UNIVERSITÉ LIBANAISE
Faculté de Droit et de Sciences Politiques et Administratives

Le recours à la banque digitale entre la légalisation et la criminalisation

Mémoire en vue de l'obtention d'un Master 2 en Droit des Affaires

Présenté par:
HAYDAR Mira

Sous la direction de
Docteur GHAYAD Wissam

2022-2023

“L’université libanaise n’entend donner aucune approbation ou improbation aux opinions émises dans ce mémoire; ces opinions doivent être considérées propres à leurs auteurs.”

À mes parents,

À mon mari,

À mes filles,

À tous ceux qui me sont chers, je voudrais faire partager ce succès.

Remerciements

Je tiens à remercier tout particulièrement Docteur Wissam GHAYAD pour avoir accepté de diriger cette memoire, pour son support et ses encouragements tout au long de ce travail.

Mes remerciements vont également à mes collègues à la banque, à leurs conseils et leurs critiques qui ont contribué à alimenter ma réflexion.

Enfin, je souhaite remercier tout ceux qui m'ont aidé à exceller dans cette recherche.

Tableau des Abbréviations

Art: Article

Al: Alinéa

AI: Artificial Intelligence

BDL: Banque Du Liban

Cass: Cour de Cassation

CNIL: Commission nNationale de l'Informatique et des Libertés

CCF: Code Civil Français

CPF: Code Pénal Français

CPL: Code Pénal Libanais

DL: Décret législatif

E-: Electronic

FINMA : Autorité Fédérale de Surveillance des Marchés Financiers

IMF: International Monetary Fund

INTERPOL: International Police

InfoSec: Information Security

IT: Information Technology

JU: Jurisprudence

JO: Journal Officiel

NCSIA : Agence Nationale de la Cyber sécurité et des Systèmes d'Information

RGPD: Règlement Général sur la Protection des Données

TIC: Technologie de l'Information et de la Communication

SIC: Special Investigation Commission

Op. Cit: De Opero Citato (Ouvrage cité)

P.: Page

Vol: Volume

ت.ج.: تمييز جزائي

غ: غرفة

Introduction

"Vers l'an 2022, Le Liban veut créer un cyberespace plus sûr et stable, tant sur le territoire national que dans les échanges internationaux.[1]"

La création d'une Banque Centrale au Liban et l'organisation du secteur bancaire Libanais se foisonnent à l'horizon par la force des choses.
Le code de la monnaie et du crédit contenant 230 articles est apparu grâce au décret-loi n° 13513 daté 1er Août 1963.
L'article 121 du code de la monnaie et du crédit définit la banque comme suit: «l'entreprise dont l'objet essentiel est d'employer, pour son propre compte, en opérations de crédit, les fonds qu'elle reçoit du public ».[2]

Selon L'article L 311-3 code monétaire financier les moyens de paiement sont « tous les instruments qui permettent à toute personne de transférer les fonds quel que soit, le support, le procédé technique utilisé ». Il en résulte que les moyens de paiement sont des engins ayant pour objectif principal le transfert de fonds peu importe les moyens utilisés pour atteindre ce but.[3]

On déduit que le secteur bancaire représente le système nerveux de tout pays vu que les banques possèdent un impact direct et essentiel sur son développement, à travers leur participation significative au financement de l'économie nationale, la gestion des moyens de paiement et à la création d'emploi.

[1] Président du conseil des ministers, stratégie nationale libanaise de cybersécurité, 2019
[2] Nammour Fadi, Le droit bancaire, Université Libanaise, Faculté de Droit et des Sciences politique et administrative 2015, P.6
[3] Nammour Fadi, Le droit bancaire, Référence précedente, P. 11

Si le milieu du XVIIIe siècle a donné naissance à la révolution industrielle, la fin de ce siècle a guidé la révolution des moyens de télécommunications, et l'humanité a été témoin de l'explosion de cette révolution qui a dominé tous les aspects de notre vie quotidienne.[4]

L'effet toujours croissant de l'internet, des smartphones et des réseaux sociaux a participé à la modernisation de notre quotidien dans tous ses aspects surtout l'aspect économique imposant de nouvelles méthodes et modèles.

En effet, L'internet permet un accès très rapide a un nombre très élevé d'information disponible en permanence.[5]

L'intégration de ces innovations technologiques a bouleversé complètement ce secteur ouvrant ainsi la fenêtre à une nouvelle ère commerciale qui s'appuie essentiellement sur les technologies d'information et de communication (TIC).
Parmi ces techniques, l'internet qui a joué un rôle primordial dans l'activité bancaire à un tel point qu'il a pu modifier la nature des services offertes par la banque.

L'internet a vu le jour durant les années 1960, lorsqu'un système de communication permettant l'échange des informations via des ordinateurs est né à des fins militaires.[6]

L'internet, désigne parfois par « toile d'araignée » est l'acronyme de l'expression anglaise « International Network ». En d'autres termes, réseau international. Elle signifie l'ensemble des ordinateurs et réseaux qui communiquent à l'aide des télécommunications utilisant le même Protocol.[7]

L'internet est donc simplement le réseau des réseaux et constitue une association ouverte de multiples réseaux et ordinateurs qui se communiquent pour partager l'information.[8]

---

[4] Dixon, Mary et Nixon, Brian. 2000. e-banking: Managing your money and transactions online. SAMS publishing, P. 140.
[5] Nicholas Carr Is google making us stupid, what the internet is doing to our brain, July 2008. Disponible sur www.theatlantic.com Date de la visite 30 Novembre 2023
[6] E. Nassif, les contrats internationaux, le contrat électronique en droit libanais, Beirut, El Halabi, 1ere édition, 2009, P. 24 et suivant
[7] F. Gusdorf et Ch. Lassure op.cit. P.226
[8] F. Colein, Manuel de l'int. Paris, Lavoissier 2001, P. 14 et suivant

Aujourd'hui, un simple contact électronique est suffisant pour joindre des milliers de systèmes électroniques.
Toutes les opérations se déroulent donc dans un cyberspace contenant à l'instar des réseaux d'ordinateurs, les utilisateurs de cet infrastructure matérielle de communication.

Pressées par la mondialisation, ce développement des moyens de télécommunications a cédé le passage à la transformation remarquable de la banque traditionnelle a la banque digitale qui est aujourd'hui en plein essor.

Connus sous des appellations diverses ; "banque électronique" (e-Banking), banque numérique, cyber banque, "Banque en ligne" (online Banking), banque digitale... Ces banques sont apparues durant les années 70, lorsqu'on a pu lier multiples ordinateurs par plusieurs réseaux et concernent donc l'intégration des TIC dans leur opération bancaire.

On entend par ces termes la possibilité de mener des transactions bancaires en ligne à travers l'internet, en utilisant un dispositif connecté. [9] (Paiement de fracture en ligne, transfert d'argent automatique, consultation du solde du compte et vérification des relevés périodiques à travers le mobile). Cela permettra aux clients d'avoir un accès direct à leurs comptes tout le temps, recevoir et payer les fractures en ligne, transférer ses fonds d'un compte à un autre et beaucoup d'autre service innombrable.

Ce tsunami digital était le résultat d'une mutation des opérations classiques aux opérations modernes. Cependant, cette évolution rapide à entrainer des modifications brusques à l'échelle nationale et internationale.

Un rapprochement entre les principes classiques et les mutations qui sont engendrés par le numérique est à l'origine d'une formule adéquate se situant entre les principes et les mutations.

Ceci étant, les banques ont vécu une explosion des services bancaires électroniques et l'apparition de nouveaux acteurs sur le marché financier.[10] L'agence bancaire n'est plus le

[9] Diniz Eduardo, web banking in USA 1997, P. 5
[10] Seybold, P.B. et Marshak, R.T. Customers.com: How to create a profitable business strategy for the internet and beyond, 1998, P. 52

seul moyen pour contacter le client, un ensemble d'outil est mis à la disposition des clients qui se trouvent face à un portefeuille de projets innovant très large basé sur la virtualité comme l'ATM et les applications du mobile.

Pour être plus précis, les services bancaire électroniques désignent le travail accompli par la banque au moyen des technologies internet et d'une variété des alternatives innovantes. Ce qui permet d'offrir aux clients des produits distingues facilitant ainsi la gestion de leurs comptes.[11] Cela est certes un indicateur pour augmenter l'investissement dans ces technologies.

La banque digitale est encore plus globale. Elle comprend toute les formes d'operations bancaires financières conduites à l'aide de la technologie, même en l'absence d'un emplacement physique.[12] On constate donc que la banque électronique ou la banque en ligne est une forme de la banque digitale.

Ainsi, la banque digitale consiste à utiliser un large éventail de techniques dans le but de fournir des services en ligne à la clientèle tout en réduisant l'intervention humaine. La seule interaction possible demeure avec la machine.

Dans ce cadre l'émergence du digital a rendu la transformation de l'information moins onéreuse et plus facile et ouvre largement la porte au développement de nouveaux produits et services financiers.[13]

En réponse à ces changements, les banques se sont trouvées obliges de répondre aux nouvelles exigences résultant de ces innovations technologiques.
Ainsi, le Liban s'est engagé dans une sévère voie de digitalisation irrévocable dans laquelle les banques étaient le secteur le plus stratégique.

---

[11] Cronin, M.J., Banking and Finance on Internet., New York, 1998, P. 27
[12] I-Vest, Banque en ligne et banque digitale, quelle est la différence? https://www.i-vest.ch/fr/trends/banque-digitale/banque-en-ligne-et-banque-digitale-quelle-est-la-difference
[13] Berdi Abdelaziz, La relation entre la banque traditionnelle et l'e-Banking: une tentative d'analyse à partir du cas marocain, Revue de contrôle de la comptabilité et de l'audit, Numéro 7, décembre 2018 P.13

Les banques se sont désormais prises dans un tourbillon constant difficile à contrôler grâce à l'évolution du digital qui s'est imposé sur tous les secteurs notamment le secteur bancaire.

Cette révolution a engendré plusieurs problématiques qui puisent leur source du bouleversement du droit tout entier en raison de l'accroissement inattendu de l'internet.
Ces questions font face à des obstacles d'ordre juridiques et pratiques notant qu'il n'est pas aussi aisé d'y répondre…

Dans la même perspective, de multiples projets de modernisation comme le travail et l'apprentissage en ligne, ont été le résultat d'une adoption très croissante de la technologie de l'information surtout que le monde entier est de plus en plus connecté à l'internet. Dans ce cadre, la banque digitale a gagné du terrain au niveau du secteur bancaire libanais et a bouleversé le travail au sein des banques.

En effet, cette digitalisation a besoin d'une base solide pour prospérer et produire des revenus et des avantages pour l'économie et la société.[14] Elle a également besoin d'un encadrement juridique et judiciaire capable de résister aux changements et pressions qu'endure le Liban.

En transférant leurs services bancaires de la face à face technique à une technique plus adaptée aux besoins et attentes des clients, les banques visent en particulier à améliorer leur productivité tout en prenant en compte le bien être de leur client. Mais cette métamorphose n'est évidemment pas sans risques ni menaces.

Eu égard que multiples services sont digitalisés au sein de la banque et les opérations sont réalisées à travers l'internet, on s'interroge sur l'importance de la protection des données clientèle surtout que les clients de la banque confient des informations confidentielles a cette dernière.

A l'ère du digital, ces informations sont exposées à de multiples risques comme le détournement de l'argent suite au vol des informations sensibles de la carte bancaire.

[14] Sofia Karim, Electronic transactions in Lebanon: legal challenges and opprortunities, Master en business law, Lebanese American University, February 2019.

Dans ce sens, un projet de loi a été approuvé par le gouvernement du président Najib Mikati en 2012 et renvoyé au Parlement Libanais. Le projet s'étendait à pratiquement toutes les matières couvertes par les directives européennes et par quelques autres conventions internationales.

Les majeures domaines d'application étaient la signature électronique, les contrats en ligne, la protection des consommateurs dans le commerce électronique, la sécurité des paiements et des opérations bancaires ; les droits de propriété intellectuelle; la protection de la vie privée et des données personnelles et les infractions liées aux réseaux et au commerce électronique.

Les discussions parlementaires entre les comités spécialisés ont prolongé la date de son transfert à l'organisme public jusqu'à son adoption lors de la législature du 24 septembre 2018.

Ce n'est donc que 13 ans plus tard après le premier projet de loi que la loi 81/2018 sur les transactions électroniques et la protection des données personnelles a été adoptée dans sa version finale dû essentiellement à la conférence CEDRE et les réformes engagées par l'Etat Libanais pour encourager les pays donateurs à apporter le soutien financier.

Par la suite, l'adoption de la banque digitale était à la base de la création d'un cadre juridique d'autorégulation qui comble les vides laissés par la révolution du numérique.

Suite à cette digitalisation, le développement du numérique a fait apparaitre des dangers non négligeables et de nouveaux méthodes de crimes à caractère international.
La banque digitale est devenue un outil stratégique au service de la cybercriminalité!

L'invention du terme « cybercriminalité » revient aux années 1960, au moment où l'internet a envahi l'Amérique du Nord et de nouveaux types de criminalité se sont répandus.

Ainsi, le premier cas d'infraction pénale est le détournement d'usage réalisé par John Draper en 1969, connu également sous l'appellation Captain Crunch. Ce dernier réussi, en utilisant un sifflet ayant la même tonalité que le réseau téléphonique américain, à transmettre des appels longues distance gratuite lorsqu'il sifflait. Captain Crunch a été

condamné pour ces actes en 1976. Après cet évènement, les actes cybercriminels ont largement évolué durant les années 80, dans le monde informatique.[15]

Définir ce que constitue un cyber crime n'est pas toujours facile surtout avec la digitalisation croissante des banques et la jeunesse des lois sur la cybercriminalité. Ce concept de cybercriminalité qui a émergé rapidement, possède évidement un caractère pénal qui diffère selon les systèmes juridiques mondial.[16] Dans l'usage courant, ce vocable "sert à désigner toutes les formes d'attaques réalisées au moyen de réseaux informatiques ou de systèmes d'information, ou les ayant pour cible".[17]

Nous nous intéressons dans notre recherche spécifiquement à la cybercriminalité dans le secteur bancaire qui suscite un très grand souci partout dans le monde comme elle engendre particulièrement, la menace de l'arrêt de l'activité bancaire qui sans doute a des effets atroces sur les opérations bancaires, surtout que dans les dernières années, les banques ont été exploites à des fins très agressives et des différents types de crimes cyber. Ces menaces varient et leur conséquence néfaste s'accroît de plus en plus avec l'évolution et la complexification des techniques d'attaques surtout que les procedures techniques liées à la preuve électronique dans ces types de crimes est régit par des principes très spécifiques.

L'adoption d'une règlementation particulière capable de garantir la cyber sécurité de leur système d'information demeure l'enjeu majeure des banques en l'absence à l'heure actuelle d'une loi régissant les transactions électroniques.

Ce terme récent, définit par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) est utilisé pour référer aux politiques de prévention, de détection et de correction mises en place pour lutter contre les cyberattaques.

---

[15] Le Net Expert, Comment est née la cybercriminalité, 31 Aout 2022, https://www.lenetexpert.fr/comment-est-nee-la-cybercriminalite-2/ date de la visite 13 Mars 2023.

[16] Christoph Chloé, la cybercriminalité bancaire, mémoire de master 2 chargée de clientele professionnelle, université de Strasbourg, faculté des sciences économiques et gestion 2020- 2021

[17] Bollo Édouard Fernandez-, institution financière et cybercriminalité, revue d'économie financière, 2015/4, (n.120) P. 181 a 198

L'objectif principal de la cyber sécurité dans la banque digitale surtout est de protéger les actifs du client. Comme de nos jours les activités et les transactions se font en ligne, les clients utilisent de plus en plus les cartes de crédit et de débit pour des transactions qui doivent surtout être protégées par la cyber sécurité.

En fait, les cyber crimes dans les services digitaux affectent non seulement le client, mais également les banques lorsqu'elles tentent de récupérer les données. Ainsi, ces derniers peuvent être obliger de dépenser une somme d'argent considérable pour récupérer des données ou des informations sensibles violées.[18] Donc, les données d'un client peuvent être facilement piratées si elles ne sont pas protégées par la cyber sécurité. Cela peut entraîner des pertes financières substantielles et un stress mental dans le cas où la cybercriminalité se produit.

N'oublions pas que la crise sanitaire du COVID 19 a impacté largement le milieu bancaire en créant des nouvelles méthodologies qui se sont, à travers le temps incarnées, dans la gestion quotidienne de diverses opérations bancaires a l'exemple du télétravail.

Selon Shawki Ahwash,[19] le Liban a connu une croissance, sans précèdent, de la cybercriminalité bancaire vu que les banques tentent à fournir de plus en plus des services bancaires sur le mobile et en ligne.

Les criminels ont désormais bénéficier de ces nouvelles méthodes afin de commettre leur crime surtout avec l'absence, dans la plupart des cas, des systèmes de sécurité du télétravail.

Il est concevable qu'une croissance économique efficace n'est stimulée et une bonne gouvernance n'est favorisée que si uniquement les systèmes informatiques sont bien protégés et sécurisés[20]puisqu'aujourd'hui, les processus utilisés par les criminels sont principalement de nature informatiques.

---

[18] Saleh M. Nsouli et Andrea Scheaechter, les enjeux de la banque électronique, Septembre 2022, Finance & développement P. 48-51

[19] Halilou Yerima, Directeur de l'unité Banque commerciale d'Arique du nord du CBA/FT, discours prononcé le 5 Décembre 2016

[20] Bruno Teboul, Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive, 14 Avril 2022

A l'instar d'autres pays, le Liban considère l'internet comme l'un des élément clés de son développement économique et ses opportunités futurs.

Loin des procédés traditionnels que l'internet a fait apparaître, les cybercriminels passent par des processus très complexes pour accéder aux ressources des clients qui parfois dépasse l'expertise des professionnels dans de tels sujets.

La lutte contre la cybercriminalité est considérée aujourd'hui un investissement économique, L'élément significatif, le plus primordial indiquant qu'une banque est prête pour faire face à la cybercriminalité est la constitution d'une stratégie de lutte contre la cybercriminalité, en installant un dispositif de cyber protection bancaire[21] mettant en œuvre sa vision économique, ses capabilités techniques, ainsi que ses priorités informatiques en matière de cyber sécurité.

Le choix de notre sujet est justifié par plusieurs raisons. D'abord le secteur bancaire est considéré comme un élément fondamental du changement à venir avec tout le bouleversement de la technologie durant les dernières années.

En outre, les banques digitales disposent de nombreux atouts qui sont exploités par les criminels et les études portant sur la problématique de la banque digitale au Liban ainsi que les risques engendrés par celle-ci surtout le risque de la cybercriminalité sont encore peu nombreuses.

Notre étude traite un sujet très récent, et les questions juridiques qu'il soulèvent prennent une importance accentuée jour après jour.

Ce sujet constitue un grand défi spécifiquement pour les spécialistes du droit pénal dans leur recherche pour trouver des réponses et des solutions appropriées à de tels problématiques, à la lumière des textes existants, traditionnels ou modernes, et en termes de modification des textes existants ou introduction de nouveaux textes avec l'évolution technique actuelle très rapide.

Aussi, on remarque une croissance des législations dans ce sujet du simple fait qu'il est attaché au monde cyber. Cela empêche de localiser ce travail dans un laps de temps précis.

[21] Reich C. Pauline, Cybercrime and security, Vol. 1, Thomson Reuters, 2012

Ainsi, certaines interprétations et analyses pourraient être contestés au fil du temps face à l'augmentation des règlements juridiques dans ce cadre.

En effet, dû à la nouveauté de ce sujet, il a rarement été discuté auparavant, malgré la disponibilité d'un certain nombre de recherches et des articles qui le traitaient au niveau international. Cependant, au Liban, les recherches conduites dans ce sujet ne traitaient pas tous ses aspects et les législations sont dans la plupart des cas inopérantes.

De plus, s'adapter à ce nouvel univers était un défi primordial vu la pluralité des systèmes et usages informatiques. D'où s'avère la nécessite de proposer des solutions indispensables pour bien appréhender ce sujet.

