PUBLICATION AU TITRE D'UNE PRE-CONTRIBUTION
AU XXXVI ème CONGRES DE L'IDEF SUR LE THEME :

« Le droit face aux défis des enjeux du numérique »

Mis à jour: 04 juin 2020

Les banques de l'espace OHADA face aux cyberattaques liées au COVID-19 : quelles leçons tirer de l'expérience chinoise ?

Par

KOUMAKO Yao Justin, Juriste internationaliste - Cybersécurité

Résumé :

Le COVID-19 a augmenté le risque cyber auquel s'exposent les entreprises en général et les banques en particulier. La Chine qui a connu premièrement cette pandémie a dû faire face à des cyberattaques ciblant ses banques et cette problématique se pose avec acuité dans d'autres Etats à l'heure où ces lignes sont écrites. Les banques OHADA qui n'ont aucune raison d'en être épargnées se doivent de prendre des mesures idoines pour prévenir les cyberattaques liées au COVID-19 afin de protéger leurs systèmes d'information et préserver les intérêts de leurs consommateurs.

Outre les craintes sanitaires qu'elle suscite, la flambée épidémique du COVID-19 fait courir des risques énormes aux entreprises en général et au secteur des services financiers en particulier. Au rang de ces risques, figure l'invisible cyberrisque[1] qui s'avère tout aussi imprévisible que le COVID-19 lui-même.

En effet, à l'heure où l'on recense les multiples défis que le COVID-19 pose aux Etats, aux administrations, aux entreprises et aux populations, le risque cyber n'est plus une hypothèse mais une réalité. Cette réalité, des particuliers, des hôpitaux[2], des entreprises[3], des villes, et des Etats ont été déjà

[1] L'OCDE définit le risque comme *« l'effet de l'incertitude sur l'atteinte des objectifs »* et le cyber risque comme *« une catégorie de risques liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit », voir* OCDE, Gestion du risque numérique pour la prospérité économique et sociale : recommandations de l'OCDE et document d'accompagnement, Éd. OCDE, Paris, 2015 cité par AJILI BEN YOUSSEF (W.) in « Les cyber risques : nature, étendue et moyens de couverture », *Lamyline,* Droit et Patrimoine, Nº 298, 1er janvier 2020.

[2] Les cyberattaques visant les centres de santé impliqués dans la lutte contre l'épidémie est un sujet d'inquiétude majeur. Le 21 Mai 2020, 128 juristes internationaux ont signé la déclaration d'Oxford sur les protections du droit international contre les cyberopérations visant le secteur médical dans le but de dénoncer ces pratiques.

contraints d'y faire face parallèlement à la lutte sans merci qu'ils livrent à la pandémie. Dans la lutte contre les cybermenaces liées au COVID-19, les banques et leurs consommateurs sont en première ligne.

A la vérité, dans le contexte actuel de crise sanitaire mondiale, les banques sont des « proies convoitées des hackeurs »[4] et pour cause. Il faut dire que si les institutions financières ont de plus en plus recours aux nouvelles technologies à des fins diverses[5], la crise sanitaire a suscité le nécessaire recours à de nouveaux usages de ces technologies pour assurer la continuité des services pendant que les agences doivent rester, pour la plupart, fermées. Les banques de l'espace OHADA sont aussi contraintes de recourir à ces usages[6]. Les autorités monétaires africaines recommandent d'ailleurs la pratique massive des services bancaires en ligne afin de limiter les affluences dans les agences bancaires.

Ce recours au numérique, est en fait normal et s'impose même, dans une période où les clients sont confinés dans beaucoup de pays d'Afrique également et que la distanciation sociale oblige le personnel à faire du télétravail. Seulement, chaque mécanisme technologique se nourrit de données personnelles et les données bancaires sont des données sensibles de la plus haute importance. Cette importance leur vaut d'être appelées le nouvel « or noir ». Fort de cette importance, elles sont la cible des cybercriminels qui usent de cyberattaques pour les dérober[7].

