commun* pour lesquelles l'Internet est le moyen facile de leur perpétration, telles que les escroqueries, injures publiques et diffamations perpétrées en ligne...
2. Ce sont ensuite les *infractions informatiques au sens strict* pour lesquelles l'informatique est la cible ou l'objet, comme le piratage dit en anglais le « hacking », l'accès illicite aux bases de données...
3. Ce sont enfin les *infractions de diffusion en ligne*, celles dont la condition d'existence est la divulgation d'information liées à la vie intime ou à la sphère privée sur le support électronique grand public, comme la revanche pornographique (France), l'enregistrement des conversations téléphoniques privées à l'insu de l'interlocuteur en vue de leur diffusion (Sénégal)…

III. Un volet cybercriminalité et un volet cybersécurité

La cybercriminalité, en tant que nouvelle forme de délinquance, s'accompagne largement d'un sentiment d'impunité et du mythe du « vide juridique ». Les cyber-délinquants éprouvent de la « sécurité derrière leurs écrans. La Justice a du mal à se déployer sur les béants interstices des lois pénales non mises à jour. Les services d'ordre public ont maille à partir avec les caractéristiques techniques du cyberespace : volatilité apparente des données en cause, anonymat primaire des avatars informatiques.

La technologie numérique est très évolutive. L'intelligence inventive met à rude épreuve les efforts étatiques de maîtrise de l'Internet lui-même et du phénomène criminel y afférent. Il ne sera pas abusif de voir en la disponibilité du réseau électronique et des outils numériques une popularisation des potentielles « armes du crime ». Ces dernières seraient à la portée d'internautes évoluant dans un cyberspace sans shérif. La puissance du code informatique porte à la fois la marque du progrès des libertés et le masque des offenses aux mêmes libertés. La rhétorique informatique procure aux actes posés en ligne la dimension internationale qui dépasse les frontières des États ainsi que leurs capacités à y répondre isolément.

La cybersécurité est la réponse à la fois multidimensionnelle et multipartite face à la cybercriminalité. Elle postule que la sécurité informatique est assurée si le système réunit son authenticité, sa disponibilité et son intégrité. Elle postule également de faire de chaque acteur, dans leurs comportements, les acteurs de cette sécurité. Elle organise à la fois :

- la prévention : réunissant les moyens de détection des menaces et de préservation des infrastructures vitales avant la survenance des sinistres informatiques,
- la résiliente : assurant la continuité du fonctionnement du système par des mesures de contingentement ou autres limitant le désastre, pendant le traitement offensif ou défensif de l'incident ;
- la répression : dotant les services de justice des dispositions législatives, de la politique cybercriminelle, des laboratoires de criminalistique informatique, en vue de l'instruction judiciaire et de la connaissance juridictionnelle des cas de cybercriminalité.

IV. Un code pénal de 1940 toujours prêt à l'emploi

Face aux nouveaux enjeux de cybercriminalité, le Décret du 30 janvier 1940 portant le code pénal congolais n'est pas totalement dépassé. Plusieurs de ses incriminations restent applicables à la criminalité informatique du 21e siècle.

Toute la cybercriminalité n'est pas que faite d'incriminations nouvelles. Le vieux répond bien du nouveau à plusieurs égards. Il est plaisant de subodorer une rime logique entre révolution numérique et révolution juridique. Cependant, le fameux « *code is law* » de Lawrence Lessig (USA, 1999) ou la déclaration de l'indépendance du Net de John Perry Barlow (Davos, 1996), pour paraître subjuguant, n'est ni l'un ni l'autre guère subrogeant de nos anciennes les lois pénales. Même si le Digital défie l'Etat de droit, notre législateur est vieux sans être un vétéran de la cyber-guerre. Certains voient en lui un pépé *BBC, born before computer,* né avant l'invention de l'ordinateur, face à des *digital natives*, ceux qui sont nés avec le clavier et la souris d'ordinateur dans la main.