En crise, depuis 4 ans, les banques libanaises tentent de diminuer les risques auxquels ils se heurtent surtout que la plupart des banques libanaises suivent la technologie moderne. Ces banques se trouvent ainsi face à multiples bravades dont la gestion et les solutions sont épineuses surtout avec l'absence des ressources nécessaires et d'un propre financement.

L'importance de cette étude se cristallise ici, car elle touche des points liés à des sujets controversés qui sont abordés de diverses manières et d'une façon très approfondie dans le cadre d'une approche juridique qui se veut la plus précise possible. Il est donc important de conduire une analyse approfondie de l'efficacité de la digitalisation des banques dans un environnement numérique.

Avec le développement technologique rapide dans le secteur bancaire et la croissance des banques digitales libanaises, la cybercriminalité a occupé la première place parmi les crimes graves en termes de danger et de méthodes avancées utilisées par les criminels. Par conséquent, il était primordial de trouver un cadre juridique efficace pour lutter contre ce type de crime a propagation rapide.

Dans cette perspective, l'étude suivra (2) axes mettant en avant l'utilisation légitime de la banque digitale traduite par son statut opérationnel et son encadrement juridique et

s’interrogeant ensuite sur les effets de l’utilisation abusive de ces banques pour des fins criminelles.
D’où la nécessite de promouvoir les lois et circulaires en vigueur afin d’accompagner les innovations inédit et brutal dans le domaine technologique et numérique.

Ce double trenchant soulève une question essentielle qui représente la problématique de cette étude: Quelles sont les implications pénales du dépassement abusif du cadre législatif auquel est soumise l'utilisation légitime de la banque digitale?
Face à ces mutations d’ordre digitales, plusieurs interrogations subsidiaires en découlent:

Quel est le cadre législatif régissant les banques digitales au Liban?
Quel est la nature juridique des services offertes par la banque digitale?
Comment la digitalisation des opérations bancaires à céder le passage aux crimes dans le monde cyber?
Quels principes procéduraux sont suivis dans la poursuite de ces crimes? Existe-t-il de nouvelles procédures spéciales à cet égard et comment obtenir les preuves qui en découlent?
Quelles sont les obligations de la banque afin de garantir un cadre sécurisé de la banque digitale?
Quel impact a la cybercriminalité sur l’utilisation légitime de la banque digitale?

L'étude répond à la problématique posée et aux questions implicitement liées, à la lumière des textes juridiques en vigueur au Liban.

Afin de bien mener cette étude et dans le but de l’amélioration du droit Libanais, on exposera les droits Français et Européens pour établir un encadrement international et mieux approfondir le droit national.

Notre analyse sera enrichie par une étude contemporaine à l’aune de de ce nouvel espace complexe. On se réfèrera à un ensemble très diversifié de conventions et chartes internationales, ainsi qu’aux législations nationales et internationales, de même qu’à la jurisprudence et la doctrine. Les études, articles et sites web, souvent purement juridiques, occuperont une place aussi importante.

De ce point de vue, il a fallu combiner différentes méthodes pour nous guider à des conclusions claires. On assistera alors à l'approche théorique, où nous définirons tous les mots clé relatifs à la banque digitale et à la cybercriminalité dans le monde numérique. Ensuite, l'approche descriptive orientée en fonction du problème, à travers laquelle nous présenterons les dispositions légales applicables à ce sujet.
L'approche analytique sera la plus utilisée, pour critiquer les textes législatifs présentés, et exprimer notre point de vue à cet égard. Enfin, on adoptera l'approche comparative qui consiste à juxtaposer différentes situations d'une manière comparative tout en suggérant les nécessaires modifications.

Après avoir exposé notre vision qui s'étale à toutes les dimensions de l'étude ainsi que la méthodologie scientifique suivie dans la rédaction de cette recherche et dans le but de répondre à la problématique posée, on divisera le sujet de cette mémoire: « Le recours à la banque digitale entre la légalisation et la criminalisation » en (2) parties:

Partie 1: La banque digitale: un outil légal au service des banques

Titre 1 – L'adoption des banques digitales par le secteur bancaire

Chapitre 1: La règlementation de l'activité des banques digitales

Chapitre 2: L'encadrement juridique de la banque digitale au Liban

Titre 2 – Les droits liés à l'utilisation des services de la banque digitale

Chapitre 1: Les droits lié aux principes de protection de la clientèle

Chapitre 2: Les droit liés à la protection des données personnelles

Partie 2: La banque digitale: un outil stratégique au service de la cybercriminalité

Titre 1 – L'utilisation abusive des opérations digitales bancaires

Chapitre 1: La règlementation de la cybercriminalité bancaire

Chapitre 2: La spécificité des crimes commis dans le monde cyber en matière pénal

Titre 2 – L'installation d'un dispositif de cyber protection bancaire

Chapitre 1: Le processus de lutte contre la cybercriminalité bancaire

Chapitre 2: La cyberdéfense: Une mise en œuvre de la stratégie de lutte contre la cybercriminalité bancaire

Partie 1 : La banque digitale : Un outil Légal au service des banques

Depuis les années 2000, le monde a vécu un énorme bouleversement lié au numérique. Cette transformation vers le digital a engendré des changements graves qui ont touché de façon directe le paysage économique et notamment le secteur bancaire.

Aujourd'hui, les banques se trouvent obliger de s'adapter à ce changement selon leurs tailles et leurs infrastructures et le digital constitue désormais une partie intégrante du secteur bancaire mondial.[22]

L'intégration de ces technologies digitales a permis la création de nouvelles dimensions dans les banques et à aider à la modernisation de ce secteur bancaire grâce aux nouvelles stratégies digitales offertes portant une valeur ajoutée pour les clients.

Ces stratégies ont bouleversé l'écosystème bancaire qui était monopoliser pendant des décennies par les banques traditionnelles, régissant multiples services bancaires offerts à la clientèle.

Par ailleurs, l'utilisation de ces service digitales incombe des droits spécifiques sur la banque. Ces derniers doivent être respectés et connu par la clientèle.

Sur la base de ce qui précède, il convient d'examiner l'adoption des banques digitales dans le secteur bancaire **(Titre 1)** et les droits liés à l'utilisation de ces services **(Titre 2).**

Titre 1 : L'adoption des banques digitales par le secteur bancaire

L'avènement de l'internet a fait émerger un changement dans les technologies de l'information et de la communication (TIC).

[22] Ben Boubaker Safa, L'évolution du modèle bancaire a l'ère du digital, Décembre 2020 P8-25

Le secteur bancaire n'a pas échappé au progrès informatique. Pendant la dernière décennie, l'amplification des nouvelles technologies et services bancaires sur Internet, ont donné naissance à un nouveau véhicule d'information, l'e-Banking ou banque digitale.

La banque électronique est un terme qui implique l'utilisation des ordinateurs, donc une livraison automatique par voie électronique. C'est un canal de distribution et de livraison des services financiers non plus sur support papier mais par voie de communication multimédia, d'une façon globale et moins coûteuse. [23]

Cette technologie surprenante s'est vite popularisée dû à la facilite de l'utilisation de cette technologie par toute personne. Cette utilisation était affectée par les services informatiques dont jouit l'utilisateur.

Cette évolution a connu un très grand essor et constitue un nouvel élan dans notre société. L'introduction de la banque digitale dans l'industrie bancaire a beaucoup simplifié les procédures bancaires grâce à sa contribution à l'instauration et à l'automatisation des services financiers et à l'augmentation du volume des transactions en ligne.[24]

Cela nous amène à étudier la règlementation de l'activité des banques digitales **(Chapitre 1)**, pour passer ensuite à l'encadrement juridique de la banque digitale au Liban **(Chapitre 2)**

Chapitre 1 : La réglementation de l'activité des banques digitales

L'introduction des nouvelles technologies alliant l'informatique et la communication dans les services bancaires a permis d'une part aux banques de mieux développer leurs affaires et, d'autre part, à leurs clients de gérer leurs comptes à distance, d'effectuer des paiements,

[23] Stamoulis, D.S. How banks fit in an Internet Commerce Business Activities Model, 1994

[24] Chencheh Ossama, Les déterminants de l'adoption de e-Banking par les institutions financières et la clientèle organisationnelle, et son impact sur l'approche relationnelle: cas de l'internet Banking en Tunisie, mémoire de maitrise, université de Quebec, Montreal, Juillet 2011.

de transférer des fonds et de faire des transactions directement ou via Internet.[25] Ainsi le client n'est plus face à des modèles d'affaires traditionnels, il est par contre en présence de plateformes dynamiques et transactionnels avec lesquelles il peut procéder à plusieurs opérations bancaires. Ce fait a révolutionné la pratique bancaire et a joué un rôle très important dans le domaine bancaire.

La valeur ajoutée qu'offre la banque digitale se traduit par la qualité du service, soit la rapidité, l'accessibilité, le caractère confidentiel, social et personnel de cette technologie. C'est un moyen moins coûteux et en même temps très efficace qui répond parfaitement aux nouveaux enjeux de la banque contemporaine.

Ce chapitre sera consacré à l'étude de la mutation du modèle bancaire à l'ère du digital **(section 1)** et à l'apport de la banque digitale aux activités bancaires **(section 2).**

Section 1 : La mutation du modèle bancaire à l'ère du digital

Il est incontournable que la banque digitale rend la vie énormément facile au client de la banque, répond à ses attentes et améliore ainsi la relation commerciale avec ce dernier, puisque le client n'a plus besoin de se déplacer pour effectuer ses opérations commerciales quotidiennes, étant donné que l'opération est déclenchée par le donneur d'ordres sur un site web exploité par la banque.

La banque digitale implique ainsi que les opérations bancaires électroniques contiennent les systèmes permettant au client, qu'il soit un individu ou une entreprise d'accéder à leurs comptes et de traiter leurs affaires par un simple clic.

Cette relation entre le client et la banque est de nature personnalisée et est surtout basée sur la confiance mutuelle et l'échange fructueux[26].

[25] Cronin, J.Mary. Banking and Finance on internet, Wiley, NEW York, 2007
[26] Saadi Makrem, Implantation de l'approche relationnelle dans le domaine des services: cas du secteur bancaire, Mémoire de maitrise, université de Québec, Montréal, 2009

Le fait que le client sera servi par sa banque à n'importe quel moment ne fait que renforcer et développer la relation qui les unit et nous amène à déduire une refonte réelle.

Il est nécessaire de déterminer dans cette section l'émergence de nouvelles technologies dans le secteur bancaire **(P.1)** et l'influence des innovations technologiques sur la transformation des banques **(P.2).**

P.1 : L'émergence de nouvelles technologies dans le secteur bancaire

Les nouvelles technologies sont la voie de l'avenir. Elles présentent de multiples avantages surtout pour la clientèle bancaire grâce aux énormes opérations simplifiées, rapide et facile et même parfois moins chères qu'offre la banque digitale.

En effet, les facteurs responsables de cette transformation digitale dans le secteur bancaire sont divers et variés et la technologie numérique contemporaine a joué un rôle indispensable dans cette transformation.

Nous examinerions ainsi les facteurs titulaires de l'intégration des banques digitales (A) et l'évolution qu'a subie la banque traditionnelle à la banque digitale (B).

A- Les facteurs titulaires de l'intégration des banques digitales

Durant les dernières années, il y avait un grand besoin pour utiliser les nouvelles technologies de l'information dans la scène mondiale. Cette maladie contagieuse de l'internet à largement touché les banques qui ont amorcé leur virage vers les canaux électroniques de distribution et de communication pour préserver leur fonds de commerce et ont par conséquence subit des mutations importantes. A ce niveau, l'internet était perçu comme vecteur d'innovation économique et sociale.[27]

Il est important de mentionner que les nouvelles technologies englobent toutes les technologies récentes permettant au client de la banque d'opérer à distance et même d'une façon quasi instantanée.

[27] Vieira et Nathalie Pinède. (2005), « enjeux et usages des TIC : aspects sociaux et culturels T1, Presses universitaires de Bordeaux, Bordeaux, p 7-20, p.12.

Ainsi, les nouvelles technologies digitales ont complètement bouleversé le travail rituel au sein des banques comme d'énormes changements structurels ont été introduites.

En effet, intégrer les innovations technologiques et les pratiques digitales dans le travail quotidien de la banque n'est pas né par hasard. Au contraire, l'engagement des banques dans cette voie considérée comme extraordinaire a été le résultat d'énorme travail. A ce titre, la technologie internet établie sur les ordinateurs et le téléphone portable a accéléré le recours aux opérations bancaires à distance et a ouvert largement la porte à la banque digitale.[28]

Comme nous l'avons mentionné un peu plus haut, l'innovation est le facteur primordial dans l'adoption des technologies moderne.

Selon Reger et Schumacher, l'individu développe un besoin d'adoption des innovations au moment où il connait qu'il existe un meilleur produit disponible sur le marché. Cette connaissance fait naitre en lui un comportement « innovatif » et par suite l'encourage a essayé cette nouveauté.[29]

Aussi, Mansfield affirme que l'entreprise adopte de nouvelles technologies en se basant sur des expériences antérieures. Ainsi, Plus les essaies antérieures dans le domaine d'innovation sont des réussites, plus l'entreprise se forge dans l'innovation, ce qui lui facilitera par la suite l'adoption à cette innovation.[30]

Plusieurs variables et facteurs ont influencé l'adoption des innovations de la technologie au niveau de la banque. On nomme de ces variables, les variables individuelles qui reviennent à la personne voulant adopter des innovations particulières comme par exemple l'âge, le revenu, le niveau de scolarité. Les variables organisationnelles relative aux caractéristiques de l'organisation comme sa taille, son personnel, son chiffre d'affaire et enfin les variables structurelles liées aux caractéristiques de l'innovation et du marché. De

[28] Les nouvelles technologies de la banque à distance: quelles conséquences pour les établissements financiers et leur autorité de contrôle, étude du rapport annuelle de la commission bancaire, 1999
[29] Roger Et Shoemaker, F.F. communication et innovations, New York, Free press, 1971
[30] Mansfiled Edwin, Technical change the rate of imitation, Econometrical, October 1961, P 741 - 766

ces caractéristiques existe le type de service offert par l'organisation, le produit présenté à la clientèle et la concurrence au niveau du marché.[31]

Aujourd'hui le digital occupe une place de plus en plus importante. Au niveau de la banque, la diffusion de l'internet a énormément favorisé l'intégration de ces innovations technologiques. La nécessité d'exécuter les opérations bancaire d'une façon plus rapide et sans effectuer aucun contact physique était la principale raison pour laquelle les banques étaient à la recherche d'élargir la palette de leur canaux électroniques pour répondre à la nouvelle concurrence des banques digitales.[32]

La nécessite d'un nouveau design bancaire est apparue afin de faire face à la révolution digitale. Ce design a eu un impact sur les structures du monde bancaire en entier et a constitué surtout un tournant dans l'évolution du digital. Effectivement, les banques ont été obliger de réinventer face à l'économie instable et aux changement du comportement des clients dû à l'entrée de ces nouveaux acteurs.

Le client se trouvent perdu et une sorte de bouillard visuelle apparait lui empechant de distinguer surtout que cherchant la simplicité, ils s'attendent à pouvoir régler leurs problèmes en ligne à n'importe quel moment.

Ainsi les banques se sont tournées vers le digital pour mieux développer une stratégie financière bien ciblée, offrant de plus en plus des services en ligne.

En guise de synthèse, les banques digitales ont ainsi bouleversé le secteur bancaire qui ne ressemble plus à la banque traditionnelle.[33]

Le succès de la banque digitale à pousser ainsi la plupart des banques à intégrer les normes du digital dans leur service quotidien amenant à une évolution extraordinaire des banques traditionnelles qui se sont noyer dans ces turbulences digitales.

---

[31] Oussama Chencheh, les déterminants de l'adoption de l'e-Banking par les institutions financières et la clientèle organisationnelle, et son impact sur l'approche relationnelle: cas de l'internet Banking en Tunisie, Mémoire en administration des affaires, Québec, Canada Juillet 2011

[32] Harb Bissane, Saleh Mariam, les enjeux de l'e-banking au Liban, revue N. 29, 2017

[33] Laurent Bour, l'évolution des banques face à la transformation digitale, Le journal du CM, Octobre 2019

B- Une évolution de la banque traditionnelle à la banque digitale

Face à l'évolution technologique et la concurrence des banques digitales, les banques traditionnelles étaient obligées de revoir leur mode de fonctionnement de manière radicale.

L'avènement de ces nouveaux services a donc cédé le passage à un nouveau genre de banque: la banque digitale ou banque par Internet. Il s'agit d'une banque, qui ressemble à la banque traditionnelle offrant une palette plus vaste, innovante et plus personnalisée des produits et services offertes qui ne se fassent que par internet ou toute autre voie électronique.

Les banques classiques se sont sues donc dans l'obligation de se mettre au digital en changeant le mode fonctionnement de leur transactions bancaires et leur croissance ne cessent de s'accélérer ces dernières années.
Les banques traditionnelles devaient s'adapter au plus vite afin de ne pas devenir obsolètes soit en se transformant en banque digitale, soit en collaborant avec celle-ci pour ne pas perdre leur situation privilégiée.

Les banques digitales se sont présentées sur le marché comme un tremplin nécessaire et indispensable. Ceci leur a permis d'améliorer l'expérience du client avec sa banque en lui offrant des services et produits simplifiés.

En fait, les banques traditionnelles entretenaient une relation très personnelle avec leurs clients, puisque ces derniers se rendaient régulièrement à l'agence pour effectuer leurs opérations bancaires. Avec le développement de l'internet et la surgit de la stratégie multicanal (dont la banque digitale), une relation virtuelle est née entre le client et sa banque.[34] En outre, cette relation virtuelle à beaucoup faciliter toutes les genres de transactions bancaires.

La banque digitale se différencie de la banque traditionnelle puisque celle-ci implique la fourniture de produits et de services bancaires par le biais de canaux de distribution électroniques. C'est une méthode innovatrice par laquelle le client effectue des transactions par voie électronique via Internet. Elle est également connue sous le nom de transfert

[34] Abdelaziz Berdi, the relationship between traditional bank and e-banking , Revue du contrôle de la compatibility et de l'audit, Numéro 7, Decembre 2018

électronique de fonds (TEF), permettant l'utilisation de moyens électroniques pour transférer des fonds directement d'un compte à un autre, plutôt que par chèque ou en espèces.

Les banques traditionnelles devraient ainsi subir une immense obligation d'adaptation afin d'assurer la continuité de leur service et préserver leur clientèle, ce qui relève l'importance de la digitalisation de leur activité. Par suite, les acteurs du secteur bancaire traditionnel devraient, par conviction ou par nécessité, exercer profonds réformes s'ils souhaitent répondre aux attentes de leurs clients.

L'automatisation des services bancaires contribue donc à une croissance pour la banque traditionnelle lui permettant de raccourcir et de simplifier les démarches bancaires. Cela constitue une révolution externe et interne à la banque qu'induit et que permet l'innovation.

Si l'on s'intéresse aux projections futures, une étude de McKinsey réalisée en 2015 estime que d'ici 2025, les acteurs non bancaires tels que les GAFA et Fintech provoqueraient une baisse de 20 à 60% des profits dans les activités des banques traditionnelles dans lesquelles ils opèrent.

Soumises à la pression technologique et réglementaire, les banques digitales offrent une interaction plus intéressante et plus adaptée que celle qu'offre la banque traditionnelle. Ce changement profond représente un défi pour les acteurs des banques traditionnelles puisqu'il s'agit de suivre les avancées digitales et être à jour avec les modèles digitaux et répondre à toute les attentes et besoin sophistiqués des clients.

Cette adaptation à ce nouvel encadrement nécessite cependant une transformation gigantesque des banques, influencée par la technologie innovatrice.