---

[3] Le 21 Mai 2020, la compagnie aérienne EasyJet a déclaré avoir été victime d'une cyberattaque ayant compromis les données de 9 millions de ses clients ainsi que 2.208 données bancaires

[4] CHOCRON (V.), « Les nouvelles cyberattaques qui menacent les banques et leurs clients », *Le Monde*, publié le18 Novembre 2019, consulté le 30/04 2020, https://www.lemonde.fr/economie/article/2019/11/18/les-nouvelles-cyberattaques-qui-menacent-les-banques-et-leurs-clients_6019524_3234.html]

[5] Les banques ont recours à l'intelligence artificielle, le machine learning ainsi que le développement des robots (Robotic Process Automation) à des fins d'optimisation des processus internes et de réduction des coûts.

[6] Groupe Ecobank, *Le Groupe Ecobank contribue à la lutte contre le COVID-19 à hauteur d'environ 3 millions de dollars sur l'ensemble de son réseau en Afrique*, Communiqué de presse, 20/04/2020

[7] En juillet 2019 par exemple, la banque américaine Capital One Financial a été victime d'une cyberattaque ayant entraîné le vol des données personnelles de 100 millions de ses clients américains et 6 millions de ses clients canadiens [https://www.ledroit.com/affaires/vol-de-donnees-de-106-millions-de-clients-chez-capital-one-eb7d050b665d66fe9182c171e02ce11b]

Mis à jour: 04 juin 2020

Pour atteindre leur but, les cybercriminels suivent et surfent sur l'actualité. Depuis le début de la pandémie du COVID-19, ils naviguent sur la vague sanitaire[8]. Selon le groupe Thalès, de nombreux noms de domaine en lien avec la pandémie ont été créés dont plus de 50% pourraient être liés à des logiciels malveillants[9].

Ainsi, la Chine, qui a dû affronter le COVID-19 avant le reste du monde, a signalé à travers sa Commission de réglementation des banques et des assurances plusieurs arnaques qui ont touché des banques nationales.[10]

En tirant leçons de l'expérience des banques chinoises et étrangères, à quoi doivent s'attendre les banques de l'espace OHADA et comment doivent-elles se préparer pour minimiser le risque cyber ?

L'expérience des banques étrangères est pleine de leçons pour les banques OHADA (II) et les oblige à bien se préparer étant donné que les banques sont une cible de choix pour les cybercriminels (I).

I. Les banques, une cible de choix pour les cybercriminels

Il est établi que les banques sont les meilleures cibles des cybercriminels en temps de crise. En cette période de COVID-19, la vigilance des banques chinoises leur a permis de n'avoir qu'une faible sinistralité de cybercriminalité liée à la pandémie (A) alors que d'autres pays ont été confrontés à des expériences similaires (B).

A. La faible sinistralité de l'expérience des banques chinoises

Les cybercriminels, confinés ou non, ne connaissent pas de trêve. Certaines banques chinoises et leurs consommateurs l'ont appris, à leurs dépens. La Commission chinoise de réglementation des banques et

[8] Dans son article, "Ransomware attacks spike 148% amid COVID-19 scams", HARDCASTLE (J.) rapporte: « Between February and March, the threat researchers saw a 38% increase in cyberattacks against financial institutions », consulté le 22/04/2020 [https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/]

[9] Groupe Thales, « Le COVID-19, une nouvelle arme pour la cybermalveillance », consulté le 01/05/2020, [https://www.thalesgroup.com/fr/marches-specifiques/systemes-dinformation-critiques-et-cybersecurite/news/le-covid-19-une-nouvelle]

[10] Florian Dèbes, « Les cyberattaques capitalisent sur le coronavirus », *Les échos*, 11/03/2020

des assurances a signalé que plusieurs banques nationales ont été victimes de cyberescroqueries liées à la crise sanitaire qu'a connue la Chine. Selon l'institution, les banques nationales ont reçu de nombreuses plaintes concernant des « fausses informations sur la situation de la maladie pour frauder ou nuire aux intérêts des consommateurs »[11]. Il s'est principalement agi d'attaques connues sous les noms de *phishing* ou d'hameçonnage[12]. Les consommateurs chinois ont ainsi reçu des mails supposés émaner de leurs banques les invitant à cliquer sur des liens pour effectuer des opérations ou obtenir remboursement de voyages ou de réservation d'hôtel annulés. Les personnels des banques travaillant à domicile auraient également été destinataires de ces courriels.