Toutefois, en son état quinquagénaire, le code pénal ordinaire congolais sert l'actualité de la répression de plusieurs comportements cybercriminels. Il reste efficace particulièrement pour les infractions classiques qui trouvent leur facilité de commission grâce à l'Internet. Injurier publiquement, diffamer, violer le secret des correspondances, divulguer le secret professionnel dont l'avocat, le ministère public, le notaire… est dépositaire n'ont pas à attendre un législateur futuriste pour être qualifiés d'infractions du moment que l'auteur se trouve sur Internet ou utilise un Smartphone.

La RD Congo n'est pas dépourvue d'incriminations légales dans tous les compartiments de la cybercriminalité. La loi-cadre n°013/2002 du 16 octobre 2002 sur les télécommunications en République démocratique du Congo prévoit des délits et des peines face à la levée de secrets de correspondances par la voie des ondes, en protégeant ainsi les données nominatives et autres à caractère personne dans les réseaux téléphoniques. Plus tôt, l'ordonnance n°87-243 du 22 juillet 1987 sur l'activité informatique au Zaïre avait déjà prévu des peines d'amende contre les usages informatiques qui seraient subversifs ou contraires aux bonnes mœurs.

Ce n'est que la méconnaissance de ces textes qui laissent aller à des conclusions, laissant à désirer, sur l'absence de cadre légal de lutte contre la cybercriminalité en RD Congo.

V. Une flopée d'incriminations applicables d'ores et déjà face à la cybercriminalité

La cybercriminalité congolaise a déjà des rudiments de réponse dans nos lois pénales.

1. Les infractions d'imputations dommageables et les injures publiques même commises sur Internet restent punies par le Code pénal. Aux termes de son article 74, la diffamation consiste à imputer méchamment et publiquement à une personne un fait précis qui est de nature à porter atteinte à l'honneur ou à la considération de cette personne, ou à l'exposer au mépris public. La diffamation, comme l'injure publique prévue à l'article 75 du même code, ne peut exister que si elles sont perpétrées « publiquement » contre les particuliers ou les entités. La publicité, qui en est le moteur, s'entend d'après les circonstances et les lieux. En tant qu'« espèce d'espace » à la George Perec, Internet est une agora que fréquente un public

indifférencié. Ce qui fait de lieu le carrefour des mondes virtuel et réel : le sixième continent formant le territoire opérationnel et directionnel du crime dématérialisé. Si la convergence numérique est l'apothéose du multimédia (son, texte, image animée ou non-animée), elle est aussi le véhicule de nouvelles apologies des délits informationnels à distance. Tous les moyens modernes de diffusion de la pensée sont à considérer comme réalisant cette condition de publicité requise pour les imputations dommageables et les injures publiques. (LIKULIA B., *Droit pénal spécial Zaïrois*, tome I, 2e éd., Paris, LGDJ, p. 231.)

2. Le fait de trafiquer les comptes informatiques d'une banque ou les écritures comptables, entre bien dans le champ de l'infraction de faux en écriture, prévu aux articles 124 à 127 du Décret du 30 décembre 1940 du code pénal congolais.

3. La non-livraison des marchandises, causée intentionnellement par un professionnel après signature d'un contrat de vente électronique, est punissable au titre d'abus de confiance, tel que prévu à l'article 95 du code pénal. Il en est de même de l'article 98 du même code qui peut s'appliquer aux escroqueries sur Internet.