P.2 : L'influence des innovations technologiques sur la transformation des banques

Face à un désordre digital, les innovations technologiques constituent l'un des piliers primordiaux de la transformation des banques. En effet, les banques ont tout d'abord adopter une attitude attentiste à l'envers des innovations et développement technologique

mais cette attitude a rapidement disparu avec le besoin de s'adapter à ce nouvel environnement qui a engendré un bouleversement énorme au niveau des banques.

Dans ce même sens, ce bouleversement était accompagné par une évolution des usages de la clientèle et la nécessite de couvrir leurs besoins non couverts par la banque traditionnelle. L'expérience clientèle dans cette digitalisation a ainsi significativement changée de perspective.

De ce fait, nous allons élaborer le bouleversement aperçu au niveau de l'environnement de la banque (A) avant de passer à la relation clientèle très particulière au sein de la banque digitale (B).

A. Un bouleversement au niveau de l'environnement de la banque

L'évolution du secteur bancaire marqué par une très importante montée digitale a eu un impact très important qui s'est présenté sous forme de changements vitales et fondamentales. Ces changements digitaux ont bouleversé le mode de fonctionnement du secteur bancaire.

Ainsi toutes les divisions de la banque sont à fortiori impactée par cette transformation digitale et ceci a créé une révolution industrielle.

En effet, on peut distinguer deux genres de banques ; ceux qui sont proactive et cherche à profiter des innovations offertes suite au digital, et ceux qui sont réactif et qui sont séduites à des pressions de la part du marché dans le but d'adopter les récentes innovations technologiques. Dans le premier cas, la banque innove en bénéficiant des possibilités offertes par le digital. Dans le second cas, la banque est soumise aux besoin des clients pour satisfaire leurs besoins.

En réalité, les individus, leurs habitudes, la culture bancaire ainsi que les pratiques managériales ont été affectées. En effet, le digital est devenu de plus en plus omniprésent dans l'industrie bancaire et a déjà pris plusieurs formes.

Le facteur de la compétitivité a par la suite joué un rôle indispensable au milieu de ces changements technologiques puisque les concurrents proposent des services compétitifs, ce qui engendre une grande pression sur la banque traditionnelle.

Par exemple, la FINMA a instauré une nouvelle loi « Licence light » pour aider à la transition des banques vers le digital ».

Le facteur humain a aussi été impacté par cette transformation digitale. Malgré que ce dernier reste toujours considéré comme un avantage compétitif de taille, néanmoins, le digital a bien baissé le nombre d'emplois durant les dernières années dans le secteur bancaire.

Il convient de rappeler qu'en contrepartie, plusieurs opportunités d'emploi et de nouvelles fonctions existent également du fait que le digital exige des personnes qualifiées dans le domaine de la technologie pouvant répondre aux atouts des innovations technologiques.

La structure organisationnelle de la banque se voit donc fortement bouleversée. La transformation digitale implique donc des changements multiples dans le fonctionnement de la banque mais pas n'importe quel changement. Beaucoup d'analyses et de coordination sont requises à ce niveau aussi pour savoir quoi faire et comment le faire.

En fait, il s'agit de pratiques récentes qui doivent être mises en place afin de pouvoir apporter une valeur ajoutée et en même temps amélioré la façon par laquelle la banque conduit ses affaires quotidiennes.

Wade a établi un outil nommé « digitization piano » où il liste (7) catégories essentielles dans lesquelles on peut envisager des changements ; le modèle d'affaires, la structure, les personnes, les processus, les compétences IT, les produits et services offerts, le modèle d'engagement.[35]

Par ailleurs, suite à la vitesse de l'évolution constante du domaine technologique, une transformation au niveau de l'apprentissage était incarnée. Cette culture d'apprentissage aide les employés à s'adapter facilement et rapidement au monde digital.

Donc la transformation des banques au digital nécessite un travail progressif afin de faciliter l'adaptation des toutes les ressources à ce changement tout en prenant compte du virage du digital et les opportunités qui l'accompagne.

[35] Jon P. Wade (2015), a definition of system thinking : a systems approach, Elsevier, 2015, P. 669-678

Paradoxalement et suite à cette vulgarisation digitale, des attentes exigeantes ont été remarquées auprès des clients.

B. Une relation clientèle très particulière

Selon un rapport publié par le Fidelity National Information Services aux États-Unis, les interactions entre le client et sa banque sont à 72 % numériques.[36]

Il est indeniable que le client et le premier beneficiaire de cette digitalisation.

Le client, une profane qui manque d'expérience et de connaissance mérite une protection particulière.
Le législateur libanais a l'instar du législateur français n'a pas donné une définition au client bancaire. Cependant la doctrine et la jurisprudence ont pris cette mission.

Selon la jurisprudence, le client bancaire est défini comme toute personne qui entre en contact de manière directe ou indirecte avec la banque même par une seule et unique opération et même s'il n'a pas lui-même choisit la banque. Il en résulte que doit être considéré comme un client de la banque, toute personne qui se présente à la banque pour encaisser un virement, une somme monétaire, ou un chèque représentant des sommes d'argent déposées auprès de la banque.[37]
Le digital a fait émerger un nouvel model bancaire décrit comme connecté, bien équipé et agile où l'agence traditionnelle tient une place complètement différente dans la relation avec la clientèle.[38]

Il est irrévocable que le client, integré dans la communauté virtuelle, constitue la base de la stratégie digitale de la banque et constitue une priorité pour la banque. En effet

[36] BPCE Recrutment, quelles sont les nouvelles habitudes bancaires des millennials, https://blogrecrutement.bpce.fr/quelles-sont-nouvelles-habitudes-bancaires-millennials
[37] JP pénale de Beyrouth, 23 Nov. 1971: Rec. Hatem fasc. 121 p. 53, note critique. Kortbawi.
[38] Boumedienne Nadia, Renaud Gracia Bardidia, L'impact du digital sur la clientèle des services bancaires cas de la BEA d'Oran, revue innovation, Volume: 11/ N°: 01A (2021), 30 Juin 2021

l'émergence des nouvelles technologie d'information et de communication à céder la place à de nouvelles façons d'interaction entre la banque et son client.[39]

La transformation digitale a fait paraitre un nouveau type de client qui est à la fois plus informé et plus exigeant.
« Les banques ont bien compris une chose, elles n'ont pas besoin de stratégie digitale, mais de digital dans leurs stratégies. » [40]

Cette nouvelle génération de clientèle connectée n'est plus obliger de se déplacer en agence, attendre des heures pour finaliser ses opérations ou bien prendre un conseil sur un produit. Tout est disponible sur internet et l'information bancaire est désormais accessible à tout le monde.

La manière d'interagir avec la clientèle a bouleversé. La digitalisation à fortement modifier les habitudes de gérer les opérations bancaires. La banque et le client sont la plupart du temps aujourd'hui connectés et ont des préférences déterminées par ce qui est accessible sur le site web. Par opposition aux générations précédentes, qui se déplaçaient beaucoup en agence pour finaliser leurs opérations.[41]
Les évolutions du digital ont été porteuses d'avantage mais aussi d'incertitude pour la clientèle. Nous pouvons désormais constater que le client de nos jours est devenu très difficile à satisfaire puisqu'il veut faire tout dans le plus court temps possible .[42] Cela vient du fait que le mode de vie a bien changer avec le développement des nouvelles technologies.

Ainsi le client a l'ère digitale s'est à son tour habitué à la facilité, rapidité et accessibilité des produits et des services offerts par la banque comme il peut tout faire en un seul clic.

[39] Adala, A., & Djellam, A. (2015). Le rôle du marketing digital dans l'amélioration des performances des banques commerciales Algérienne, étude analytique statéstique. Finances et marchés, p 26-44
[40] Lamirault, F. (2017). L'évolution du modèle bancaire à l'ère du digital. Paris: Livres blancs
[41] Institut de recherche en management et en pratique de l'entreprise, la digitalisation au sein du secteur bancaire entre causes et consequences, Juillet 2020
[42] Mk Mckinsey, accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France, Mckinsey&Company, 2014.

Son expérience bancaire est significativement meilleure dans ce nouvel type de relation avec sa banque.

En effet, le client de notre temps détient la capacité d'interagir facilement avec sa banque. La communication est devenue plus interactive. Il est devenu plus informé notamment grâce aux diverses informations accessibles sur le web[43]. Il peut même affecter la réputation de la banque ou même la valoriser simplement en laissant un commentaire sur le web, en la recommandant ou pas.

La banque digitale a offert des services plus personnalisés, adapter au profil de sa clientèle et par conséquence les attentes du client à cet égard ont évolué. Cependant les clients, reconnaissant les avantages de la banque digitale, ont peur de l'utilisation compliquée et parfois difficile de ces services diverses, ce qui parfois crée un frein pour l'utilisation et une relation tendue avec la banque. Cela nous amène a étudié profondément l'apport de la banque digitale aux activités bancaire.

Section 2 : L'apport de la banque digitale aux activités bancaires

La digitalisation du secteur économique a touché toutes ses branches surtout les banques comme on a déjà mentionné. La montée digitale très importante a affecté largement le secteur bancaire au cours des dernières années, ce qui a entrainé un changement indispensable dans les opérations bancaires effectuées au sein de la banque (P.1).

Tenant compte dela singularite des pratiques en ligne et leur croissance incessante, cette transformation s'est accentue encore avec l'avènement de la pandémie qui malgré ses conséquences néfastes sur le domaine sanitaire notamment la santé mentale, elle a eu un impact extraordinaire sur la transformation digitale des banques (P.2).

P.1 Une transformation digitale des opérations bancaires

Parallèlement a l'avènement des modalités facilitant l'interaction humaine, l'avènement des banques digitales constitue un évènement marquant cette évolution du numérique. En fait, le numérique se caractérise par des stratégies obscures et des pratiques sophistiqués.

[43] Chamoux J.P., L'ère du numérique 2 : l'économie revisitée, Ed ESTG, London, 2018.

Au cours des dernières années, les banques digitales ont élargi la gamme des services digitaux offertes, qui sont souvent au cœur de la transformation digitale, dans le but de rester à jour compte tenu des nouvelles règlementations et évolutions dans le secteur économique et dans le but de satisfaire les besoins de ses consommateurs (A).

Les recherches autour ces services étaient préciseuses et profitables, adaptées à leur nature électronique. Ces derniers ont été le témoin de la transition des opérations manuels au digital avec la digitalisation de tous les processus existants au sein de la banque qui espèrent battre les opérations manuelles à leurs propre jeu (B).

A. Les services digitaux offerts par la banque digitale

L'évolution des services digitaux a suit le développement des usages du client bancaire et les besoins qui n'ont pas été couverts par les banques traditionnelles.

a. Le Mobile ou web Banking

Il y a quelques années, le téléphone servait juste pour prendre un rendez-vous avec le client ou pour savoir les produits et sévices offertes par la banque. Aujourd'hui les plateformes téléphoniques ont développé. La banque mobile concerne le système par lequel le client peut accéder à tous les informations relatives à son compte sur le téléphone. Cet accès est activé avec l'utilisation d'appareils mobiles par les clients des banques.

L'émergence des tablettes numériques et smartphones a contribué à l'essor de la banque digitale. Ils offrent multiples services simples disponible par téléphone au lieu de se déplacer en agence. Par exemple effectuer un virement, connaitre un solde, renseignement sur un produit et beaucoup d'autres.

Le web Banking permet de même de conduire les mêmes opérations que le mobile Banking mais sur le web.

b. La carte de paiement (E-Paiement)

Au Liban, selon un article publié dans la revue économique mensuelle libanaise « le Commerce du Levant », se basant sur les sources de la BDL, le nombre de cartes bancaires en circulation a connu une augmentation mensuelle moyenne de 0,56% durant le premier

trimestre 2011 jusqu'en avril 2011, pour atteindre 1,72 million de cartes bancaires utilisées dans le marché libanais[44].

La carte de paiement est une carte en plastique qui est encodée magnétiquement, standardisée et utilisée par le client comme un moyen de paiement pour retirer ou transférer les fonds. En effet, le numéro sur la carte permet d'effectuer tous les paiements requis.

Le concept de carte de paiement, de crédit et de retrait a fait son apparition lorsque le législateur a complété l'article 70 du Code de la monnaie et du crédit lié à la mission de la BDL en vertu de la loi n° 133 du 26 octobre 1999 qui a pénétré à l'activité de celle-ci, celle de faire évoluer et de règlementer « les moyens de paiement et en particulier les opérations se réalisant par le biais du distributeur automatique de billets et les cartes de retrait ou de paiement ou de crédit ». Cette législation a été précédée de l'arrêté n° 7299 du 10 juin 1999 issue du gouvernement de la BDL relatif au « distributeur automatique et – aux - cartes de crédit et de paiement ». Aussi la BDL a consacré le règlement relatif à la compensation électronique des cartes de paiement en vertu de la décision n° 8341 du 24 janvier 2003[45].

c. Le portefeuille numérique ou digital wallet

La carte virtuelle est une carte stockée exclusivement sur le téléphone. Elle peut être utiliser pour les paiements en ligne ou dans les magasins avec la technologie sans contact. Telle la carte bancaire physique, cette dernière a un numéro et une date d'expiration. Elle est utilisée souvent pour éviter les risques de piratage informatique et de fraude qui ont émergé avec l'essor du e-commerce.

Il suffit d'entrer son numéro à 16 chiffres, sa date d'expiration et son code de vérification au moment du paiement pour effectuer une opération. Les portefeuilles numériques utilisent les capacités sans fil d'un appareil mobile comme le Bluetooth, le Wi-Fi et les signaux magnétiques pour transmettre en toute sécurité les données de paiement de l'appareil à un point de vente conçu pour lire les données et se connecter via ces signaux.[46]

---

[44] Le Commerce du Levant, Les cartes bancaires en hausse fin 2011, 24févr. 2012.

[45] Decret. No 8341, Circ. no92, 24 janv. 2003, relatif à l'émission des cartes électroniques : JO no 9 du 6 févr. 2003 p. 995s.

[46] Carte bancaire virtuelle, définition et utilisation, 07 Juin 2021, https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1502381-carte-bancaire-virtuelle-definition-et-utilisation/ date de la visite le 6 Octobre 2021

d. Le guichet automatique (Automated Teller Machine)

L'ATM, disponible 24 heures sur 24, est considéré comme l'outil le plus utilisé pour transférer des fonds par voie électronique. Pour accéder aux comptes via un guichet automatique, les clients doivent utiliser la carte bancaire et utiliser les fonds sur le terminal informatique de la machine de manière appropriée. Les clients peuvent ainsi retirer de l'argent d'un compte bancaire, transférer de l'argent d'un compte à l'autre et effectuer d'autres fonctions grâce à l'utilisation de l'ATM.[47]

e. Le cloud computing

Au Liban, il n'y a pas de réglementation spécifique sur le cloud computing. Néanmoins, tout cloud computing impliquant des données personnelles doit être conforme à la loi sur les transactions électroniques et les données personnelles et à la loi sur la protection des consommateurs.

Cependant, le cloud computing est spécifiquement interdit en ce qui concerne certaines activités, telles que le financement participatif; et il est interdit aux institutions de financement participatif de stocker des bases de données par le biais de toute forme d'informatique en nuage partagée. De plus, bien qu'il n'y ait pas d'interdiction légale expresse contre les banques utilisant le cloud computing, la loi sur le secret bancaire semble être un obstacle pour les banques libanaises, en raison des exigences de protection des données des clients prévus par cette loi.

Le cloud est un pilier des technologies de communication et de l'information. Il permet aux banques d'améliorer leur agilité. En effet la digitalisation des banques de nos jours dépend fortement du cloud computing. Ce dernier permet l'accès aux divers services via l'internet comme les applications de stockage de données et les banque de données. Le choix de faire transférer ces services vers le cloud dépend largement de l'évaluation des besoins et attentes a priori.[48]

[47] Toufaily, E., Daghfous, N., & Toffli, R. (2009). The Adoption of "E-Banking" by Lebanese Banks: Success and Critical Factors. International Journal of E-services and Mobile Applications, 1(1), 67-93.

[48]Nicolas Spatola, e cloud computing : quels avantages et risques dans le cadre de la transformation digitale ?

f. Les crypto technologies (Block Chain, crypto-monnaies)

La BDL a longtemps adopté une position plutôt défavorable à l'égard des crypto-monnaies et a mis en garde les banques et institutions financières libanaises contre leur utilisation, en attendant la promulgation des lois et règlements pertinents. Cependant, il a été récemment rapporté dans la presse que le gouverneur de la BDL pourrait lancer une crypto-monnaie libanaise. Notant que la BDL est investie, en vertu de la loi sur les transactions électroniques et les données personnelles, d'une autorité étendue concernant l'émission et la réglementation de la monnaie électronique et numérique.

En effet, le gouverneur de la BDL, Riad Salameh, a déclaré lors du quatrième forum anti cybercriminalité organisé par le groupe de presse Economie et Travail et la Banque Centrale à fin octobre 2019 : "Le Liban introduira sa propre monnaie numérique dans un avenir proche". Cette monnaie numérique « 100% Made in Lebanon », va être lancée par la banque centrale en livres libanaises et ne sera utilisé qu'au Liban. « Son but est de simplifier les méthodes de paiement, entreprendre une révolution technologique des institutions financières et réduire les dépenses de consommation, mais d'abord, la BDL doit prendre les mesures nécessaires et mettre en place un système de prévention de la cybercriminalité”.

Aucune réglementation spécifique ne réglemente explicitement le block Chain au Liban.
L’adoption des services digitales par les banques a été suivi par l’arrêt des opérations manuels au sein des banques. Ces derniers ont ainsi été remplacé par des solutions plus techniques sur des interfaces simples et conviviales.

B. Une transition des opérations manuels au digital

https://artimon.fr/perspectives/le-cloud-computing-quels-avantages-et-risques-dans-le-cadre-de-la-transformation digitale/#:~:text=Le%20cloud%20computing%20est%20un%20processus%20d'acc%C3%A8s%20%C3%A0%20des,outil%20digital%20de%2 l'utilisateur. Date de la visite 07 Octobre 2022

La transformation numérique entamée il y a quelques années et le développement rapide des services digitalisés ont permis aux banques de s'adapter à tous les changements qui ont affecté le secteur bancaire et spécialement la crise sanitaire et par suite assurer une continuité de l'activité bancaire. En fait, avec le COVID-19 et les divers divisions bancaires ont accéléré l'utilisation des canaux digitaux.[49]

Les banques pourraient générer jusqu'à 140 milliards de dollars de gains de productivité et d'économies en modernisant les technologies de la main-d'œuvre.[50]

Les recherches du McKinsey Global Institute concluent que 40 % des activités financières à l'exemple du décaissements et des opérations générales peuvent être entièrement automatisées.[51]

Le digital a piloté l'automatisation intelligente dans le secteur bancaire. Grâce aux nouvelles technologies d'information et de communication, les banques ont développé une relation à distance avec leurs clients. Ainsi ces derniers peuvent utiliser leur compte bancaire en temps réel via le mobile Banking ou web Banking sans se déplacer en agence.

Signalons que tous les données des clients sont disponibles sur les applications de la banque.[52] Une convergence est donc essentielle entre tous les canaux et les agences physiques.

Le développement de la banque digitale a pris (2) formes différentes, la première est traduite par le développement d'opérateurs en ligne et la seconde par le développement des majeurs services en ligne offertes à la clientèle.

La transition des opérations de la banque traditionnelle a la banque digitale est caractérisé par la rapidité, la facilité et l'autonomie. En conséquence, les banques ont réalisé une

[49] La transformation numérique dans le secteur bancaire français, ACPR banque de France, N. 131, 2021
[50] Accenture ,Rapport annuel, 2012-2022
[51] Frank Plaschke, Ishaan Seth, and Rob Whiteman, Bots. Algorithms and the future of the finance function, Article, 9 January 2018
[52] Boumedienne Nada et Renaud Garcia Bardidia, l'impact du digital sur la clientele du service bancaire, revue innovation, Volume: 11/ N°: 01A (2021), p 814-830

augmentation des bénéfices et une diminution des frais opérationnels, comme ces derniers ont renoncé aux procédures utilisées pour effectuer les transactions financières en l'absence de transactions électroniques. Dans le même sens, l'évolution de l'automatisation des services bancaires a diminué énormément le coût du capital humain.