Cependant le taux de sinistralité de ces attaques sur les banques chinoises ainsi que sur leurs clients s'est avéré relativement faible. Comment les banques chinoises notamment celles de Hong-Kong se sont-elles organisées pour contrer la cybermenace ?

Bien avant que la pandémie n'atteigne son pic en Chine, près de quatre douzaines de banques à Hong Kong ont fait une simulation intéressante. Elles ont été confrontées à un scénario de «test de résistance» cauchemardesque: une pandémie qui a balayé la ville, suivie d'une cyberattaque majeure et d'une panne des télécommunications[13]. Sans qu'il soit nécessaire de revenir sur les détails de cette simulation, il est intéressant de noter que cet exercice préventif a été le fer de lance dans la riposte anticipative contre les cybermenaces liées au COVID-19. Il a en effet amené les banques à reconsidérer la façon dont elles traitaient les données sensibles lorsque le personnel travaillait à domicile sur des systèmes plus ou moins sécurisés. En ce qui concerne les clients, une bonne communication a permis de les avertir pour leur éviter de tomber dans les pièges tendus par les cybercriminels.

La Chine n'est pas une exception. D'autres Etats ont connu une trajectoire similaire dans les cyberattaques liées au COVID-19.

---

[11] « Les craintes liées au coronavirus exploitées par les cyberattaques », [https://complyadvantage.com/fr]
[12] Tout comme le pêcheur qui utilise un hameçon avec un appât pour capturer ses poissons dans la rivière, le cybercriminel utilise un email présenté comme authentique pour appâter sa victime. En y mordant (en cliquant sur le lien contenu dans le mail), la victime se laisse avoir et donne au cybercriminel, un accès intégral à ces données personnelles.
[13] Voir https://www.reuters.com/article/us-china-health-hongkong-finance-idUSKBN2070N2

B. La forte similarité des expériences observées dans d'autres Etats

Selon une étude réalisée par le Centre d'analyse technique des cybermenaces du groupe Thalès, *« les cyberattaques suivent la même évolution que le virus à travers le monde, avec des attaques importantes en Asie, puis en Europe Centrale et de l'Est et en Europe de l'Ouest »*[14]. Ainsi, au fur et à mesure que le COVID-19 atteint les pays, on observe des cyberattaques sous diverses formes. Les cas du Singapour et de la France sont intéressants pour les besoins de la présente analyse.

A Singapour, l'autorité monétaire a instruit les institutions financières à prendre des mesures qui s'imposent pour protéger leurs systèmes d'informations suite à des cyberattaques[15]. Pour comprendre la situation singapourienne, il faut procéder à une analyse chronologique. Le premier cas de COVID-19 a été détecté à Singapour le 7 février 2020. Le gouvernement a donc relevé son niveau d'alerte intitulé « Disease Outbreak Response System Condition (DORSCON) » du niveau jaune au niveau orange[16]. Le 09 Février 2020, soit 48h après, les premières cyberattaques liées au COVID-19 visant les banques ont été signalées au MAS alors même que les mesures de distanciation sociale impliquant le télétravail n'étaient pas encore prises par le gouvernement singapourien[17]. Ensuite, conformément aux mesures prises par le gouvernement, l'autorité monétaire a exhorté les particuliers et les entreprises à utiliser les services financiers numériques et les paiements électroniques afin de recourir le moins possible aux visites dans les locaux des institutions financières. Ce recours systématique aux services financiers numériques a donc induit une augmentation sévère des attaques visant d'une part les télétravailleurs pour accéder aux bases de données de leur banque et d'autre part les usagers pour leur soustraire des informations confidentielles. Le MAS n'a pas fait de communication détaillant les attaques visant les systèmes d'information de ses institutions, mais concrètement en ce qui concerne les usagers, les attaquants vont jusqu'à se faire passer pour le ministère de la santé pour demander les informations bancaires.