4. Que dire du comportement déviant de certains agents publics, des dépositaires de missives personnelles, des coursiers ou des préposés aux courriers officiels qui s'adonnent, ces derniers temps, à leurs publications sur les réseaux sociaux numériques ? L'article 71 du code pénal congolais sanctionne de tels comportements au titre de violation de secrets de correspondance. De même, l'article 73 punit la révélation de secrets professionnels. Ces dispositions visent expressément les personnes dépositaires par état ou par profession de tels secrets. Tel en est du magistrat tenu au secret de l'instruction, de l'avocat tenu au secret des informations lui révélées par son client dans un lien professionnel de confiance. En effet, l'article 74 de l'ordonnance-loi nº79-028 du 28 septembre 1979 portant organisation du barreau, du corps des défenseurs judiciaires et du corps des mandataires de l'État dispose : « il est interdit aux Avocats […] de révéler les secrets qui leur sont confiés en raison de leur profession ou d'en tirer eux-mêmes un parti quelconques ». Le mandat de l'avocat l'oblige un devoir envers son client, sous peine de sanction d'ordre public pour protéger la prérogative que tel mandat engendre. Sa violation, soit-elle en ligne ou hors ligne, constitue une faute disciplinaire grave et une infraction pénale.

5. Dans une jurisprudence de 2018, le Tribunal de paix de la Gombe condamnait un célèbre député provincial sur le pied de l'article 1er de l'Ordonnance-loi du 16 décembre 1963 réprimant l'offense envers le chef de l'état pour des contenus outrageant trouvés sur son téléphone et son activité connectées.

6. L'exposition ou la publication sur Internet des images obscènes et/ou immorales peut être sanctionnée sur base de l'article 175 du code pénal qui incrimine l'outrage aux bonnes mœurs. La comparution devant le Procureur d' Héritier Watanabé et sa copine Naomie prouvent cette assertion, pour le motif de dévoilement public de leurs images enlacées, comme des lotus, dans une alcôve où les actes qu'ils posaient sous caméra devaient rester « enfants non-admis ».

7. L'utilisation des canaux numériques pour harceler, menacer une personne de façon malicieuse en vue d'obtenir des faveurs sexuelles notamment par l'envoi répété des SMS, e-mails non-sollicités peut constituer le harcèlement prévu à l'article 174-d du code pénal modifié et complété par la loi n°06/018 du 20 juillet 2006 sur les violences sexuelles. L'article 174-m du code pénal, tel que modifié et complété par la même loi, punit au titre de la pédopornographie, quiconque aura fait toute représentation, quel que soit le moyen (y compris sur Internet), d'un enfant s'adonnant à des activités sexuelles ou toute représentation des organes sexuels d'un enfant, à des fins sexuelles.

Le droit positif congolais dispose donc d'une légion d'exemples de droit pénal spécial contre la cybercriminalité. Il faut néanmoins reconnaître, au-delà du développement ci-dessous, que la déviance informatique déborde du cadre de notre dispositif législatif répressif.

VI. Une plaie de la modernité : pansement à changer, changement à penser

Evolution et révolution ? Bâtir la virtualité sur la réalité ? Faire peau neuve sur peau de chagrin ? La cybercriminalité est la plaie du web. Il ne faut ni s'arrêter à changer de pansement (avec du vieux), ni s'abstenir à penser le changement.

Il n'existe pas d'infractions sans loi, ni de sanctions pénales sans elle. Le droit pénal est de stricte interprétation. L'interprétation téléologique est permise en droit pénal, bien avant le vol de l'électricité. Notre poussée pour la téléologie voudrait spécialement aboutir à une qualification judiciaire du « vol des données » sur la base de l'article 79 du code pénal.

Toutefois, un nouveau catalogue d'incriminations doit s'ajouter à l'ère numérique. Les nouvelles infractions n'ayant (eu) leur existence que grâce au réseau numérique et à la révolution connectée. Le législateur renforcerait ainsi le dispositif répressif national en légiférant contre des infractions informatiques au sens strict. Autant d'anglicismes que sont : *hacking* (piratage informatique), *cracking* (bris de coffre-fort numérique), *ransomware* (logiciels malveillants), *bot nets* (ordinateurs Zombies), *phreaking* (fraude téléphonique), phishing (hameçonnage, filoutage), espiogiciels (logiciels espions), *porn revenge* (revanche pornographique)… témoignent de la nouveauté des modes opérationnels de l'informatique qui caractérisent ces cyber-infractions qui portent définitivement leurs noms.