Le directeur général de Deutsche Bank John Cryan a affirmé : "Dans notre banque, nous avons des gens qui travaillent comme des robots. Demain, nous aurons des robots qui se comporteront comme des personnes. Peu importe que nous, en tant que banque, participions ou non à ces changements, cela va se produire".[53]

Par exemple aussi, le numérique a dispensé les agents de services de plusieurs tâches quotidienne citons la clôture du comptes, l'envoi de notification, le blocage de code et la gestion des transferts de clients ce qui a amélioré l'efficacité opérationnelle des employés.

Ainsi, l'automatisation des paiements a permis aux agents de services de consacrer plus de temps aux tâches quotidiennes stratégiques et a par suite accélérer la vitesse de traitement.[54]

Toutefois, la transformation numérique n'est pas un simple processus technique. Cette transition impacte fortement les ressources humaines suite aux transformations énormes induites dans les métiers bancaires.

Selon le Financial Times, Micheal Corbat, PDG de Citigroup, a annoncé que la numérisation pourrait contribuer à éliminer des dizaines de milliers d'emplois dans les centres d'appel.[55]

Notons enfin que cette digitalisation était impératif surtout avec l'avenu de la pandémie qui a obligé le monde entier à choisir la digitalisation comme le seul et premier choix pour échapper à son influence catastrophique dans le domaine de la technologie.

---

[53] Deutsche Bank, boss says 'big number' of staff will lose jobs to automation, the Guardian, 2017

[54] Katherine Manning, l'automatisation intelligente dans le secteur bancaire, 12 Octobre 2021, https://www.processmaker.com/fr/blog/intelligent-automation-in-banking/ date de la visite 06 Octobre 2021

[55] Laura Noonan and Patrick Jenkins, Citigroup CEO says machines could cut thousands of call centre jobs, Financial Times 2019

P.2. L'impact de la pandémie sur la transformation digitale des banques

Les résultats de la pandémie du Covid19 sur la digitalisation du secteur bancaire ont été énorme dans un univers électronique. Recourir au digital durant la crise était essentiel afin de sauvegarder le pouvoir d'achat, maintenir l'économie et chercher des solutions qui puissent limiter les conséquences néfastes, voire les préjudices.

Malgré le contexte défavorable de la pandémie, il est incontestable que celle-ci a réussi à bâtir un nouveau model digital pour s'adapter à ses conséquences défavorables, encourageant un recours vaste au services financiers à distance.

Il convient de traiter en premier lieu la digitalisation accélérée par la crise sanitaire (A) et d'analuser en second lieu le défis de la crise sanitaire en matière de digitalisation des banques (B).

A. La digitalisation accélérée par la crise sanitaire

L'année 2020 a permis une transformation digitale d'une supérieure vitesse dans le monde entier.

Il n'est pas surprenant que le confinement, les mesures sanitaires et le développement fort du télétravail introduits dans le monde entier suite au COVID-19 ont précipité la mutation digitale, changé les habitudes de la clientèle bancaire et bouleversé l'équilibre des banques traditionnelles.

Ainsi les succursales ont fermé leurs portes suite à la fermeture nationale et les clients n'ont plus d'autres moyens pour interagir avec leurs banques qu'à travers le mobile et les services bancaires en ligne pour assurer la continuité de l'exploitation.

A ne pas oublier que les points de contact digitaux ont remplacé les points de contact physiques.

Le confinement a pris la relation client-banque vers une autre dimension et a par la suite modifié les usages bancaires.

Le changement du comportement bancaire des clients durant la crise sanitaire était très évident et cela a été traduit dans leur façon de gérer leurs opérations bancaires surtout les clients encore réticents à adopter les technologies de l'informatique.

Ce changement était à la base du changement de la culture bancaire et sa transition au digital à travers le monde surtout avec le recours au télétravail. Ce recours s'est accompagné de la mise en place de nouveaux mode travail parfois hâtive qui ont fait accroître la vulnérabilité de ce secteur.

Selon Fidelity National Information Services (FIS), une organisation qui travaille avec les plus grandes banques du monde, a annoncé une augmentation de 200% des nouvelles inscriptions aux services bancaires mobiles début Avril 2020, et un bond de 85% du trafic des services bancaires mobiles.[56]

47% des consommateurs interrogés par Accenture ont réclamé préférer recourir à une application mobile ou un site web pour ouvrir un nouveau compte bancaire, alors que 37% favorise l'ordinateur portable.[57]

D'un autre côté, la pandémie a changé la façon par laquelle les clients effectuent leurs achats. Ces derniers utilisent de plus les paiements mobiles sans contact. Cette augmentation a surgit de 40% dans le monde et le nombre des comptes enregistrés sur les paiements mobiles a surgit de 13%[58].

Ainsi, la crise a augmenté le pourcentage des clients bancaires ouverts à l'utilisation de la banque digitale et cette dernière à son tour a pu facilement répondre aux besoins du marché

[56] Ellen Sheng, Corona virus crisis mobile banking surge is a shift that's likely to stick, Mat 27, 2020 https://www.cnbc.com/2020/05/27/coronavirus-crisis-mobile-banking-surge-is-a-shift-likely-to-stick.html date de la visite 2 Decembre 2022

[57] Accenture Global Banking Consumer Study, Making digital banking more human, 2020

[58] StarDust CTG Group, Comment le covid19 accélère la transformation numérique de la banque de détail https://www2.stardust-testing.com/blog-fr/comment-le-covid-19-accelere-la-transformation-numerique-de-la-banque-de-detail date de la visite 3 Decembre 2022

grâce à ces techniques digitales accessible à tout le monde et à même améliorer ses services en ligne et mobiles pour répondre aux enjeux de cette transformation numérique.

La pandémie a joué le rôle du catalyseur de la digitalisation des banques. Cette accélération dans l'utilisation du digital dans le quotidien est un signe de l'agilité de la banque et sa capabilité de répondre aux besoins de ces clients.

La concurrence féroce entre les banques s'est augmentée puisque ces derniers développaient des offres à distance pour répondre aux besoins de la clientèle et aux nouveaux mode de consommation.

Il était donc urgent pour les banques traditionnelles de chercher des nouvelles modèles digitales et d'ajuster les modèles de gestion de leurs opérations pour investir dans la technologie et suivre le marché financier[59].

Les entreprises ont bondi en moyenne 6 ans dans leur stratégie de transformation numérique grâce à la crise. De même, la crise a consacré l'omni canal dans le but de garder le lien avec les clients. 53 % des entreprises interrogées ont ajouté de nouveaux canaux digitaux durant la pandémie[60].

Cependant cette digitalisation était pleine de défis auxquels le secteur bancaire devait faire face, car les banques étaient projetées en première ligne face à la crise assumant une très grande responsabilité.

B. Les défis de la crise sanitaire en matière de digitalisation des banques

La transformation digitale est un enjeu majeur pour le secteur bancaire et l'économie. La pandémie a eu un impact énorme sur ces enjeux de digitalisation du secteur bancaire.

[59] Salma Aider, Covid-19 et secteur bancaire: la digitalisation des banques s'accélère 4 Juin 2021, https://fr.linkedin.com/pulse/covid-19-et-secteur-bancaire-la-digitalisation-des-banques-aider date de la visite 3 Decembre 2022

[60] Twilio, Covid-19 digital engagement report, date de la visite 3 Decembre 2022 https://www.twilio.com/covid-19-digital-engagement-report

Il est incontournable que la digitalisation est la seule raison qui a permis la continuité des activités bancaire durant la crise sanitaire. Cette crise n'a pas seulement favorisé la digitalisation mais aussi accélérer la transformation des banques traditionnelles en banques digitales.

Ainsi les conséquences de la pandémie sur la digitalisation des banques ont été énormes. En effet, cette digitalisation est un défi essentiel auquel la banque devait faire face surtout durant la crise puisque maintenir la banque c'est maintenir le pouvoir d'achat de ces clients en particulier et maintenir l'économie en général.

Malgré ce contexte défavorable, les banques devaient construire de nouvelles modèles pour s'adapter aux conséquences défavorable de la pandémie. En effet, la vitesse de la digitalisation des banques durant l'année 2020 a connu son essor. La pandémie a fortement encourage le recours au télétravail et l'utilisation des services financiers à distance[61].

Le mode de paiement sans contact a constitué la nouvelle norme. Cependant, cette modernisation était accompagnée par des défis majeures surtout sur le niveau de la sécurité et de l'infrastructure.

Dans ce sens, ces nouvelles technologies adoptées durant la crise on fait face à une résilience de la part des clients non adaptes à l'utilisation de telle technologie. Ce qui a créé des tensions au niveau de la clientèle et même des employés.

La période de rebond doit laisser une place à la phase d'évolution dont le but est de changer le paradigme de la banque traditionnelle et qui fournit une gestion des activités bancaires plus adaptée aux évolutions introduites par la pandémie.[62]

Les banques devraient accélérer les outils nécessaires pour prévenir les risques qui peuvent surgir d'une telle crise. Ainsi, cette crise a révélé des lacunes énormes dans la

[61] ZAOUI Asmae, BOUDAOUD Fatima, HASSEB Mohamed Lamine, L'impact du covid-19 sur la transformation digitale du secteur bancaire, Revue d'excellence pour la recherche en économie et en gestion, Vol 05, N°01 (2021), P 497-509 3 Juin 2021
[62] Hamilton Gomes, Covid-19, un accélérateur de la transformation du secteur bancaire ?. https://www.cgi.fr/.

transformation digitale considérées comme essentielles pour le bon fonctionnement de la banque et la gestion des crises.

Aussi, les banques ont cherché à créer de nouveaux services bancaire pour répondre aux besoin de leurs clients surtout les banques traditionnelles qui étaient obligées à se transformer rapidement dans un environnement exceptionnel.

Les banques ont connu une croissance significative dans l'adoption des moyens de paiement sans contact et les paiements par téléphones mobiles. Ces moyens se sont avérés très efficace pour cantonner la prolifération du virus. Cependant, le taux de fraude a aussi augmenté suite à l'augmentation des paiements électroniques.[63]

Ainsi la crise a accéléré l'adoption du digital par beaucoup de banque traditionnelle ce qui a permis d'ouvrir de nouveaux horizons dans le domaine de l'innovation des produits et services ou répondre à la mutation rapide du secteur bancaire.

On peut conclure que la pandémie à renforcer l'importance énorme de la digitalisation dans le secteur bancaire. La nécessite de faire face à la crise a permis aux banques de chercher les meilleurs outils de l'innovation et d'activer leur transformation numérique.

Afin de bien comprendre la légitimité de la banque digitale au sein de ce bouleversement numérique, il est primordial d'étudier le cadre réglementaire de la banque digitale au Liban.

[63] Boudchicha Rima, Kahoul Mohamed Yazid, Impact de la Pandémie du Coronavirus sur le Paiement Électronique en France – Etude Descriptive Analytique, 31 Décembre 2021, Revue EL - Maqrizi pour les études économiques et financières Volume:5 / N°:2 (2021), p 329-348

Chapitre 2 : L’encadrement juridique de la banque digitale au Liban

Dans cet environnement digital, l’ensemble des lois qui englobe le cadre juridique de la banque digitale au Liban est encore timide. En effet, pour bien comprendre les nouveaux règlements qui ont donné une légitimité aux opérations électroniques des banques digitales, il convient de reconnaitre la nature de ces règlements, les garanties et les contrôles.

Dans ce cadre, nous examinerons la réglementation libanaise timide de la banque digitale (section 1), pour passer ensuite aux fragilités et menaces dans le cadre juridique libanais (section 2).

Section 1 : Une règlementation libanaise timide de la banque digitale

Dans cette section, on exposera deux réglementations importantes dans le sujet de la banque digitale ; la réglementation des opérations électroniques par la BDL (P.1), ainsi que le statut législatif de la loi 81/2018 en matière électronique (P.2)

P.1 : La réglementation des opérations électroniques par la BDL

La BDL est l'organisme de réglementation chargé d'octroyer le consentement aux établissements qui exercent des activités bancaires, de change et/ou financières, y compris les établissements de crédit et les prestataires de services de paiement électronique.

Nous aborderons dans ce sujet, la circulaire 69/2000 liée aux opérations bancaire et financières électroniques (A) ainsi que l’évolution des opérations digitales suite aux révisions introduites à la circulaire 69.

A. La circulaire 69/2000 – Les opérations bancaires et financières électroniques

Les transferts électroniques de fonds, également connus sous le nom de EFTs (Electronic Funds Transfers) sont une technique courante pour transférer des fonds d'un compte à un autre via un serveur informatique.

Ces transferts, offrent aux clients la commodité de gérer leurs propres transactions, ainsi que remplacer les transactions sur papier et les intermédiaires humains.

Chaque fois qu'un client d'une banque utilise sa carte de crédit ou de débit à un point de vente ou électroniquement, un transfert électronique d'argent se produit.

En fait, une seule licence EMT est considérée comme le seul service EMT moderne du Liban : PinPay. Cependant, PinPay, n'a obtenu cette licence que lorsque Bank Audi et Bankmed ont acheté l'entreprise et se sont portés garants de la solvabilité et de la sécurité de PinPay. Les deux banques ont ensuite rendu PinPay accessible uniquement à leurs clients, un service que d'autres banques au Liban ont maintenant copié.

Environ 65 banques commerciales, ainsi que quelques institutions de transfert d'argents, sont autorisées à effectuer des EFT nationaux et internationaux, par BDL.

En conséquence, ces institutions jouissent d'une position dominante sur le marché et n'ont que peu d'intérêt à offrir des frais EMT compétitifs à l'échelle mondiale, des services sur place ou des taux de change moyens.[64]

Ainsi le client est toujours incapable d'effectuer des paiements électroniques à quiconque en dehors de sa propre banque sans payer des frais exorbitants.

Notant que seul les banques licenciées par BDL ont le droit de conduire des activités EMT.

En addition, les transferts d'argent mobiles, également connus sous le nom de MMT (Mobile Money Transfers) sont des services qui permettent aux consommateurs d'envoyer et de recevoir de l'argent en utilisant leur appareil mobile - ou, pour le dire autrement, en

[64] Halabi Sami, the need to reform electronic money transfer regulations, June 7, 2019 https://www.executive-magazine.com/business-all/the-need-to-reform-electronic-money-transfer-regulations

utilisant un téléphone intelligent pour faire un paiement numérique d'un utilisateur à l'autre. Les services de transfert d'argent comprennent à la fois des fonds nationaux et internationaux, ou transfrontaliers.

On peut conclure que les services de la banque digitale sont en plein essor au Liban.

La BDL a renforcé les règles pour les transferts électroniques enregistrant un retard considérable par rapport à d'autres pays arabes.

Ainsi, au menu des banques libanaises, le parlement a publié la loi 133 du 26 Octobre 1999 qui a modifié l'article 70 du code de la monnaie et du crédit qui donnent à la BDL le pouvoir de développer et de réguler les moyens et les systèmes de paiement, en particulier les transactions effectuées au moyen de guichets automatiques bancaires, les cartes de débit, ou de crédit et les virements en espèces, y compris les transferts électroniques jouissant ainsi du droit de surveillance et d'imposer des amendes et des pénalités administratives.

Dans ce sens, le 30 Mars 2000, la banque du Liban a émis désormais la décision 7548, circulaire basique N. 69 relative "aux opérations bancaires et financières effectuées par voie électronique". Ce texte est à présent le seul régissant le domaine de la banque électronique au Liban. Il est adressé à toutes les institutions effectuant des transactions financières et bancaires électroniques au Liban.

Selon l'article 1 de la circulaire 69, la définition des EFT est la suivante « toutes opérations ou activités conclues, exécutées, ou promus par des banques ou des institutions financières ou toute autre institution par voie électronique ou par moyens électroniques (téléphone, ordinateur, internet, guichet automatique, etc.) ».

Cette circulaire a règlementé les transactions électroniques dans le secteur financier et a défini les transactions électroniques fournissant ainsi un premier cadre réglementaire général.

Ainsi, Le transfert électronique d'argent est réglementé par la BDL ; Les paiements électroniques et les transferts d'argent ne peuvent être effectués que par des banques, des

institutions financières ou d'autres institutions légalement autorisées ou agréées par la BDL.

Le paiement électronique et les opérations bancaires comprennent :

- Les opérations conclues, exécutées ou promues par des moyens électroniques ou photo-électroniques (par exemple, mobile, ordinateur, Internet, guichets automatiques);
- Les opérations exécutées par les émetteurs ou les promoteurs de tous types de cartes électroniques de paiement, de débit ou de crédit ;
- Les transferts électroniques d'espèces; et
- Les offres, achats, ventes et tous autres services bancaires électroniques exécutés par le biais de sites Internet spécialisés.

Ces prestations sont soumises à la surveillance de la BDL. Les prestataires de services de paiement doivent prendre toutes les mesures nécessaires et présenter les documents demandés pour faciliter et assurer l'efficacité de ce contrôle.

Selon la circulaire 69, Les prestataires de services de paiement électronique doivent prendre des mesures, entre autres, pour :

- Fournir des termes et conditions clairs et explicites des paiements électroniques au client conformément aux règlements de la BDL, y compris les droits et obligations relatifs aux services bancaires électroniques, les frais, les dépenses, etc. ;
- Obtenir l'accord écrit préalable du client sur les conditions régissant les paiements électroniques, les virements et leur annulation ;
- Prendre toutes les mesures d'atténuation des risques nécessaires ;
- Stocker et protéger les données contre la divulgation, la destruction, l'utilisation abusive, la perte et le vol ;
- Faciliter l'accès de la BDL à leur système à des fins de supervision ;
- Faire préparer par leurs vérificateurs externes un rapport annuel sur les opérations électroniques;
- Maintenir le secret des transactions ; et

- Assurer le respect des lois, réglementations et guides applicables en matière de protection des données, de cyber sécurité, de lutte contre le blanchiment d'argent (AML), de lutte contre le financement du terrorisme, etc.

Les opérations bancaires exécutées par mobile entre clients de banques différentes sont interdites, à l'exception de la réception par une banque d'une demande de virement bancaire d'un client, à condition que :

- Le transfert n'est pas exécuté instantanément via une application ou un logiciel mobile ;
- Le back office de la banque concernée vérifie que la demande de virement est conforme aux lois et règlements applicables ; et
- Le transfert est exécuté uniquement par les méthodes conventionnelles habituelles (c'est-à-dire par SWIFT).

Signalons ici que l'entrée du réseau SWIFT (Society for Worldwide Interbank Financial Télécommunication) en juin 1994 a été une raison primordiale de l'évolution des transferts bancaires internationaux du Liban. Cette introduction a permis au secteur bancaire libanais l'échange mondial instantané de tous ses messages.

La connexion des banques libanaises au SWIFT a permis au Liban de faciliter ses opérations bancaires internationales et d'amplifier sa participation mondiale dans le réseau SWIFT.[65]

Toutefois, les clients de différentes banques peuvent effectuer des opérations bancaires ou financières électroniques par le biais d'applications et de logiciels installés sur des appareils mobiles et électroniques, en utilisant des cartes et/ou des comptes bancaires, à condition, entre autres :

- L'approbation préalable du BLD est obtenue pour ces applications et logiciels ;
- Les opérations sont exécutées instantanément entre les clients ;

[65] Dr. Nasser Saidi, Le système de paiement au Liban

- La valeur de ces opérations ne dépasse pas certains seuils, tels que déterminés par la BDL ; et
- Les opérations sont conformes aux lois et réglementations applicables en matière de conformité et de lutte contre le blanchiment d'argent.

La dite circulaire s'applique également aux prêts en ligne et les établissements agréés doivent se conformer à ses dispositions, notamment les suivantes :

- S'inscrire auprès de la BDL pour effectuer des paiements électroniques et des opérations financières ; et
- Obtenir l'agrément préalable de la BDL pour effectuer des opérations bancaires ou financières électroniques exécutées via des applications ou des logiciels sur des appareils électroniques mobiles et fixes et au moyen de cartes bancaires.