---

[14] Groupe Thales, « Le COVID-19, une nouvelle arme pour la cybermalveillance », *op. cit.*

[15] « Monetary Authority of Singapore (MAS) has also reminded financial institutions that they should remain vigilant on the cyber security front as there have been cases of cyber threat actors taking advantage of the 2019 Novel Coronavirus (2019-nCoV) situation to conduct email scams, phishing and ransomware attacks" [https://www.mas.gov.sg/news/media-releases/2020/mas-urges-use-of-digital-finance-and-e-payments-to-support-covid-19-safe-distancing-measures]

[16] Troisième niveau sur 4 au total

[17] En effet, il faut attendre le 20 Mars 2020 que le le ministère singapourien de la santé prenne des mesures strictes de distanciation sociale en mettant un accent particulier sur la nécessité pour les entreprises de privilégier le télétravail dans la mesure du Singapore, Voir Ministry of Health, « Stricter Safe Distancing Measures to Prevent Further Spread of Covid-19 Cases », 20/03/2020

PUBLICATION AU TITRE D'UNE PRE-CONTRIBUTION
AU XXXVI ème CONGRES DE L'IDEF SUR LE THEME :

« Le droit face aux défis des enjeux du numérique »

Mis à jour: 04 juin 2020

En France, le COVID-19 a beaucoup servi aux cyberattaques qu'il n'y paraît. Tout d'abord, dès le début de la crise, l'Assistance publique des hôpitaux de Paris a subi une cyberattaque ayant nécessité la coupure des accès externes aux mails et des outils de télétravail. Il s'est agi d'une attaque de déni de service communément connu sous le nom de DOS.[18] Ensuite, c'était au tour de la ville de Marseille de subir une attaque *ramsomware ou* rançongiciel. Cette attaque a été d'une grande ampleur avec de lourds dégâts. L'agence nationale de sécurité des systèmes d'information (ANSSI) s'en est d'ailleurs saisie. Dans un document rendu public faisant état de rapport sur l'analyse de l'attaque, l'agence déclare que le rançongiciel utilisé contre la ville de Marseille est dénommé Mespinoza/Pysa[19]. Il est important de rappeler que les cybercriminels ont demandé une rançon pour déchiffrer les données de la ville.

Les exemples peuvent être multipliés en France. Cependant, aucune banque, à notre connaissance, n'a été directement l'objet de cyberattaque à l'exception de la banque postale dont les clients sont visés par des arnaques relatives à des pseudo-colis. La culture de cybersécurité des banques françaises et la mobilisation des institutions nationales pour assurer la veille de cybersécurité pendant la « guerre sanitaire »[20] sont des éléments qui, jusqu'alors, ont permis d'avoir des résultats satisfaisants. Ainsi l'ANSSI et cybermalveillance.gouv.fr publient régulièrement les nouveaux types d'attaques liées au COVID-19 tout en prenant soin de rappeler les mesures pour s'en prémunir.

---

[18] Selon le Lexique sur le cyberespace, une attaque par déni de service « consiste à cibler un serveur, une adresse mail et à l'inonder de requêtes ou de mails. Imaginons des milliers de lettres que l'on essaie de faire entrer de force dans une boîte aux lettres individuelle placée dans l'entrée d'un immeuble : la boîte sature, la cage d'escalier est inondée de courrier, l'entrée de l'immeuble est bloquée. L'attaque peut être provoquée d'un poste, par un seul individu (attaque dite DOS pour *Deny of Service*) ou en mettant en œuvre un réseau d'ordinateurs robots, dit zombies, à travers un *botnet* (voir définition *botnet*), terme dérivé de *robot-network*. On parle alors d'attaque DDOS pour *Distributed Denial Of Service* ou « déni de service distribué ». Ce type d'attaque est très difficile à contrer. L'attaque DOS, par contre, peut se régler plus facilement, en inscrivant en site indésirable sur son pare-feu l'adresse IP (voir définition adresse IP) d'origine de l'attaque. » DESFORGES (A.), ENGUERRAND (D.), « Lexique sur le cyberespace », *Hérodote*, vol. 152-153, no. 1, 2014, pp. 22-25.