Le statut de lanceurs d'alerte et des libertaires sont aussi un enjeu législatif. Les paradigmes Edward Snowden (NSA) et Assange (Wikileaks) font des émules et offrent une impunité, mieux une immunité, en faveur de ceux qui divulguent des informations secrètes. Le but est altruiste. La tendance est celle du droit sans limitation à s'informer et à informer, du droit de savoir et de faire savoir, du droit non-privatif d'accès aux « communs informationnels ». C'est là que la cause « hacktiviste » distingue le délinquant hacker du héros de la presse. Entre la sécurité née de la peur et la liberté née de l'audace, leur alliage produira la sagesse.

VII. Une perspective heureuse d' « informatique légale » en RD Congo

Notre position, d'ores et déjà, avec ou sans téléologie, est de soutenir que la législation anticriminelle en vigueur ici et maintenant, reste largement applicable à la cybercriminalité,

dernière-née de la société de l'information. Selon certaines sources, sources certaines néanmoins, 1882 plaintes semblent avoir été enregistrées entre fin 2017 et mi-2018, par la DTNTIC de la Police Nationale Congolaise.

Face à ces chiffres gris de la Cybercriminalité congolaise, la grande problématique demeure la difficulté majeure d'administration de la preuve informatique, de détection de l'identité numérique, de l'indentification de la personne derrière ses traces informatiques.

C'est en ce sens que le Ministre de la Justice dans son communiqué de presse du 15 mai 2020 annonce le renforcement des moyens de politique criminelle. La criminalistique informatique devrait venir en appui du travail d'instruction et des poursuites criminelles au profit des parquets aux prises aux plaintes de cybercriminalité.

La mise en place d'un laboratoire moderne d'« *inforensic* », en anglais, est l'atout majeur du FBI et d'Europol. La France dispose de son « Procureur numérique », le seul ayant juridiction sur l'ensemble de l'Hexagone, vu le substrat déterritorialisé des infractions de sa compétence. La formation des autorités judiciaires devra être couplée à la démarche. Le tout en un devra assurer la performance de l'« informatique légale ». Cette dernière consiste en l'application de techniques et de protocoles d'investigation numériques respectant les procédures légales et destinée à apporter des preuves numériques à la demande d'une institution judiciaire par réquisition, ordonnance ou jugement.

Elle permettra à la Justice de la RD Congo d'adresser les problématiques suivantes :

- investigations informatiques,
- télé-perquisitions,
- exploitation des sources techniques,
- relevé des traces technologiques de connexion, de navigation.

Sans coopération internationale, ni entraide judiciaire, le combat national sera esseulé à la Don Quichotte, porté par moulin à parole contre moulins à vent… L'ère numérique tourneboule la vue d'infractions de nouvel ordre et de genre nouveau.

VIII. Un épilogue pour un « universalisme pluriel » contre la cybercriminalité

La RD Congo devrait envisager son adhésion à la Convention du Conseil de l'Europe sur la cybercriminalité, dite Convention de Budapest conclue en 2001, en vigueur en 2004, comme instrument efficient de portée mondiale. Il faut aussi s'intéresser à la ratification de la Convention sur la cybersécurité et la protection des données personnelles, adoptée en 2014, par une déclaration des Chefs d'Etats et de gouvernement de l'Union africaine. Seuls la Guinée, le Sénégal et le Congo/Brazza, en attendant son entrée en vigueur au seuil de sept ratifications.

Fait à Kinshasa, les 23 mai 2020.

Kodjo NDUKUMA ADJAYI
Professeur des universités
Master 2 en Droit du cyberespace africain
Spécialiste du droit comparé et du droit du Numérique
Docteur en sciences juridiques de l'Université Paris 1 Panthéon Sorbonne