La BDL circulaire 69 était l'objet aussi de plusieurs modifications qui ont joué un rôle très important dans l'évolution de la banque digitale. On les verra ci-après.

B. L'évolution de la banque digitale suite aux révisions introduites à la BDL circulaire 69

La BDL circulaire de base 69/2000 relative aux opérations bancaires et financières électroniques a fait l'objet de plusieurs modifications pour tenir compte des évolutions technologiques.

La Circulaire intermédiaire 355 du 28 février 2014 a été révisée dans le but de n'accepter la signature électronique qu'après réunion des conditions suivantes:

- Accord express entre l'établissement concerné et le client qui: - indique les risques potentiels en cas de signature électronique - et définit les procédures adéquates à suivre et ce en applications des plus hautes mesures de sécurité et ce sous l'entière responsabilité des parties concernées.
- Utilisation par le signataire d'un code d'identification personnelle
- Confirmation adressée par la société exécutrice, dans un premier temps par courrier électronique dans un délai maximal de 24 heures à dater de l'exécution de

l'opération, puis dans un second temps par courrier normal sauf autre instructions de l'intéressé

- Notification d'une situation mensuelle détaillée, à l'adresse indiquée préalablement par le client (l'alinéa (3) de l'article 21).

L'utilisation des services en ligne dans le domaine bancaire, gagne progressivement une popularité au Liban. Dans le but de réglementer ce marché, la BDL a publié le 30 Juin 2015, la circulaire intermédiaire 393, interdisant l'exécution de toutes les opérations bancaires au moyen d'appareils électroniques portables ou fixes entre les clients de différentes banques, sauf s'ils doivent recevoir des transferts d'argent. Ces transferts d'argent ne peuvent pas avoir lieu à l'aide d'une application ou de tout autre programme installé sur l'appareil du client, elles ne peuvent être exécutés que via le réseau SWIFT traditionnel adopté par les banques commerciales.

La BDL a également exigé des banques commerciales qu'elles fassent preuve de diligence en ce qui concerne les consommateurs impliqués dans ces transferts d'argent. Le back-office des banques impliquées dans les transferts d'argent électroniques doit s'assurer que la transaction est conforme aux règles et réglementations. Les banques devraient également s'appuyer sur des documents officiels pour vérifier l'identité des clients et leurs adresses. En outre, des registres spéciaux doivent être conservés pour les clients effectuant des virements électroniques d'une valeur de USD10 000 ou plus et une copie de ces registres doit être conservée par les banques pendant au moins cinq ans. On remarque ainsi que la BDL a fait accroitre les mesures de diligence dans le but de protéger le client au cours de ces opérations.

De même, La BDL a publié une circulaire intermédiaire 539 le 27 janvier 2020, qui fixe les exigences et réglementations relatives aux opérations financières et bancaires électroniques entre les clients des différentes banques.

Cette nouvelle décision, affirme que toutes les applications ou plates-formes électroniques utilisées à cet effet doivent être préalablement approuvées par la BDL. Aussi, il stipule que les opérations bancaires doivent être réalisées instantanément entre les clients et seront donc réglées via le compte de la banque concernée à la BDL.

Cette circulaire a aussi interdit l'émission et l'usage de la monnaie électronique.

Aussi, elle a autorisé la réalisation d'opérations financières et bancaires par le biais d'applications mobiles ou informatiques utilisant des cartes et/ou des comptes bancaires, sous certaines conditions, dont l'accord de la BDL. Cela est le résultat de la récente promulgation de la loi 81/2018 sur les transactions électroniques et les données personnelles, qui réglemente les paiements électroniques et les transferts d'argent, les cartes bancaires et les chèques électroniques.

Encore, une modification nouvelle de la circulaire 69 - Circulaire intermédiaire 588 – daté 21 Juin 2021, a permis à tous les libanais d'accéder à la porte-monnaie électronique, même les libanais qui ne détiennent pas de compte bancaire. Cette porte-monnaie électronique vise à stocker de l'argent sur un support électronique comme la puce d'un téléphone portable, ou à distance sur un serveur à l'aide d'un compte en ligne et par suite d'effectuer des opérations sans passer par un compte bancaire. (Electronic wallet)

Cette révision autorise les titulaires de porte-monnaie électronique, en plus de la réalisation de opérations électroniques via leur compte ou une carte bancaire, à les alimenter ou à exécuté des retraits d'espèces, par le réseau physique d'une société partenaire comme la banque ou l'institution de transfert d'argent.

Ces portefeuilles peuvent être libellés en livres libanaises ou en devises étrangères.

Notons que les portefeuilles électroniques étaient déjà autorisés pour les titulaires de comptes bancaires depuis janvier 2020, suite à l'adoption de la circulaire intermédiaire 539 précitée.

Enfin, la plus récente modification de la circulaire 69 est la circulaire intermédiaire 606, datée le 23 Décembre 2021 qui affirme que tous les virements entrants et sortants doivent contenir les coordonnées complètes de l'expéditeur et du bénéficiaire, y compris le nom complet, l'adresse complète et le numéro de compte / IBAN. En cas d'insuffisance, le transfert ne doit pas être traité. Cette circulaire avait comme but initial de combattre le blanchiment d'argent et autres crimes financiers.

Ces textes récentes, clairement insuffisantes et incomplètes, ne semble en aucun cas être conforme aux pratiques actuels en matière de digitalisation.

Après avoir décrypter la BDL circulaire 69/2000 et ses principales révisions, on abordera la loi 81/2018 qui a constitué une révolution dans le monde numérique au Liban.

P.2. Le statut législatif de la loi 81/2018 en matière électronique

Officiellement, le 10 octobre 2018, le Liban est devenu l'un des 145 pays ayant des transactions électroniques et l'un des 107 pays du monde dotés de lois sur la protection des données.[66]

En effet, la loi 81/2018 sur les transactions électroniques et données personnelles, révise la loi précédente n° 133, qui a été votée en 1999. La loi codifie les signatures électroniques et les lignes directrices pour la protection de la confidentialité des données dans les transactions électroniques, après près de (14) ans de recherches approfondies.
Surtout que le parlement Libanais fait face à d'innombrables problèmes ce qui rend la situation instable eu égard à la mise en place d'un édifice juridique nouveau.

On verra dans ce qui suit, les provisions liées aux services bancaires électroniques (A) afin d'aborder les documents et signatures électroniques. (B)

A- Les services bancaires électroniques

Aux termes de la loi 81/2018, la troisième partie intitulée les services monétaires et bancaires électroniques a stipulé dans sa première section « les paiements et transferts électroniques de fonds » que tout ordre de paiement ou de transfert électroniques est un ordre exécute partiellement ou complètement de manière électronique à travers lequel le client autorise la banque d'exécuter l'opération électronique.

[66] Tion. New Lebanese law on e-transactions and data protection. www.dentons.com/en/insights/alerts/2019/january/21/new-lebanese-law-on-etransactions-and-data-protection, date de la visite 10 Decembre 2022

Les moyens électroniques tel que mentionner ci-dessus signifient l'ensemble des moyens électroniques y inclus les moyens numériques utilisés par le client pour exécuter ou donner l'ordre pour exécuter l'opération de paiement ou de transfert électroniques de fonds liquides. (Art 41). Ces opérations doivent être conformes aux lois et régulations issues par la BDL (art 42).

Selon l'article 43, le client doit accepter les conditions relatives aux paiements et transferts électroniques par écrit et a priori. Ces conditions doivent être claires et directes et inclure les droits et obligations liés aux services bancaires électroniques.

Le moyen électronique utilisé doit être capable de transférer et bien stocker l'ordre d'exécuter le paiement ou le transfert électronique.[67]

Ces ordres doivent être donner par écrit et signer manuellement ou électroniquement sous peine de nullité.[68]

Les banques sont responsables de la non-exécution partielle ou complète des paiements ou transferts électroniques sauf dans les cas énumérés dans l'article 5. La non-exécution peut être le résultat d'une erreur, négligence, ou manque d'instructions issues par le client, ou de sa mauvaise foi, fonds insuffisants dans le compte du client pour exécuter l'opération ou dans le cas d'une force majeure hors de son contrôle.

La loi rassure que toutes ces opérations électroniques doivent êtres écrites et fournis au client à travers des relevés périodiques.

La section 2 a stipulé diverses provisions liées à la carte bancaire et la responsabilité de la banque et du titulaire de la carte. En effet, ces provisions ont insisté sur le fait que le contrat exécuté pour obtenir la carte doit être écrit.[69] La banque doit se commettre à un ensemble de conditions requises chaque fois qu'elle issue une carte bancaire. Ainsi, la banque doit

[67] Art. 45 de la loi 81/2018
[68] Art. 48 de la loi 81/2018
[69] Art. 53 de la loi 81/2018

garantir la confidentialité des informations d'identification et retenir les relevés de comptes de opérations exécutées. [70]

Aux termes de l'article 60, la monnaie électronique et numériques a été évoqué dans la section (3) et a été soumises aux même provisions évoqués à l'article 41.

En ce qui concerne le chèque électronique et numérique développé dans la section (4), la BDL aura à déterminer ce concept, l'autorité responsable de son émission, son utilisation et les technologies et systèmes qui le parrainent.[71]

B- Les documents et signatures électroniques

Le Parlement libanais a adopté cette législation sous le concept de « la législation de nécessité » qui est déjà une création absurde hautement contestée sur le plan constitutionnel.

Cette loi accorde à la BDL des pouvoirs étendus supplémentaires pour la réglementation des services bancaires et financiers électroniques. Elle définit le cadre juridique des transactions effectuées par voie électronique et réglemente le commerce électronique, les contrats électroniques, les documents électroniques et les signatures numériques.

Une signature électronique est un mot général qui fait référence à tout type de signature stockée sous forme numérique. Selon les lois de l'Union européenne (UE) sur les signatures électroniques (eIDAS) - Electronic identification and trust services for electronic transactions in the internal market - une signature électronique est une « donnée sous forme électronique qui est jointe à ou associée à d'autres données sous forme électronique et qui est utilisée par le signataire pour signer.[72]

L'une des réalisations les plus importantes de la loi n° 81/2018 est qu'elle reconnaît la culture d'entreprise d'aujourd'hui, dans laquelle les communications électroniques sont d'une importance majeure.

[70] Art. 54 de la loi 81/2018
[71] Art. 62 de la loi 81/2018
[72] eIDAS regulation EU N. 910/1014

La principale contribution de la loi à cet égard est une tentative de mettre sur le même étage les signatures électroniques et documents électroniques avec les signatures sur papier et documents.

Il est important de noter que les écrits et les signatures ont été définis pour la première fois dans la loi 81/2018.

En ce qui concerne la légitimité des licences d'authentification électronique, par exemple, un décret d'application est requis (utilisé dans la procédure d'authentification des signatures électroniques). Sans aucune mise en œuvre d'un décret émis par le gouvernement libanais, les critères et la procédure détaillée pour authentifier les signatures numériques restera largement vague.

En addition, à moins que le prestataire de services de vérification (également définis comme prestataires de services de certification ou CSP) est autorisé par le Conseil libanais d'accréditation (COLIBAC), qui n'a pas encore identifié les conditions préalables à une telle accréditation, les tribunaux dans ce scénario auront un pouvoir discrétionnaire d'évaluer la fiabilité de tous les documents électroniques et signatures électroniques associées. [73]

Il convient de noter qu'avant la mise en œuvre de la législation, les communications électroniques au Liban ne pouvaient être utilisées qu'à titre de preuve préliminaire. Ceci représentait un défi commercial important. Nous verrons ainsi dans la prochaine partie la validité juridique des documents et signatures électroniques

L'écrit est valide quel que soit le format en place et le canal par lequel les données sont transférées, qui peuvent également être papier ou électroniques, tandis que la signature exige des conditions spécifiques pour acquérir des effets juridiques.

Ainsi, la principale réalisation de la loi est l'assimilation des signatures électroniques et papiers avec signatures et documents papier. En effet, conformément à l'article (4) de la loi

[73] Tion. New Lebanese law on e-transactions and data protection. www.dentons.com/en/insights/alerts/2019/january/21/new-lebanese-law-on-etransactions-and-data-protection

81/20018, « Écrits et signatures électroniques doivent avoir le même effet juridique que les écrits et les signatures apposées sur papier ou sur tout autre moyen » si les deux conditions suivantes sont remplies: la personne qui crée les documents peut être identifiée ; et que les documents sont classés et conservés de manière sécurisée.

A défaut, si l'écrit électronique ne remplit pas les conditions précitées, il sera traité comme une preuve circonstancielle qui pèse moins que la preuve directe car il manque authentification.

De même, l'article (7) vise un impact juridique spécifique et important qui est la validité de la preuve des documents et des signatures électroniques, qui doit être reconnu comme légitime et fiable a l'instar de la validité de la preuve des documents écrits pourvu que les 2 conditions mentionnées ci-dessus sont remplies.

En vertu de l'article (10) de la loi précitée, l'exigence d'avoir plusieurs copies tel que mentionné dans l'article 152 de la loi de procédure civile pour les documents papier s'applique toujours aux documents électroniques. Tant que le document est organisé conformément aux exigences légales de fiabilité, et que chaque partie a accès à une copie de ce document, la règle des copies multiples est considérée comme remplie.[74.]

La rubrique suivante mettra l'accent sur l'approche timide du législateur quant à la rédaction des législations relative au monde digital.

Section 2 : Les fragilités et menaces dans le cadre juridique libanais

Le positionnement du Liban dans l'économie digitale est malheureusement pas stable et manque un effort collectif de tous les acteurs responsables. Ce défi était à la base d'innombrables menaces et tensions. Voulons-nous demeurez juste des spectateurs face à cette croissance du digital ou bien donner la chance à l'économie et les banques

[74] COVID-19 and Electronic Signatures in Lebanon. Tohme Law Firm. www.tohmelaw.com/news/covid-19-and-electronic-signatures-lebanon

spécifiquement pour relever ces menaces et créer un pilier exceptionnel de transformation de la technologie que les banques ont clairement besoin?

Pour essayer de trouver des réponses à nos questions, nous allons étudier dans un (P.1) l'approche libanaise encore timide vis-à-vis du digital, pour passer dans un (P.2) aux menaces accentuées liées à l'adoption des services électroniques par les banques digitales.

P.1 Une approche encore timide en droit Libanais

La structure réglementaire au Liban en matière électronique que ce soit les innombrables circulaires de la BDL ou la loi 81/2018, soulève multiples questions car elle n'aborde pas l'origine du problème spécifiquement les retards exceptionnels dans les réformes surtout que les règlements d'application de la loi 81/2018 n'ont pas encore été publiés.

De ce fait, on développera le besoin de renforcement des législations en matière digitale : La France comme exemple (A) mais aussi la faillite au niveau de l'implémentation de la loi 81/2018 (B).

A. Le besoin de renforcement des législations en matière digitale: La France comme exemple

Il est incontournable que le Liban est très en retard en matière de technologies numérique. En ce sens un renforcement des aptitudes et des lois en matière d'exploitation du digital est primordial. Les changements technologiques avérés très rapide ont permis à nombreux pays de se transformer et de s'accroître.

En ce sens, la France a issu une loi appelé loi Macron sur la mobilité bancaire, entrée en vigueur le 6 Février 2017.

Selon l'association de défense des consommateurs, seulement 2,5% des consommateurs ont changé d'établissement bancaire en 2019 alors que près d'un sur cinq (17%) en exprime le souhait.

Cette loi vise à aider les clients lors du changement d'une banque à une autre. Ce qui fait que les banques sont les seuls responsables de toutes les procédures administratives lors de ce changement suite à un accord écrit avec la nouvelle banque.

Ce service s'applique uniquement aux comptes courant et s'adresse aux particuliers, ainsi, les sociétés, associations et professionnels sont exclus de ce privilège.[75]

Cette procédure est gratuite et simplifie la démarche fastidieuse du changement d'adresse.

Avec l'augmentation des frais bancaires, beaucoup de personne se sont dirigés vers les néo banques dû à leur transparence en terme de frais. Ainsi, l'aide à la mobilité bancaire a permis une simple transition d'une banque traditionnelle à une banque sans banque.

Suite à la signature du client sur le mandat de mobilité bancaire, la nouvelle banque va s'occuper de toute la démarche. Elle doit informer son client gratuitement à l'aide d'un guide détaillé sur la mobilité bancaire et lui fournir gratuitement un document détaillant les transactions bancaires exécutées sur son compte durant les (13) dernières années. [76]

Après la signature du mandat de mobilité, la banque d'arrivée contacte la banque de départ et demande le transfert de la liste des mandats de prélèvements valides et des virements récurrents réalisés au cours des 13 derniers mois, de même que la liste des chèques non débités sur les chéquiers utilisés durant la même période.

Après avoir reçue les informations demandés, la banque d'arrivée notifie dans les 5 jours ouvrés, les nouvelles coordonnées bancaires aux émetteurs de virements et prélèvements qui ont 10 jours ouvrés pour confirmer ce changement à leur client.[77]

[75] L'aide à la mobilité bancaire, www.economie.gouv.fr
[76] Frederic Masard, Mobilité bancaire : le dispositif d'aide au changement de banque - https://www.moneyvox.fr/tarif-bancaire/mobilite-bancaire.php
[77] Frederic Masard, Mobilité bancaire : le dispositif d'aide au changement de banque - https://www.moneyvox.fr/tarif-bancaire/mobilite-bancaire.php

Cette transformation digitale de la relation entre la banque et son client a connu un grand essor. En effet l'arrivée du numérique dans la relation du client avec sa banque bénéficie les deux acteurs réduisant et même supprimant la charge du « papier » entre les deux.

La question qui se pose maintenant est quelles sont les lacunes au niveau des règlementations libanaises en matière électronique et pour quelles raisons le législateur libanais a échoué à implémenter ces règlementations.

B. La faillite au niveau de l'implémentation des règlements libanais

Les procédures corrompues et obsolètes sont l'obstacle numéro 1 lorsqu'il s'agit des législations ne servant pas leurs objectifs ou n'étant pas autorégulatrices.

L'un des premiers défis de l'application de la loi est celui du traitement des documents électroniques. Ces derniers n'auront aucune valeur juridique à moins qu'ils soient réglementés par un décret gouvernemental proposé par le ministre de la Justice. Le décret servira pour couvrir les processus et assurances spécifiques liés aux documents ainsi que leur applicabilité.

Aussi, il convient de noter que certaines transactions relatives au droit des personnes (mariage, divorce…), doivent être exclus des transactions électroniques en général; c'est notamment le cas de la loi fédérale de l'UAE n°1/2006 relative aux transactions électroniques et au commerce. En revanche, la loi libanaise, ne fait aucune exception à cet égard.

En ce qui concerne l'exécution large de la loi, cette dernière est en vigueur depuis Janvier 2019 (3 mois à compter de sa publication au journal officiel).

En effet, au terme de l'article 135, la loi précise que modalités d'application de la présente loi seront définies, le cas échéant, par décrets pris en Conseil des ministres sur proposition du ministre de la justice, du ministre de l'économie et du commerce, du ministre des finances, le ministre de l'Industrie et le ministre des Télécommunications, chacun selon ses pouvoirs.

Toutefois, l'article 64 de la loi, qui permet à la BDL de délivrer des mesures de vérification des signatures électroniques liées aux paiements électroniques, reste une exception au principe.

Malheureusement l'autonomie de la BDL dans la règlementation et le contrôle du secteur bancaire explique la raison pour laquelle le secteur bancaire est très en retard, notamment en matière de commerce électronique.

Ainsi, étant donné qu'aucun décret d'application de la loi susmentionnée n'a été publié, les ministres concernés qui existent depuis sa promulgation continuent à ajourner la mise en œuvre des règlements relatives aux transactions électroniques et à la protection des données.[78]

Au sens de l'article 1 de la loi, afin de prouver que la signature électronique répond aux exigences de fiabilité nécessaires, le fournisseur de services d'authentification est censé être un juriste public ou privé qui proclame les certificats d'authentification à la suite de la mise en œuvre des procédures de protection qui garantissent les fonctions spécifiées dans l'article 15 de la présente loi ou l'un d'eux.