[19] Selon ce rapport, « Le rançongiciel Mespinoza est utilisé depuis octobre 2018 au moins. Ses premières versions produisaient des fichiers chiffrés portant l'extension «.locked», commune à de nombreux rançongiciels .Depuis décembre 2019, une nouvelle version de Mespinoza est documentée en source ouverte, parfois appelée Pysa car elle produit des fichiers chiffrés portant l'extension «.pysa».

[20] « Nous sommes en guerre, en guerre sanitaire, certes : nous ne luttons ni contre une armée, ni contre une autre Nation. Mais l'ennemi est là, invisible, insaisissable, qui progresse. Et cela requiert notre mobilisation générale ».
Discours d'Emmanuel MACRON, le 16 Mars 2020

Ces expériences pourraient inspirer les banques de l'espace OHADA dans leur stratégie numérique pendant la crise sanitaire.

II. Les leçons pour les banques de l'espace OHADA

Au regard des expériences étrangères et de multiples autres raisons, les banques de l'espace OHADA doivent prévenir les cyberattaques (A). Pour cela, cet article se veut un réceptacle de quelques mesures phares à adopter pour s'assurer une sécurité numérique pendant la pandémie (B).

A. Des raisons plurielles d'adopter une approche préventive

Si de nombreuses campagnes de cyberattaques ont été observées ailleurs dans le monde contre des banques, les banques de l'espace OHADA n'ont aucune raison d'en être épargnées surtout quand on sait que les Etats membres de l'espace OHADA et leurs voisins sont des Etats depuis lesquels beaucoup de cyberattaques sont souvent menées[21].

Pour les banques de l'espace OHADA, il s'agit d'un véritable sujet d'inquiétude d'autant plus que le voisin nigérian est considéré comme un épicentre de la cybercriminalité où s'est développé au fil des années, une véritable économie souterraine de cybercriminalité. Par ailleurs, les « brouteurs » en Côte-d'Ivoire, les « gays man » au Bénin, les « fay man » au Cameroun élaborent des techniques pour arnaquer aussi bien les entreprises locales qu'étrangères. Olivier DUMONS et Jean TILOUINE observent qu' *« En Afrique de l'Ouest, les réseaux de cybercriminalité se sont considérablement renforcés et structurés ces dernières années. Ce ne sont plus seulement des amateurs utilisant des techniques basiques depuis des cybercafés mal équipés pour échapper à la pauvreté. Désormais, des experts bien formés lancent des offensives pour piller des individus ainsi que des entreprises de la*

[21] La cyberescroquerie sous toutes ses formes représenteraient 90% des cas de cybercriminalité en Afrique. BARMA (A.), « La Cybercriminalité : le nouveau visage de la menace en Afrique », in Péril digital : un point lucratif. Pourquoi ?, *La Tribune Afrique*, Janvier Février 2019, Interpol, Trend Micro, "Cybercrime in West Africa: Poised for an Underground Market"

région et d'ailleurs »[22]. Ce constat fait suite à une étude publiée par Interpol et le fournisseur de solutions japonais Trend micro sur la cybercriminalité en Afrique de l'Ouest intitulé « La cybercriminalité en Afrique de l'Ouest : naissance d'un marché souterrain ». D'après cette étude, « *le nombre de cyberescroqueries signalées a augmenté de 132 % entre 2013 et 2015, le montant moyen des sommes ainsi dérobées chaque année aux entreprises et aux particuliers s'élevant respectivement à 2,7 millions d'USD et à 422 000 USD… les cybercriminels se livrent à des attaques plus élaborées, comme les escroqueries au président et les escroqueries aux impôts, et ils utilisent souvent des logiciels enregistreurs de frappe, des chevaux de Troie contenant un outil de prise de contrôle à distance (RAT) et d'autres logiciels facilitant la commission d'infractions.* »[23].