Au sens de l'article 25, lorsqu'un fournisseur d'authentification est utilisé, le système peut vérifier si un utilisateur individuel est autorisé ou non à accéder au système de même que les groupes ou les rôles qui leur ont été attribués.

Ainsi, conformément à l'article 16, le fournisseur de services d'authentification n'est pas obligé, mais peut, sur demande, obtenir une certificat d'accréditation délivré par le Conseil Libanais d'Accréditation (COLIBAC) et devenir un prestataire de services d'authentification accrédité.

On se demande si cela signifie que le prestataire de services d'authentification doit nécessairement être certifié pour que la signature soit fiable. En d'autres termes, est ce que

[78]COVID-19 and Electronic Signatures in Lebanon. Tohme Law Firm. www.tohmelaw.com/news/covid-19-and-electronic-signatures-lebanon

cela signifie que si le fournisseur de service d'authentification n'est pas certifié, la signature ne demeure plus fiable?

D'un autre côté, l'article 15 de la loi stipule que les moyens de protection appliqués aux écrits et signatures électroniques sont conçues pour améliorer leur fiabilité.

Le rôle des outils de protection est de vérifier l'identité de l'émetteur de l'obligation et/ou assurer l'intégrité des provisions inclus. Ces fonctions sont sécurisées par un fournisseur de service d'authentification, qui, après être titulaire d'un certificat d'authentification, garantit la fiabilité de la signature électronique.

En effet, l'article 21 de la loi dispose que la COLIBAC établit une liste des conditions techniques que les prestataires doivent respecter pour obtenir l'accréditation, et cette liste de conditions précise les éléments nécessaires pour bien compléter les procédures d'évaluation technique, notamment les conditions administratives, techniques et financiers joint au dossier de demande d'agrément, sous réserve que COLIBAC tienne compte des normes internationales adoptées dans les mêmes domaines.

Cela est impossible, à moins que l'objet de cet article 21 ne soit d'étendre la fonction du

COLIBAC au-delà de ce qui est autorisé par sa loi n° 572/2004, à ce titre un élargissement des fonctions du COLIBAC change la nature de son travail et nécessite donc une modification complète de la loi susmentionnée. La contradiction juridique est que la loi No. 81/2018 élargit le rôle et l'autonomie du COLIBAC en lui donnant des rôles qui n'étaient pas offerte par la loi COLIBAC originelle. Par conséquent, une modification de la loi est inévitable à ce point.

Il est inévitable que la loi instituant le conseil libanais pour l'accréditation du COLIBAC a été rédigée parallèlement aux débuts du projet ECOMLEB en 2004, date à laquelle le législateur ne doutait pas que COLIBAC serait bientôt actif et assumerait ses fonctions.

L'article 8 de la loi n° 572/2004 a établi un délai maximum de quatre mois après la date de son entrée en vigueur pour l'adoption des décrets fixant le règlement du conseil. Cependant,

la réglementation du seul organisme national d'accréditation au Liban n'a été révélé qu'en 2010.

A ce jour, le COLIBAC est une entité inactive et non fonctionnelle du fait de l'absence d'un directeur et d'un personnel nommé et ne peut donc pas jouer le rôle qui lui est dévolu à l'instar des autres organismes d'accréditation du monde entier.

Il n'est donc pas en mesure d'exercer ses fonctions en matière d'évaluation de la conformité, tel que stipulé dans la loi.

Notant que l'accréditation au Liban est actuellement fournie par des organismes d'accréditation qui signent les accords internationaux liés à des sujets d'accréditation, qui fournissent une solution pratique acceptable pour l'évaluation des conformités par des organismes agréés à l'étranger.

De plus, conformément à l'article 12 de la loi n° 572/2004, les organismes opérant au Liban peuvent continuer leur travail temporairement aussi longtemps que le COLIBAC est suspendu, à condition qu'ils déposent leurs dossiers complets au plus tard dans les trois mois à compter de la date de la déclaration du COLIBAC pour l'exercice de ses fonctions. Le COLIBAC peut être attribuée à toute autre partie nationale ou étrangère.

En conclusion, depuis 2004 jusqu'à nos jours, le COLIBAC n'existe pas et n'a fait l'objet d'aucune tentative ultérieure de l'activer, et l'affaire reste la même à ce jour.

Mais on se demande, comme le projet de loi 81/2018 a fait l'objet d'un débat et d'une discussion très longue au parlement avant son adoption, pourquoi va-t-il pas été modifié pour se conformer au fait qu'il n'y avait pas de conseil d'adoption efficace? Les législateurs ignoraient-ils le contenu de la loi n° 572/2004, ou n'étaient-ils pas familiarisés avec le sujet des signatures électroniques et ses conditions ?

Ces questions légitimes nous ouvrent un autre sujet épineux concernant la façon par laquelle les législations sont votées au Liban et nous poussent à s'interroger sur

l'expérience, la compétence et la réelle familiarité des personnes qui participent à la prise de décision.[79]

La loi sur les transactions électroniques et les données personnelles a constitué une base pour légitimer les services électroniques offertes par les banques, cependant les menaces liées à l'adoption de ces services doivent être prise en compte vu qu'ils rendent potentiellement les banques digitales vulnérables.

P.2 Les menaces liées à l'adoption des services électroniques par les banques digitales

L'adoption des services électroniques dans les banques digitales est naturellement accompagnée de multiples défis et enjeux au niveau de l'implémentation de cette politique de transformation numérique. Ces défis se sont manifestés dans (2) importantes domaines : Juridique (A) et informatique (B).

A. Les défis juridiques

En France, Selon « Accenture », 43% des clients considèrent la protection des données comme le facteur primordial de leur fidélité à une banque.

De nombreuses questions juridiques se posent d'ores et déjà : quels sont les défis légaux que la banque doit prendre en considération pour orienter sa stratégie digitale ?

Il est incontournable qu'il manque un encadrement juridique fort qui règlemente et sécurise la banque digitale au Liban. En effet, Les services digitaux offerts par les banques posent de majeures questions juridiques. Par exemple, dans le système du cloud computing, la problématique juridique se traduit par le fait que la banque confie ses données et les données de ses clients à un prestataire externe. La crainte que la banque perd la maîtrise sur ses propres données se pose ainsi.

[79] Law 81/2018. Digital Commons, 5 July 2020
BAU.digitalcommons.bau.edu.lb/lsjournal/vol2020/iss2020/7/

La protection des données n’est pas un phénomène nouveau mais elle s’est considérablement accélérée sous la pression de la digitalisation et le développement incroyable des services bancaires numériques.

Dans un environnement conçu comme sensible à la protection des données des clients, le défi juridique consiste donc à pouvoir trouver un encadrement légal contractuel dans le but de protéger ce traitement externe des données et pouvoir le contrôler pour garantir la sécurité et la fiabilité des informations échangés.[80]

Ainsi, la digitalisation de la relation client a conduit à une croissance rapide des données clientèle disponibles.

Dans cette approche, on se songe bien sûr à la loi 81/2018, cet encadrement juridique est assez ambigu quant à ce qui constitue une cause légitime pour l'acquisition des données. Au lieu de cela, il se concentre sur la présentation d'une large liste d'organisations qui sont exclus de l'obligation d'obtenir une autorisation pour collecter et traiter des données à caractère personnel[81.] Ce manque de spécificité rend très facile pour le ministère de l'Économie et Le commerce d’accorder des permis aux organisations qu'il favorise tout en rejetant les demandes de ceux qui ne sont pas dans les bonnes grâces du parti au pouvoir.

Fruit d’ajout successif, il est sûr de supposer que le ministère de l'Économie et du Commerce manque des ressources nécessaires (personnel qualifié avec suffisamment d’experience) pour s'assurer que tous les aspects de la gestion des données couverts par les transactions électroniques font l'objet d'un contrôle efficace. Même si des personnes allèguent des abus, leurs demandes seront traitées avec des retards importants, empêchant les citoyens de préserver leurs données personnelles à temps.

A cette aune, il aurait été bien préférable d'avoir une plus grande séparation des pouvoirs entre les départements exécutifs et administratifs dans le but de former un organisme distinct et indépendant de contrôle du traitement des données personnelles.

[80] Jürg Schneider, Digitalisation, les nouveaux défis juridiques, smart media, Walderwyss avocats, 2019
[81] Aricle 94 de la loi 81/2018

La loi libanaise sur les transactions électroniques ne protège pas non plus de manière adéquate le droit à la réparation et à la modification de tout aspect des données recueillies. Les particuliers ont le droit de demander des modifications à des données trompeuses, inexactes ou incomplètes. Cependant, il n'est pas clair si ce droit s'applique pendant la durée de gestion des données personnelles.

Les personnes ordinaires, pour exemple, ne peuvent s'opposer à la collecte et au traitement des données que s'ils n'ont pas préalablement accepté le traitement en vertu de l'art. 101.

En outre, au terme de l'article 102, la loi stipule que si une personne notifie au responsable des données son désir d'avoir ses données supprimées et que le responsable des données ne prend pas de mesures efficaces, la personne doit déposer une plainte auprès du magistrat de la justice sommaire rendant l'exercice du droit de recours et de rectification extrêmement coûteux et difficile pour les citoyens libanais.

Toutefois, si une seule personne est accusée de nuire à l'intérêt public ou au bien commun du pays, il est permis d'accéder aux données du téléphone portable du suspect. Par conséquent, les données personnelles sont accessibles selon une seule règle, qui est celle du pays et l'intérêt supérieur du public. Les intérêts supérieurs du public comprennent le fait d'infliger des dommages au pays dans son ensemble ou étant lié à des attentats terroristes.

Enfin, la loi comporte un article qui fait référence au droit d'être protéger contre les décisions effectuées à l'aide de traitements automatisés ayant des conséquences juridiques ou administratives. Cependant, la loi mentionne seulement que les individus ont le droit d'examiner et d'objecter, et il ne fait aucune mention de la responsabilité du responsable des données de fournir aux individus une l'explication de la décision et un moyen efficace de la contester.[82]

Ainsi s'avère la nécessite inévitable de renouveler les contrats entre client-banque et client-fournisseur pour les adapter à cette loi, ainsi que d'adopter les notices et règlements de confidentialité sur leur site web tel qu'exigé par les lois internationales.

[82] Article 86 de la Loi 81/2018

Cependant, le défi juridique n'est pas le seul acteur sur la scène numérique, un autre défi énormément sérieux s'ajoute à lui qui est le défis informatique ou risque cyber.

B. Les défis informatique ou risques cyber

Le nerf de la guerre : la data[83]

Avec l'évolution des technologies, les nouveaux services bancaires offerts par les banques digitales se sont explosées engendrant des risques de sécurité.

La transformation digitale a considérablement augmenté l'exposition de la banque digitale au risque cyber et par suite leur vulnérabilité a ce risque. A son tour, la crise sanitaire a sensiblement augmentée cette exposition au risque.

Ce déplacement vers le digital a entraîné avec lui une migration des enjeux sécuritaire à un autre niveau. Ainsi, les acteurs du secteur digital devraient s'adapter eux aussi a ce contexte changeant et mettre en place des dispositions pour protéger et sensibiliser leur clientèle aux pratiques sophistiques de la sécurité numérique pour garantir la sécurité des interactions bancaire en ligne.[84]

Une autre question importante est de savoir comment garantir la sécurité des écrits et signatures électroniques, ce qui est une nécessité légale pour leur validité.

Comme indiqué précédemment, l'une des exigences qui permettront aux documents et aux signatures électroniques d'obtenir les mêmes effets que leurs homologues papier est leur organisation et leur stockage dans une façon qui assure leur sécurité.

L'article 5 de la loi précitée définit le « stockage de données électroniques » comme « l'enregistrement de données sur un support de stockage d'une manière qui garantit que les données sont accessibles à tout moment permettant de copier ou d'extraire le contenu »,

[83] PWC, Banques: une transition digitale longue, couteuse et douloureuse? https://www.pwc.fr/fr/decryptages/securite/banques-une-transition-digitale-longue-couteuse-et-douloureuse.html
[84] Benoit grangé, Cybersecurity : les banques face au défi de la protection de leur clientèle ZD NET, 30 Septembre 2021

Mais la loi 81 ne semble pas être clair sur l'obligation d'assurer la sécurité des documents et signatures électroniques.

En réalité, dans le commerce électronique, la sécurité est cruciale, c'est pourquoi les transactions électroniques doivent être contrôlées dans toutes leurs spécificités et technicités ; En ce sens, la sécurité engendre l'intégrité, et l'intégrité engendre la fiabilité. Ce concept se reflète dans l'article 15 de la loi, qui stipule que « les mesures protectives sont appliquées dans les écrits et les signatures électroniques pour les rendre plus crédibles. »

Les mesures de sécurité faciliteront une variété de tâches, y compris la vérification de l'identité de l'organisateur du document, à condition que le document porte une date valide et/ou en assurant l'intégrité de l'archivage et du contenu d'une manière qui empêche la modification de son contenu.

Conformément à l'article 9, si une signature électronique est délivrée et certifiée via une procédure menée par un fournisseur de services d'authentification, la loi établit une "présomption de crédibilité". Ce n'est que dans cette situation, sauf indication contraire, que l'on suppose que le signataire est identifiable et que la signature est conforme à la procédure légale en cours.

En ce sens, il est important de mentionner que l'utilisation d'un ou plusieurs fournisseurs de services d'authentification (appelé aussi Certification Service Provider ou CSP) est l'une des nombreuses méthodes utilisées par la législation pour garantir la sécurité des signatures et des écrits. Ainsi, selon l'article 15, ces fournisseurs de services d'authentification émettront un certificat d'authentification à la personne concernée.

Enfin, conformément au chapitre IV de la loi, le Conseil libanais d'accréditation (COLIBAC) fixera les exigences de l'accréditation du CSP, un décret gouvernemental sera nécessaire pour mettre en œuvre les reconnaissances des licences d'authentification électronique.

En raison de l'absence d'un tel décret et de l'impossibilité pour COLIBAC d'assurer ses missions, y compris la définition des normes d'accréditation, la mise en œuvre de la loi est

malheureusement impossible. Ainsi, jusqu'à l'approbation des CSP par le COLIBAC, la présomption de l'article 9 concernant la fiabilité a été désactivée.

Pour finir sur ce sujet, l'article 18 de la loi énonce qu'à moins que les parties n'en conviennent autrement, les juges jouissent d'un pouvoir discrétionnaire pour évaluer la force de la preuve d'une signature électronique ou d'un écrit dans le cas où le fournisseur de services d'authentification n'est pas accrédité.

Titre 2 : Les droits liées à l'utilisation des services de la banque digitale

Les opérations digitales effectuées par la clientèle impose une obligation sur la banque vis à vis ses clients, d'où l'existence de nombreux droits dont jouit ce dernier. Nous développerons ces droits dans 2 chapitres comme suit, les droites liés à la confidentialité et à la sécurité de la clientèle (Chapitre 1) et les droits liés à la protection des données personnelles (Chapitre 2).

Chapitre 1 : Les droits liés aux principes de protection de la clientèle

La clientèle de la banque est la raison de son existence. La banque doit faire de son mieux pour gagner sa confiance et la maintenir tout au long de la journée commerciale. Cette dernière était la préoccupation constante des régulateurs depuis des décennies. Ainsi, la banque doit mettre en œuvre un système de protection efficace qui assure la légitimité des activités bancaires.

Nous présenterons dans ce chapitre la protection juridique au niveau international (section 1) ainsi que la protection juridique au niveau national (section 2).

Section 1 : La protection juridique au niveau international

Dans le monde juridique, la protection de la clientèle au niveau internationale est divisée entre le cadre règlementaire internationale (P.1) et les directives émises par les organisations compétentes (P. 2).

P.1 : Le cadre règlementaire international

Les déclarations et accords internationaux et régionaux (A) et les directives émises par des organisations compétentes (B) constituent le cadre réglementaire international de la protection juridique de la clientèle. Nous évoquerons dans ce qui précède l'importance de

cet encadrement dans une telle relation commerciale pour protéger le client des conséquences très dommageables en cas de non-conformité.

A. Déclarations et accords internationaux et régionaux

La Déclaration universelle des droits de l'homme étant un document historique dans le domaine de la définition des droits fondamentaux a stipulé le droit à la vie privée notamment dans l'article 12: « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

De même, l'article 17 du Pacte international relatif aux droits civils et politiques est venue affirmé l'article 12 ci-dessus.

Quant aux importants textes juridiques qui ont constitué les initiatives positives les plus marquantes en matière d'établissement de la protection de la confidentialité au niveau international, ces derniers sont inscrits dans le cadre d'accords internationaux à caractère régional, caractérisés par le fait d'être contraignante et par suite lient les États membres qui sont tenus de respecter les règles qu'ils contiennent.

Ces textes comprennent le texte de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales daté de 1950[85] intitulé « Le droit au respect de la vie privée et familiale ». Cet article stipule dans son premier alinéa « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Cependant l'alinéa (2) habilite l'autorité publique sous certaines conditions - par exception au principe de confidentialité - de s'ingérer dans l'exercice de ce droit. De ces conditions, on nomme le fait que la loi prévoie expressément l'intervention, et que l'intervention est nécessaire pour l'une des raisons suivantes : préserver la sécurité de la patrie, maintenir la sécurité publique, préserver la prospérité économique du pays,

[85] Traité international pour la protection des droits de l'homme sur le continent européen, entré en vigueur le 3 septembre 1953.

maintenir le bien-être économique du pays, et enfin et surtout, protéger les droits d'autrui et leurs libertés.

Aussi, l'article 11 de la Convention américaine relative aux droits de l'homme de 1969, sous le titre « La protection de l'honneur et de la dignité de la personne » a stipulé dans son alinéa (2) que « Nul ne peut être l'objet d'ingérences arbitraires ou abusives dans sa vie privée, dans la vie de sa famille, dans son domicile ou sa correspondance, ni d'attaques illégales à son honneur et à sa réputation. »

La Charte des droits fondamentaux de l'Union européenne 2000[86] a sacrifié ce droit dans un article (7): « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

Dans les pays arabes, nous constatons que ce droit a été consacrée comme résultat des efforts régionaux dans le domaine des garanties des droits de l'homme dans tels pays, représentés par la Charte arabe des droits de l'homme adoptée par le Conseil de la Ligue arabe en septembre 1994 qui stipule en son article 6 que : « La vie privée a un caractère sacré, sa violation est un crime. Une telle vie comprend l'intimité de la famille, le caractère sacré du foyer, la confidentialité de la correspondance et d'autres moyens de communication.

Notant que la charte précitée a défini une version plus récente de son contenu, qui est approuvée par le seizième sommet arabe, accueilli par la Tunisie le 23 mai 2004.

La charte a mentionné dans sa nouvelle version un texte qui restitue le contenu des articles (12) de la Déclaration universelle des droits de l'homme et (17) du Pacte international relatif aux droits civils et politiques susmentionné.
Il est à noter que toutes les chartes internationales mondiales et régionales, qui consacrent les droits fondamentaux de l'homme n'ont pas clairement noté la portée du droit à la vie

[86] Charte des droits fondamentaux de l'Union européenne 2000, au nom du parlement européen, du conseil européen et de la commission européenne, le 7 Décembre 2000, Nice.

privée, ni noté la vie privée dans le domaine de L'information, qui est soumise à une violation continue de différentes manières numériques ou non numériques.

Cette richesse dans le droit a certes orienté le législateur libanais dans plusieurs domaines.

Quant aux instructions contenues dans certaines recommandations et décisions émis par d'importantes organisations internationales, ils sont venus plus détaillée à cet égard, comme nous le verrons dans la suite.

B. Décisions émises par des organismes internationaux

Au cœur des défis posés par l'ère de la technologie sur tous les niveaux, l'anxiété a augmenté chez les organisations internationales concernant l'incapacité des législations existantes à suivre le rythme très rapide des risques découlant des formes modernes de la violation des droits de l'homme.

De ce point de vue, le travail des organisations s'est récemment concentré sur la recherche de solutions qui dépassent les effets négatifs du développement technologique rapide sur les droits de l'homme, y compris le droit à la confidentialité et à la vie privée. Ainsi, les directives suivantes sont considérées comme un bouleversement qui a été adoptée par les autorités concernées à cet égard afin de remedier les lacunes et renforcer la protection.

La résolution 167/68 émise par l'Assemblée générale des Nations Unies sur le droit à la vie privée à l'ère du numérique[87] qui a affirmé principalement les principes suivants :

- La surveillance et ou interception illégale ou arbitraire des communications et la collecte de données personnelles Illégalement ou abusivement, violent le droit à la vie privée.
- Le droit au respect de la vie privée ne permet à personne de faire l'objet d'ingérences arbitraires ou illégales dans sa vie privée, ses affaires familiales, son environnement ou ses correspondances, et son droit de jouir de la protection de la loi contre telle

[87] Assemblée générale des Nations Unies, Résolution n° 68/167, 18 Décembre 2013, session 68, section 69 (b) https://documents-addsny.un.org/doc/UNDOC/GEN/N13/449/45/PDF/N1344945.pdf? 02/02/2020 date de la visite 17 Octobre 2022

intervention est garantie par l'article 12 de la Déclaration universelle des droits de l'homme et l'article 17 du Pacte international relatif aux Droits civils et politiques.

- Les droits hors internet dont disposent les personnes doivent également être protégés sur internet, y inclut le droit à la vie privée.

En conséquence, l'Assemblée générale a appelé tous les États à respecter et protéger le droit à la vie privée et prendre les mesures nécessaires pour limiter ou prévenir les atteintes à celle-ci.

Le rapport du Haut-Commissaire au Conseil des droits de l'homme pour l'année 2014[88], émis dans la perspective de trouver un cadre légal et efficace pour promouvoir et protéger le droit à la vie privée à la lumière du développement technologique. Ce rapport a constaté que l'ingérence illégale ou arbitraire dans la vie privée des personnes constitue une violation manifeste de la vie privée.

Ainsi, nous constatons que le rapport et la résolution ci-dessus n'ont pas donné une définition claire de ce que constitue une ingérence légale ou légitime dans le droit à la vie privée, et il ne fait aucun doute que l'ingérence arbitraire et illicite est une violation des dispositions des conventions et pactes internationaux applicables qui respecte le droit à la vie privée comme nous l'avons vu, ce qui signifie qu'un État ne peut, selon les dispositions du droit international général, adopter une législation nationale contraire aux textes précités de sorte que leur contenu constitue une violation au droit à la vie privée, sans intérêts particuliers ou publics, justifiant une telle « atteinte » par une disposition de la loi.

P.2. Directives émises par les organisations compétentes

En matière de confidentialité et de sécurité, plusieurs autorités compétentes ont émis de bonnes pratiques dans le domaine de la protection de la clientèle. Ces mesures bien encadrées devaient être respecter sous peine de sanctions graves. On nommera les décisions diffusées par la Commission Nationale de l'Informatique et des Libertés (CNIL) (A) et les

[88] Conseil des droits de l'homme - Rapport du Haut-Commissaire sur "Le droit à la vie privée à l'ère numérique", session 27, 30 Juin 2014, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session date de la visite 17 Octobre 2022.

règlementations diffusées par L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

A. Décisions diffusées par la commission nationale de l'informatique et des libertés (CNIL)

Trente ans se sont découlées depuis la sortie en vigueur de la nouvelle rédaction de la CNIL, le 1er juin 2019.
Créée en 1978 par la loi Informatique et Libertés n° 78-17, la CNIL est une autorité administrative indépendante, composée d'un Collège de 18 membres et d'une équipe d'agents contractuels de l'État. 12 des 18 membres sont élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent.

Les fonctions de La Commission Nationale de L'Informatique et des Libertés ont été révisées par le règlement 2016/679 daté le 27 Avril 2016 sur la protection des données. Grâce à ces nouvelles missions introduites, La CNIL a réussi a contribué a assurer la protection des données en France dans le cadre du respect des normes européennes. On peut ainsi déduire que la CNIL possède le pouvoir de contrôler et de sanctionner les organismes qui traitent les données personnelles.

Dans un univers numérique, Le primordial principe de la loi informatique et liberté est la sécurité et la confidentialité. Ainsi les données personnelles doivent garantir ces (2) droits et amélioré la sécurité juridique aux personnes et organismes concernées garantis par les textes juridiques. On déduit que la CNIL analyse rigoureusement le respect des obligations en matière de sécurité et de confidentialité.
Durant les dernières années, la CNIL a publié de nombreuses décisions soit des lignes directrices ou référentiels, soit des sanctions et des mises en demeure.

Dans le but d'apporter une énorme confiance dans le monde numérique, la Commission estime essentiel de définir des modalités techniques de cette méthode d'authentification afin de garantir la sécurité des informations. Dans cette perspective, la CNIL a adopté une

recommandation ayant pour but définir les exigences techniques et organisationnelles minimales pour les authentifications par mot de passe ou par tout autre secret non partagé

La CNIL a déposé une recommandation en 2017 pour garantir un niveau de sécurité minimale dans le domaine de l'authentification par mot de passe. Cette recommandation a permis aux professionnels et aux particuliers de bénéficier de mesures constituant le niveau minimal applicable en matière de pratiques de sécurité.

Aussi, la délibération n° 2022-100 du 21 juillet 2022 est née portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés. Cette délibération est très célèbre dans le champ des recommandations générales en matière de sécurité des mots de de passe. Elle stipule les principales modalités opérationnelles de l'utilisation de mots de passe et inclut les modalités de conservation des mots de passe, les modalités de changement du mot de passe et d'information des personnes ainsi que les modalités de l'authentification par mot de passe.[89]

D'après une étude de Verizon de 2021, 81 % des notifications de violations de données mondiales sont liées aux problèmes de mots de passe. En France, environ 60 % des notifications reçues par la CNIL depuis le début de l'année 2021 sont liées au piratage et un grand nombre aurait pu être évité par le respect de bonnes pratiques en matière de mots de passe.[90]

En outre la CNIL a publié multiples décisions en matière de santé comme dans le but d'apporter une énorme confiance dans le monde numérique, la Commission estime essentiel de définir des modalités techniques de cette méthode d'authentification afin de garantir un la sécurité des informations. Dans cette perspective, la CNIL à adopter une recommandation ayant pour but définir les exigences techniques et organisationnelles

[89] Legifrance, Délibération 2022-100 du 21 juillet 2022 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046437451?isAdvancedResult=&page=3&pageSize=10&query=*&searchField=ALL&searchProximity=&searchType=ALL&sortValue=DATE_DECISION_DESC&tab_selection=cnil&timeInterval=&typePagination=DEFAULT

[90] Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité,17 Octobre 2022, https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

minimales pour les authentifications par mot de passe ou par tout autre secret non partagé.[91]

La politique de sanction de la CNIL s'illustre classiquement par sa démarche pédagogique, poussant à la mise en conformité. En 2018, alors que la CNIL recensait 11 077 plaintes et 310 contrôles, ceux-ci se sont soldés par 48 mises en demeure et seulement 9 sanctions pécuniaires.[92]

Une autre agence aussi importe que la CNIL, s'est apparue ayant un caractère international et proclamant des règlements en matière de sécurité ; L'ANSSI.

B. Règlementations diffusées par l'agence nationale de la sécurité des systèmes d'information (ANSSI)

Sous la forme d'un service à compétence nationale, le 7 juillet 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834. Elle a remplacé la direction centrale de la sécurité des systèmes d'information (DCSSI) qui découle du secrétariat général de la défense et de la sécurité nationale.

Dans un monde où la cybercriminalité est en forte croissance et où il est très difficile d'assurer la protection des données personnelles, le principal enjeu de l'ANSSI est de protéger les particuliers en développant des actions de sensibilisation à la sécurité numérique et de formation adaptées aux usages de la clientèle.

Avec la transformation digitale des différents acteurs de la société et l'accroissement de leur connexion, la gestion des risques numériques liés à la protection des données personnelles a tellement évolué au sein des entreprises. Ainsi, l'ANSSI tient à assurer l'exécution des règlementations en matière de sécurité. Ce dernier, avec le développement rapide économique et technologique pèse lourdement sur l'activité des organisations.

[91] Legifrance - Décision n°DR-2022-142 du 14 juin 2022

[92] Roche David, Bencheliha Farah, Atteinte à la sécurité des données clients : propos sur l'évolution de la procédure de sanction de la CNIL, 1 Avril 2020 https://droit-des-affaires.efe.fr/2020/04/01/atteinte-a-la-securite-des-donnees-clients-propos-sur-levolution-de-la-procedure-de-sanction-de-la-cnil/, date de visite 18 October 2022.

En ce sens, l'ANSSI a rédigé un guide concernant les recommandations pour la protection des systèmes d'information essentiels, daté du 18 Décembre 2020.
Ce guide s'adresse aux opérateurs de services essentiels et aux fournisseurs de services numérique, ainsi que toute entité visant à protéger ses systèmes informatiques.
Bref ce guide constitue un ouvrage de bonnes pratiques en matière de sécurité qui propose des recommandations lie à des mesures de sécurité et propose des solutions dans le même domaine.
Le cadre règlementaire sur lequel se base ce guide est constitué de divers lois, arrêtés et règlements.
On nomme dans ce sens la loi n. 133/2018 du 26 Février 2018 relatives aux règles de l'union européenne dans le domaine de la sécurité, aussi l'arrêté du 14 Septembre 2018 qui détaille les règles de sécurité applicables aux entreprises et celles relative à la protection des systèmes d'information qui constitue le sujet principal de ce guide.[93]
Encore, un des principaux objectifs de l'ANSSI est de promouvoir la confiance dans les services offerts en ligne. Ainsi, l'ANSSI intervient au sein de cet environnement à travers ses règlementations dans le but de soutenir les acteurs économiques dans leur combat contre la cybercriminalité.[94]

L'ANSSI regroupe également des réglementations techniques liées à la protection du système d'information. De même, elle délivre des visas de sécurité. Ces visas permettent d'identifier les efficaces et robustes solutions de cyber sécurité suite à une évaluation effectuée par des laboratoires spécialisés et selon une méthodologie éprouvée.
En outre, L'ANSSI sensibilise ces entreprises aux bonnes pratiques de sécurité numérique et aide ces derniers dans l'implémentation des mesures de sécurité requises selon le type de chaque entreprise.

Dans ce même contexte, on note que l'ANSSI effectue de façon permanente des scans réseaux sur internet en France. Ces scans constituent un système d'alerte aux entreprises.

[93] ANSSI, Recommendations pour la protection des systemes d'information essentiels, Version 1.0, 18 Decembre 2020
[94] Voir le règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS)

Effectuer de façon récurrente ou ponctuellement, ils ont pour mission d'améliorer la sécurité de l'internet et réduire la possibilité des attaques informatiques suites aux services exposés sur internet mais aussi de contrôler les vulnérabilités du système informatique qui peut être largement affecté par ces menaces technologiques.
Après avoir exposer la protection juridique de ces droits au niveaux internationale, on verra ci-après l'application de cette protection au niveau national.

Section 2 : La protection juridique au niveau national

Le Liban est certainement doté d'un régime de protection en matière de confidentialité (P.1), ainsi qu'en matière de sécurité (P.2). Ce dispositif législatif est dans la phase de faire ses preuves. De multiples initiatives privées ainsi que publiques proposent toujours des solutions pratiques afin de protéger la clientèle de la banque.

P.1 : La protection de la confidentialité du client bancaire

Pour pouvoir bénéficier des services bancaires, le client est obligé de révéler un certain nombre de données.

Compte tenu d'un certain nombre d'atouts, la politique de confidentialité a occupé une énorme place dans les recherches des législateurs qui ont développé ce droit dans la constitution libanaise (A) ainsi que dans d'autres lois ordinaires (B).

A. La constitution libanaise

Le paragraphe (b) du préambule de la constitution libanaise stipule que le Liban est « un membre fondateur et actif de l'Organisation des Nations Unies et est engagé à ses pactes et à la Déclaration universelle des droits de l'homme. »
Le paragraphe (c) soulignait également que le Liban est une république « fondée sur le respect des libertés publiques. »
En application, les dispositions de la Constitution viennent au sommet de la hiérarchie de la législation interne de l'État, posant les droits et les libertés humaines fondamentales sur le rang le plus élevé dans la hiérarchie des lois et sont considérées comme des droits constitutionnels inviolables par toute autre disposition.

Or, le législateur libanais n'a inscrit dans la constitution aucun texte sur le droit à la vie privée, sauf pour ce qui a été stipulé dans l'article 14, qui instituait le droit au caractère sacré du domicile (1), sans aborder la propriété privée de l'individu stipulée dans les pactes internationaux approuvés (comme la confidentialité des correspondances).[95]

Ceci s'ajoute au texte de l'article (8), qui consacre légalement la liberté individuelle .[96]

On déduit que le législateur libanais n'a pas consacré le droit à la vie privée comme un droit constitutionnel.

Cependant, les lois ordinaires émises par l'autorité législative du pays et dérivées des chartes internationales que le Liban s'y est engagé explicitement en matière de protection des droits de l'homme ont contribué à déterminer l'étendue du droit à la vie privée et à la protection juridique approuvée à cet égard comme nous le verrons ci-dessous.

B. Autres lois ordinaires

Les dispositions légales relatives à la protection du droit à la vie privée ont été reçues soit dans le cadre des textes juridiques généraux (tels que le Code pénal libanais), ou dans le cadre des lois spéciales. Nous les exposons du plus ancien au plus récent en vue de noter l'évolution de la protection législative de ce droit.

1- Le Code pénal libanais de 1943

Conformément au texte de l'article 14 de la Constitution, le code pénal a sanctionné la « violation du caractère sacré du domicile ».[97] Il a également puni la « privation de liberté » en application du texte de l'article 8 de la Constitution.[98]

En plus il a criminalisé l'atteinte à la réputation et à l'identité individuelle, qui d'une manière ou d'une autre constitue une agression sur la vie privée (comme l'usurpation de l'identité [99]et le chantage[100])

---

[95] Article 14 de la constitution libanaise: "Le domicile est inviolable. Nul ne peut y pénétrer que dans les cas prévus par la loi et selon les formes prescrites par elle."

[96] Article 8 de la constitution libanaise: La liberté individuelle est garantie et protégée. Nul ne peut être arrêté ou détenu que suivant les dispositions de la loi. Aucune infraction et aucune peine ne peuvent être établies que la loi.

[97] Référer aux Aet. 571 et 572 du CPL

[98] Référer aux Art. 569 et 570 du CPL

[99] Voir art. 391, 392 et 460, 470 du CPL

[100] Voir art. 577 et 578 du CPL

Dans notre opinion, la reconnaissance par le législateur du droit à la confidentialité s'est traduite en vertu des dispositions du code pénal qui ont criminalisé les actes suivants :

- L'acte d'espionnage qui se traduit par le fait d'entrer ou de tenter d'entrer dans un lieu interdit afin d'obtenir des choses, des documents ou informations qui doivent être tenus secrets pour la sûreté de l'Etat (art. 281 et suivants du code pénal)
- Le fait de divulguer ou d'utiliser des secrets pour son propre profit ou au profit d'autrui (articles 579 à 581 inclus du code pénal.)
- Le chantage c'est le fait de menacer une personne d'exposer son affaire, de la divulguer ou d'en parler, si cette affaire affecte son destin, son honneur ou le destin et l'honneur d'un de ses proches, et vise à inciter la victime à apporter un bénéfice à l'auteur ou à d'autres (article 650 code pénal).

2- Loi du 3 Septembre 1956 sur le secret bancaire modifié par la loi 306 du 3 Novembre 2022

La loi prévoyait l'obligation légale de conserver la confidentialité des informations bancaires (transactions, correspondances…) sous le secret absolu dans l'intérêt des clients.[101] La personne qui y est exposée n'a pas le droit de divulguer ces informations (noms des clients, leur argent et d'autres questions les concernant à toute personne ou à toute autorité)

3- Loi réglementant le patrimoine administratif et financier de la Direction Générale des Postes et Télégraphes pour l'année 1959[102]

L'article 9 de ladite loi stipule que : « Le secret de la correspondance postale est inviolable et ne peut être divulgué. Dans ce sens, les articles 580 et 581 sanctionnent toute personne qui abuse de sa qualité relative au poste et télégraphe, en parcourant une lettre scellée, ou en détruisant ou en chapardant l'une des lettres ou en révélant son contenu a une personne autre que le destinataire, avec un emprisonnement de (2) mois à (2) ans. Dans le même sens, ils sanctionnent tout le monde qui détruit ou brise intentionnellement un message ou un télégramme qui ne lui a pas été envoyé, ou regarde frauduleusement un appel téléphonique avec une amende n'excédant pas cent mille livres.

[101] Art. 2 - loi du 3 Septembre1956 sur le secret bancaire
[102] Publié par le décret 126 du 12 Juin 1959

A l'époque actuelle, ces textes semblent bien en delà de la réalité, sachant que la communication électronique s'est imposée, notamment via les applications de messagerie disponibles sur les réseaux sociaux, ce qui nécessite de modifier les textes en interdisant la violation de la confidentialité des communications électroniques.

4- Loi sur les publications de 1962

Sur la base de l'article 12 du décret législatif portant modification de certaines dispositions de la loi 1962[103], il est interdit de publier : « (...) 3- les Lettres, les Publications, les papiers, les dossiers appartenant à une administration publique et marqués comme confidentiel.

Si des personnes ou des organisations sont lésées par la publication, elles ont le droit de poursuivre la publication devant les tribunaux. »

L'acte d'intimidation sanctionné par l'article 650 du code pénal est également considéré, s'il est fait par des publicités ou publications ou toute image de publication.[104]

5- Loi de 1994 sur l'éthique médicale

Cette loi a consacré dans son article (7) le secret professionnel parmi les obligations confiées au médecin, et il comprend, selon le dispositif de cet article : « Les informations que le patient lui donne, et tout ce qui est été vu, informé, découvert ou inféré dans le cadre de l'exercice de sa profession ou à la suite des examens médicaux subis ».

6- La loi de 1999 sur les services de renseignement secrets[105]

Cette loi concerne explicitement la protection du droit à la vie privée car elle est centrée sur la prévention des écoutes clandestines en vue de préserver le droit de garder le secret entre ses parties.

Ainsi l'article (1) stipule « Le droit à la confidentialité des communications internes et externes par tout moyen de communication filaire ou sans fil (Appareils téléphoniques fixes et appareils mobiles de toutes sortes, y compris téléphones portables, fax et courrier électronique…) est protégé par la loi et ne fait l'objet d'aucune forme d'écoute, de

[103] DL 104 du 30 Juin 1977

[104] Article 16 du décret 104/1977

[105] Loi n. 140 du 27 Octobre 1999 visant la préservation du droit à la confidentialité des communications effectue par tous moyens de communication. La mise en œuvre de ses dispositions a été retardée jusqu'en 2005 en raison du retard dans la publication des décrets d'application à cet égard. Les décrets d'application publiés en 2005 n'ont également été mis en œuvre qu'à partir de la date du 3 février 2009.

surveillance, interception ou divulgation sauf dans les cas prévus par la présente loi et par les moyens qu'elle précise et identifie. »

Le Liban est le premier pays arabe à réglementer l'interception des écoutes clandestines en vertu de la loi 140/1999 permettant autorisant l'interception des renseignements de (2) manières [106]:

- L'objection judiciaire : il appartient au premier juge d'instruction de prononcer une grâce ou suite à la demande du juge chargé de l'enquête, une décision d'intercepter les appels des suspects du crime d'une peine privative de liberté d'au moins un an, en cas d'extrême nécessité non précisée (Ces cas sont laissés au pouvoir discrétionnaire du juge pour les estimer).
- L'objection administrative : selon laquelle il revient au Ministre de la Défense Nationale et au Ministre de l'Intérieur, après approbation du Président du Conseil des ministres, de permettre l'interception de renseignements afin de collecter des informations destinées à lutter contre le terrorisme, les crimes contre la sûreté de l'État et les crimes organisés.