Il est donc clair qu'en Afrique de l'Ouest et dans l'espace OHADA *lato sensu*, le cyberrisque est permanent et accentué en période de crise. Il est, en outre, potentiellement systémique comme partout ailleurs. C'est l'avis de la Banque de France dans son rapport 2019 sur l'évaluation des risques du système financier français[24]. Selon Camille BAUDOUIN, *« le cyberrisque est considéré comme un risque systémique pour les banques, i.e. que l'ensemble du système financier pourrait être affecté par une attaque cyber de grande ampleur »*[25]. Une cyberattaque pourrait porter atteinte à l'ensemble de réseau bancaire de l'espace OHADA et peut leur coûter très cher.

De ce fait, les banques de l'espace OHADA ne peuvent pas attendre, par les temps qui courent, d'être surprises avant de réagir pour plusieurs raisons :

Tout d'abord, les cyberattaques sont de nature transfrontière et les entreprises victimes ne peuvent pas, en principe, riposter de leur propre chef à une cyberattaque. Ce qui pourrait être appelé une légitime défense privée n'existe pas en droit international. Au surplus, l'hypothétique utilisation de la cyberforce à titre défensif par une personne privée victime de cyberattaque (le hack-back) est une aventure hasardeuse et risquée techniquement et juridiquement pour les personnes privées[26].

---

[22] DUMONS (O.), TILOUINE (J.), « Les nouvelles « cyberarnaques » africaines », *Le Monde Afrique*, publié le 09/03/2020, consulté le 02/05/2020 [https://www.lemonde.fr/afrique/article/2017/03/09/les-nouvelles-cyber-arnaques-africaines_5092106_3212.html]

[23] Interpol, Trend Micro, "Cybercrime in West Africa: Poised for an Underground Market", *op. cit.*

[24] Banque de France, Evaluation des risques sur le système financier, Juin 2019

[25] BAUDOUIN (C.), « Entre opportunité et risque : le défi de l'IA, au cœur de la révolution numérique et technologique du secteur financier », *Lamyline*, Droit et Patrimoine, N° 298, 1er janvier 2020

[26] Sur ces questions, voir *RDAA*, Regard Mai 2020 – « Les enjeux cyber du COVID 19 », KOUMAKO Yao Justin, [http://www.institut-idef.org]

Ensuite, l'attribution d'une cyberattaque n'est pas un exercice aisé pour les Etats, encore moins pour les entreprises.

Par ailleurs, les consommateurs ont besoin d'être assurés, de savoir que dans la tempête leurs institutions financières sont fortes et stables.

Enfin, vu les dégâts qu'une cyberattaque est susceptible de causer aux banques[27], il est préférable que les banques de l'espace OHADA penchent pour une approche préventive. D'ailleurs, plusieurs banques africaines auraient déjà été victimes de plusieurs cyberattaques avec des dégâts importants. Déjà en 2018, l'établissement NSIA Banque Côte d'Ivoire avait reconnu d'importants dégâts à la suite d'un détournement de fonds par piratage informatique. Elle aurait perdu près de 1,2 milliard FCFA. En mars 2019, c'est la filiale sénégalaise d'Ecobank qui a déclaré s'être fait soutirer frauduleusement 323 millions FCFA, selon un procédé analogue[28]. Au surplus, une étude menée par Dataprotect sur 148 banques africaines montre que plus de 85 % de ces institutions financières déclarent avoir déjà été victimes d'une ou plusieurs cyberattaques ayant entraîné des dommages, parfois à répétition et seuls 6% de ces attaques ont été détectées par les employés de cybersécurité.

Pour toutes ces raisons, les banques de l'espace OHADA se doivent d'adopter une approche préventive. Prévenir vaut mieux que guérir dit-on. Alors que faut-il faire ?

B. Un tantinet de mesures phares contre les cyberattaques liées au COVID-19

Toutes les autorités monétaires de l'espace OHADA s'accordent sur un fait en cette période de pandémie : la nécessité du recours à la banque en ligne. C'est le cas au sein de l'UEMOA où, la Banque Centrale des Etats de l'Afrique de l'Ouest a pris des mesures incitatives pour encourager ses banques et leurs clients à adopter massivement la banque en ligne[29]. La même réaction est observée

[27] L'enjeu d'une cyberattaque dans une entreprise n'est pas négligeable. Il s'agit d'une atteinte sévère aux actifs tangibles de l'entreprise que sont le capital intellectuel, la réputation, l'image, les brevets, les marques, les données, etc. (AJILI BEN YOUSSEF (W.), *op. cit.*). C'est ce qui explique d'ailleurs que les entreprises communiquent peu sur les cyberattaques dont elles sont victimes.

[28] KIE Frank, « Pourquoi les banques devraient s'inquiéter de la cybercriminalité », *Financial Afrik*, publié le 17 Mars 2020, consulté le 02 Mai 2020, [https://www.financialafrik.com/2020/03/17/la-tribune-de-franck-kie-pourquoi-les-banques-devraient-sinquieter-de-la-cybercriminalite/]

[29] Pour voir les mesures incitatives prises par la BCEAO, lire BCEAO, « Communiqué relatif aux mesures de promotion des paiements électroniques dans le contexte de la lutte contre la propagation du Covid-19 », 1ER Avril 2020

dans les pays ayant une autorité monétaire nationale. En RDC par exemple, la Banque centrale du Congo (BCC) a déclaré dans un communiqué du 24 Mars 2020 : *« S'agissant de la circulation fiduciaire, la BCC invite l'ensemble de la population congolaise à utiliser les moyens de paiement électronique (M-Pesa, Airtel Money,Orange Money,etc.) afin de réduire le risque de contamination due à la manipulation des espèces »*[30]. A priori le recours à la banque en ligne prêché par ces autorités monétaires est louable. Cependant, elles commettent un péché : l'absence de mesures incitant à la sécurité numérique. Recourir massivement à la banque en ligne sans mesures de sécurité numérique est synonyme de courir à la perte des banques et de leurs clients.

Il urge donc que les banques se prennent elles-mêmes en mains en ce qui concerne la sécurité de leurs systèmes d'informations et la protection des données personnelles de leurs clients. Les mesures à prendre sont certes techniques mais surtout humaines et organisationnelles.

Quelle que soit la robustesse des systèmes d'information d'un organisme, l'humain est le maillon le plus faible de sa chaîne de sécurité. Les banques doivent donc tout d'abord sensibiliser et former leur personnel sur les questions relatives à la sécurité de leur système d'informations, les employés des banques en Afrique de l'Ouest étant régulièrement victimes du *phishing*[31].

Une formation du personnel sur les problématiques liées à la cybercriminalité doit donc être réalisée par les banques pour aviser et rendre vigilants leurs employés. A l'image des banques hongkongaises qui ont fait faire des exercices de simulation à leurs employés, il aurait été opportun pour les banques de l'OHADA de procéder à des exercices-types mais dans l'urgence du confinement, des formations à distance sur des applications de visio-conférence seraient bienvenues. Il s'agit pour les banques de s'assurer une compréhension du positionnement en matière de cyber-risques en s'appuyant sur des évaluations et des simulations[32].

---

[30] Banque centrale du Congo, « Mesures prises par la BCC pour atténuer les impacts négatifs du COVID-19 sur l'économie congolaise », communiqué du 24 Mars 2020

[31] « *Des mails fictifs sont envoyés aux utilisateurs ; ils peuvent comporter des liens permettant d'installer des logiciels malveillants qui sont des outils de prise en main à distance, mais aussi des "key loggers" pour enregistrer les frappes des claviers. Ils ciblent des gestionnaires ou toutes autres personnes hautement habilitées et ayant la possibilité de faire des opérations sur des comptes* DIA (M.), « En Afrique de l'Ouest, les banques rispostent face à la cybermenace », *La Tribune*, consulté le 23/04/2020 [https://afrique.latribune.fr/africa-tech/2019-04-08/afrique-de-l-ouest-les-banques-ripostent-face-a-la-cybermenace-813496.html]

[32] HESLAULT (L.), « La cyber-résilience, une approche nécessaire et pragmatique pour la sécurité informatique », *Club des directeurs de sûretés et sécurité des entreprises*, 12/12/2014

Par ailleurs, vu les multiples services bancaires en ligne que proposent les institutions financières, les clients devraient également être informés. C'est à ce prix que la banque en ligne pourrait être efficiente. Des consignes claires données peuvent être salutaires ; des gestes barrières contre les virus informatiques. Les banques devraient à cet effet adopter les meilleures techniques de communication pour faire passer le message auprès de leurs clients tout en mettant l'accent sur l'augmentation des risques pendant la pandémie. Certaines banques à l'instar de NSIA Côte d'Ivoire ou encore Ecobank ont une approche louable allant jusqu'à mettre au profit des réseaux sociaux ou encore leur newsletter.

Les banques du Groupe intermonétaire de l'UEMOA (GIM-UEMOA) ont établi récemment des protocoles et procédures définies pour sécuriser leurs données. Ces mesures de sécurité doivent être mises à jour et scrupuleusement respectées. En l'absence de règlementation unique au niveau de l'Union, les banques doivent respecter la règlementation en vigueur dans leur pays respectif en matière de sécurité de système d'information. Il doit en être ainsi pour toutes les banques de l'espace OHADA car les banques sont des secteurs stratégiques pour chaque pays. En France, elles sont classées parmi les opérateurs d'importance vitale (OIV)[33] par la loi de programmation militaire 2019-2025 qui exige d'elles une politique de cybersécurité particulièrement exigeante[34].

Techniquement, les outils de sécurité doivent être renforcés et régulièrement mis à jour pour identifier le plus rapidement possible les menaces ou les brèches avant toute intrusion malveillante dans les systèmes. En outre, les banques doivent mettre en place ou développer des procédures et activités leur permettant d'identifier le plus rapidement possible toute sorte de cyberattaques et garantissant une réponse adaptée. Par ailleurs, l'accès extérieur aux systèmes par les travailleurs à distance doit demeurer sécurisé. Travailler à distance et travailler avec sécurité ne sont pas antinomiques[35].

---

[33] Selon le glossaire de l'agence nationale de sécurité des systèmes d'informations, « Un opérateur d'importance vitale : exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ; gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population. »

[34] Loi nº 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense

[35] Sur le plan technique, lire les recommandations de sécurité informatique pour le télétravail en situation de crise édictées par le gouvernement français.[www.cybermalveillance.gouv.fr]

Juridiquement, il est possible pour les banques de souscrire à un contrat de cyberassurance, « un contrat encore méconnu dans les entreprises »[36]. Les contrats de cyberassurance, même si leurs contours restent encore à définir clairement, portent des bénéfices inédits. Outre les bénéfices communs à tous les contrats d'assurance dans une entreprise, ils ont des bénéfices propres allant de l'audit des systèmes d'information à des fins d'obtention d'une « évaluation précise de la qualité des protections mises en place »[37] à la couverture « des frais de gestion de crise (honoraires de consultants), d'expertise informatique dite « forensique », d'avocat, de relations publiques, de notification, de restauration et reconstitution des données »[38].

Enfin, les banques doivent privilégier le partenariat public-privé dans la gestion des cybermenaces. Autrement, elles doivent signaler les tentatives d'intrusion repérées aux autorités nationales de cybersécurité à des fins d'analyse et d'intervention si nécessaire.

[36] SEJEAN (M.), « Le contrat de cyberassurance, un contrat encore méconnu dans les entreprises », *Gazette du Palais*, 05 Mai 2020, [www.lextenso.fr]
[37] Delcamp C. in Guicheteau C., « Une cyberassurance ? Pour quoi faire ? », Daf magazine, n° 40, juin 2019, p. 47, cité par SEJEAN (M.) in « Le contrat de cyberassurance …», *op. cit*
[38] V. Zicry L., Cyber-risques. Le nouvel enjeu du secteur bancaire et financier, Saiz J. (préf.), 2017, RB édition, p. 109-116, cité par SEJEAN (M.) in « Le contrat de cyberassurance …», *op. cit*