Sous réserve que des décisions rendues dans l'affaire précitée, soient motivées, et que le délai d'opposition n'excède pas les (2) mois.

7- Loi 2005 sur la protection du consommateur[107]

L'article (58) de la loi stipule: « Le professionnel contractuel doit conserver les informations qu'il obtient et ne pas en disposer, à moins que le consommateur n'y a pas consentit. Il doit également prendre toutes les mesures pour préserver la confidentialité de ces informations. »

La protection de la confidentialité du client bancaire n'est pas le seul volet qui a été régit par les lois internes. Aussi la protection de la sécurité de ce client était l'objet de plusieurs études juridiques.

P.2. La protection de la sécurité du client bancaire

La sécurité de la profusion massive d'information de la clientèle de la banque sur internet a fait l'objet de plusieurs initiatives conduits par précisément par la BDL tel que la

[106] Voir Art. 2 à 13 loi 140/1999

[107] Loi N. 659 du 4 Février 2005 modifiée par la loi N. 265 du 15 Avril 2014

circulaire 144/2017 sur la prévention des crimes sur l'internet (A) ainsi que le guide sur la protection contre les crimes par courrier électronique (B).

A. La circulaire 144/2017 de la banque centrale du Liban

En mai 2017, des pirates ont tenté de violer les comptes BDL. Depuis lors et suite à une série de cyberattaques enregistrées contre le Liban en 2017, le gouverneur de la BDL Riad Salameh a souligné que la cyber sécurité financière en particulier est une priorité.

Dans ce sens, la BDL a émis le 28 novembre 2017, une nouvelle circulaire n°. 144, sur la prévention des crimes sur l'internet, posant une exigence sur les banques de renforcer le contrôle de la cybercriminalité dans leurs activités,

Cette circulaire de base impose des obligations supplémentaires aux banques pour prévenir la cybercriminalité.

Tout d'abord, La Banque devrait définir les politiques de sécurité de l'information et mettre en œuvre des mesures de sécurité pour prévenir les cyber crimes, ceci inclut l'analyse des risques de cybercriminalité potentielle et le suivi des derniers développements dans le domaine de la sécurité informatique, l'allocation des fonds et du budget nécessaires à la mise en œuvre des politiques et règles de sécurité informatique, le développement des procédures de sécurité pour la gestion des incidents et la continuité des activités.

La prudence lors de la signature d'un contrat avec un tiers pour attribuer des tâches liées aux systèmes informatiques tout en prenant en considération que ces parties ne traitent pas avec des subordonnés moins fiables.[108]

En ce qui concerne les procédures techniques, elle inclut l'adoption d'une technique qui s'appuie sur au moins deux facteurs pour garantir l'identité des utilisateurs accédant au système hors de la banque, l'adoption des règles strictes pour le filtrage des e-mails reçus et le contrôle de l'accès au mail box dehors la banque, la mise à jour les systèmes informatiques et vérifier la sécurité des appareils des employés utilisés à l'extérieur de la banque. Et enfin la validation et surveillance de l'intégrité des données afin de détecter toute manipulation illégale et remonter à la source de l'accès illégal.[109]

[108] BDL circulaire 144 – Art. 1-Al. 1
[109] BDL circulaire 144 – Art. 1 – Al. 2

En outre, La banque doit prendre des mesures administratives, techniques et judiciaires pour alerter, surveiller et combattre la cybercriminalité financière notamment mettre en place des systèmes et des procédures internes pour l'exécution des demandes de virements reçues par voie électronique (E-Banking, etc.), inclure dans le contrat signé avec le client des dispositions particulières relatives à la spécification d'autres méthodes que les e-mails pour contacter le client afin de confirmer la validité des demandes de virements soumises par voie électronique à condition que ces techniques puissent être modifiées par un accord écrit entre les parties, informer le client des risques résultant de l'utilisation des e-mails lorsqu'il demande des virements financiers et le guider vers d'autres techniques plus sécurisées et obtenir son accord écrit pour supporter ces risques.[110]

Enfin, la circulaire mentionne les actions rapides et efficaces que la banque doit entreprendre lorsqu'elle découvre, a été informée ou notifiée que l'un de ses clients a été victime de cybercriminalité tel que fournir au correspondant et à la banque bénéficiaire les informations relatives et demander l'annulation de l'opération de virement et restituer son montant au client, aviser les entités responsables de l'enquête – La commission spéciale d'investigation – des éléments suivants : La source de l'e-mail (adresse IP) attribué au client ou par son intermédiaire par lequel les transferts suspects ont été envoyées, Le nom du fournisseur d'accès Internet via lequel les demandes de transfert suspectes ont été envoyées. Le nom de la société fournissant le service Internet utilisé pour l'accès non autorisé au compte du client via le service de banque électronique.

Pour finir, la banque doit encourager le client à soumettre un rapport ou une plainte légale aux autorités compétentes.[111]

D'un autre côté, la BDL a émis aussi dans le même cadre un guide sur la lutte contre les cyber cimes financiers par courrier électronique.

B. Le guide sur la lutte contre les cyber crimes financiers par courrier électronique

[110] BDL circulaire 144 – Art. 2
[111] BDL circulaire 144 – Art. 3

Connu par le guide de la BDL sur la lutte contre les cyber crimes financiers par courrier électronique publié en octobre 2016 en collaboration entre la Commission Spéciale d'Enquête (SIC), l'Association des Banques du Liban (ABL) et les Forces de Sécurité Intérieure (FSI), ce guide constitue une prévention contre la cybercriminalité financière au Liban. Il est le résultat d'énormes effort mis en place après la fin du premier forum contre la cybercriminalité qui a eu lieu en Novembre 2015.[112]

Ce guide est divisé en deux parties, la première concerne les lignes directrices pour le secteur financier (banques, institution financières…) et la deuxième concerne les personnes et les autres institutions non financiers.
Il traite les signes indicatifs des actes criminels par e-mail, les instructions et mesures de prévention et de protection numérique des actes criminels utilisés dans la cybercriminalité et les actions correctives mais aussi présente les formalités à suivre en cas de détection d'actes criminels commis dans le secteur financier pour l'aider à éviter le vol, les actes de piratage, le détournement de fonds, le chantage et de l'espionnage par voie électronique

Ainsi, les banques devraient mettre en place des règles internes spécifiques pour traiter les demandes de transfert d'argent reçues par des moyens électroniques tels que les e-mails et les opérations bancaires électroniques.

Par exemple, la banque doit bien examiner l'adresse e-mail du récipient, et être consciente de toutes formes d'anormalité, comme les fautes de frappes ou les changements dans la présentation de l'e-mail. De même, elles sont obligées d'appeler le client pour pouvoir exécuter la transaction. Si la banque réussit à contacter la banque bénéficiaire du transfert dans les 24 heures qui suivent la fraude, elle peut « sauver » ce montant et arrêter tout de suite la transaction.
Les contrats signés avec les clients doivent inclure des clauses spécifiques qui identifient les moyens autres que les e-mails pour contacter les clients, tels que les appels

[112] Celine Haddad, Un guide pour aider les banques à lutter contre la cybercriminalité financière, L'orient le jour 25 Octobre 2016,
https://www.lorientlejour.com/article/1014552/un-guide-pour-aider-les-banques-a-lutter-contre-la-cybercriminalite-financiere.html - Date de la visite 20 Octobre 2022

téléphoniques pour vérifier que les demandes de transfert d'argent reçues par voie électronique sont authentiques.

Ce guide vise enfin à sensibiliser le secteur financier, les entreprises et les particuliers à tous les types de cybercriminalité par courrier électronique et constitue une référence pour la mise en œuvre des opérations électroniques en toute sécurité tout en évitant les risques de piratage des informations et leur utilisation à des fins illégales telles que l'extorsion financière, la fraude et le vol.

Chapitre 2 : Les droits liés à la protection des données personnelles

De nos jours, en juste quelques secondes, de multiples quantités de données font l'objet des opérations bancaires entre les clients. Dans ce sens, il est important de comprendre la nature, les outils, et l'impact de ces données à caractère personnelle sur la banque.

Ainsi, nous exposerons les dispositions du RGPD dans la digitalisation des banques (Section 1), et l'impact du RGPD sur la banque digitale (Section 2).

Section 1 : Les dispositions du RGPD dans la digitalisation des banques

Dans une société désormais numérique, les données personnelles des clients se sont transformées en marchandises que tu achètes et vends. Au niveau international, l'union européenne a émis une règlementation spécifique qui tient à conserver et sécuriser les données personnelles tout en interdisant la collection de ces données sans avis préalable des personnes concernées. Alors qu'au Liban, les législateurs ont essayé de légiférer une loi visant le respect de ce genre de données.

Que signifie données à caractère personnel ? Selon l'article 4 du règlement européen 2016/679 « constitue une donnée a caractère personnel toute information relative à une personne physique identifié ou identifiable.[113]
De sa part la loi libanaise sur les transactions électroniques et les données a caractère personnel définit ces genres de données comme suit « toute espèce d'informations relatives à une personne physique, dont elles permettent l'identification , directe ou indirecte, y compris par voie de regroupement ou de croisement[114]

On remarque qu'il existe deux types de données en France comme au Liban : les données permettant une identification directe à l'exemple du nom ou du prénom et les données

[113] Règlement (UE) 2016/679 du parlement et conseil europpéen 27 Avril 2016 relatif à la protection des personnes physique à l'égard du traitement des données a caractère personnel et à la libre circulation de ces données, Art. 4
[114] Loi n. 81, 10 Octobre 2018, Art. 1

permettant une identification indirecte suite au regroupement de deux ou plusieurs données.

Au Liban, on remarque l'absence d'une législation qui régit la collecte et le traitement des données personnelles de manière optimale. Au contraire, les auteurs encouragent une conception généralisée de cette notion.[115]

Selon la doctrine, constitue une donnée personnelle, toute donnée susceptible de permettre ou de faciliter l'identification d'une personne.[116]

Une telle vision extensive de la notion ressort principalement de la définition qui a été proposée par l'Association Libanaise des Technologies de l'Information (LITA) dans un projet de texte de loi qui vise a régir la protection des données à caractère personnel.[117]

Dans la même optique, le législateur européen a opté pour une définition encore large dans l'article 4 du règlement 2016/679 concernant la protection des données.[118]

Tenant compte de ce cadre actuel, nous exposerons la protection des données personnelles au niveau international, (P.1) pour passer au cadre législatif du RGPD au Liban (P.2).

P.1 La protection des données personnelles au niveau international

Dans les textes internationaux de lois contemporains, on parle récemment beaucoup de la protection des données à caractère personnelles, même si le concept de la vie privée diffère pour chaque pays.

---

[115] Moughabgheb N., la protection des programmes informatiques. Les moyens et les lacunes, Beyrouth, El Halabi, 2006, P 193 et suivant

[116] M. Al ASHKAR Jabbour et M A. Jabbour, op. Cit., P. 171

[117] Projet de texte de loi propose par LITA. Art. 3 http://www.lita-lb.org

[118] Règlement 2016/679 du 27 Avril 2016, art. 4: " toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Il est donc opportun d'entamer principalement les lois de l'union européenne compte tenu que l'Europe est le premier continent qui a rassemblé ces normes dans un concept juridique bien encadré. Nous parlerons ainsi du Règlement Général sur la Protection des Données (RGPD) (A) et de la directive police justice (B).

A. Le RGPD

Le Règlement Européen sur la protection des données impacte toute entreprise traitant des données à caractère personnel sur des résidents européens.

Il est considéré comme un des piliers fondamentaux de la conformité des données personnelles.

Au sens du RGPD, le mot « traitant » signifie l'accès, la collecte, le stockage, la destruction et la manipulation de ces données.

En fait, il s'agit d'un règlement européen qui est entré en vigueur le 25 Mai 2018. Ce règlement a remplacé la loi 95/46/CE daté du 1995 qu'on a déjà évoqué grâce à l'évolution numérique et technologique très rapide durant les dernières années.

Ce règlement donc place un cadre juridique pour la protection des données à caractère personnel tout en donnant aux responsables de ces données le privilège de contrôler leurs données personnelles.

Le règlement définit les données à caractère personnels comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Ainsi le RGPD s'applique à la protection des données personnelles attachées uniquement à des personnes physiques ou bien au représentants des personnes morales[119].

[119] Par personne physique identifiable, il faut comprendre « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

Ainsi, ce dernier s'applique à toute genre d'entreprises, publique ou privée étant un état membre de l'union européenne. Plus spécifiquement, les entreprises offrant des biens et services sur le marché européen et celles qui utilisent et collectent ce genre de données sur les résidents de l'union européenne.[120] Il s'applique tout au long de la vie des données de la conception jusqu'à la suppression.

En ce qui concerne les principes régissant le RGPD, ces derniers constituent le fondement des dispositions du règlement. On évoque le consentement qui doit être explicite et positif. En fait, le consentement est bien visible dans la gestion des cookies qui demandent l'acceptation de l'utilisateur sur le poursuivi de sa navigation sur un site et parfois imposent un consentement explicite (case à cocher par exemple). Aussi les entreprises sont obligées de fournir des informations claires et concises sur la façon dont les données sont traitées, c'est le principe de la transparence. Le RGPD a renforcé de même le droit des résidents européens comme le droit d'oubli ou la suppression des données suite à une demande. Enfin, on nomme le principe de la responsabilité visant à obliger les entreprises de documenter toutes mesures et procédures en matière de sécurité à l'aide d'un registre de traitement.

Signalons que toute entreprise qui effectue des traitements sur les données sensibles doit désigner un Délégué à la Protection des Données (DPO) dont la mission est de piloter la gouvernance des données et de contrôler la conformité juridique de l'entreprise avec la nouvelle règlementation.

Au-delà de ce règlement, la France a publié une directive spécialisée du traitement des données à caractère personnelles en matière pénale et particulièrement aux activités menées par la police.

B. La Directive Police justice

La directive n° 2016/680 daté le 27 Avril 2016, connue sous le nom de directive police justice relative « à la protection des personnes physiques à l`égard du traitement des

[120] L'essentiel à connaître sur le RGPD : définition, périmètre, principes et mesures https://www.custup.com/introduction-gdpr-rgpd/ date de la visite 25 Octobre 2022.

données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d`enquêtes et de poursuites en la matière », présente les règles relatives à la protection des personnes physiques via a vis le traitement des données personnelles par les autorités responsables dans le but de prévenir et détecter les infractions pénales, de conduire les enquêtes et les poursuites et d'appliquer les sanctions pénales. Elle a été transposée au chapitre 8 de la loi Informatique et Libertés en France.
Ainsi, ladite directive s'applique en matière pénale et spécifiquement dans les activités conduites par la police par exemple les traitements qui permettent de gérer les mesures d'application des peines réclamées par l'autorité judiciaire. De même que les activités préventives de police ayant pour but de protéger contre les menaces de sécurité publique pouvant amener à une qualification pénale (le maintien de l'ordre public).
Donc les données à caractère personnel concernent les personnes coupables ou victimes d'une infraction pénale, les tiers à une infraction pénale et ainsi de suite.

Par suite les données à finalité pénale n'entrent dans le champ d'application de ladite directive que s'ils sont conduites par une autorité compétente. On veut dire par autorité compétente, une autorité publique responsable d'exécuter des sanctions pénales ou de détecter et prévenir les infractions pénales comme la police par exemple. [121]

On conclut que la règlementation RGPD et la directive police justice s'applique dans des champs d'applications différents cependant ils sont complémentaires dans le sens ou tous les deux visent la protection des données à caractère personnel.
Notons que le traitement des données assurant la sureté de l'état ou la défense nationale sont régis exclusivement par la loi informatique et libertés.

Donc la directive se caractérise par sa spécifié en terme du champ d'application et des droits qui lui sont relatives. On nomme de ces droits l'information de la personne concernée.[122], le droit de rectifier au d'effacer les données personnelles, la limitation du

[121] CNIL, Directive Police-justice- De quoi parle-t-on? 20 Fevrier 2019
https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t-on
[122] Voir Article 13 du RGPD

droit d'accès dans le but de ne pas entraver les enquêtes ou nuire à la détection des infractions pénales.[123]

Au niveau national et dans un nouveau concept sur la scène règlementaire libanaise, le Liban à règlementer l'ensemble des transactions électroniques ainsi que les données à caractère personnel dans un cadre réglementaire qui englobe en même temps le civil, la procédure civile, le pénal, la procédure pénale ainsi que le commercial contrairement aux lois habituelles qui traitent normalement un seul type de droit.

P.2 Le cadre législatif du RGPD au Liban

La BDL a traité la problématique de la protection des données personnelles dans une circulaire 146/ 2018 (A) mais aussi le parlement libanais a publié une loi 81/2018 proposant un ensemble de nouvelles lois ainsi que des modifications aux lois existantes dans le but de règlementer le marché numérique actuel. (B)

A. La circulaire 146/2018 de la banque centrale du Liban

La BDL a émis le 13 Septembre 2018, le circulaire de base 146 – Décision 12872 – relatif à la protection des données à caractère personnel adressée aux banques et aux institutions financières ayant un effet immédiat.

Cette décision est tellement cruciale comme elle montre clairement l'occupation des régulateurs non européen à un règlement européen de telle importance et elle a permis de donner le premier cadre légal pour la protection des données personnelles au Liban.

Selon ledit circulaire, les banques doivent prendre les mesures nécessaires pour se conformer au RGPD issue par le Parlement Européen et le Conseil de l'Union Européenne.

Aussi, la BDL a demandé aux banques d'effectuer une série d'actions avant le 31 décembre 2018 : informer la BDL et la BCC des actions entreprises par la Banque pour mettre en œuvre le RGPD ; Notifier la BDL et la BCC du délégué à la protection des données et le représentant auprès de l'Union européenne désignés par les responsables de conformité juridique et enfin modifier le programme de la conformité juridique pour inclure les exigences du RGPD.

[123] Voir Article 15 du RGPD

Ce circulaire vise à permettre aux clients du secteur financier de contrôler leurs données personnelles et à simplifier le cadre réglementaire du secteur financier dans l'ère de l'économie digitale.

En ce qui concerne la loi 81/2018 précitée, cette dernière a constitué une révolution dans le monde électronique numérique contemporain surtout qu'au Liban les lois et règlements en cette matière étaient encore très timide et vague.

B. La loi 81/2018 en matière de protection des données personnelles

Bien que la loi couvre les questions de collecte, de traitement et d'utilisation des données personnelles par voie électronique, la loi contient diverses lacunes, notamment dans le domaine de la protection des données personnelles. Plus précisément, la loi ne prévoit pas une protection juridique adéquate pour le droit des citoyens libanais de demander réparation et de rectifier leurs données personnelles collectées, et le droit d'être protégé contre les utilisations contraires à l'éthique de leurs données personnelles, telles qu'une prise de décision automatisée qui pourrait avoir un impact négatif sur leurs moyens de subsistance.

L'article 7 de la Constitution garantit la liberté personnelle aux personnes qui ne violent pas la loi, et qu'aucune peine ne peut être appliquée si elle n'est pas légale. Il existe plusieurs cas où les entreprises effectuent des choix automatisés concernant les clients ou les utilisateurs (par exemple, sur plateformes de médias sociaux) pouvant avoir un impact significatif sur leur vie et les exposer à un préjudice grave. Même si les décisions automatisées sont associées à des décisions humaines, cela reste une atteinte majeure à la vie privée qui soulève d'importants débats constitutionnels qui doivent être discuté [124].

Lorsque des entités collectent des données personnelles auprès des citoyens libanais, la loi sur les transactions électroniques n'offre pas une protection totale. Bien que la législation exige que les individus ou que les groupes soient informés de la collecte de leurs données, le consentement éclairé n'est pas nécessaire si l'organisation collectant les données peut invoquer des circonstances qui rendent difficile la notification les personnes auprès desquelles les données sont collectées au terme de l'article 88 et 89.

[124] ETER Sanaa, The Lebanese e-transaction law in relation with personal data protection law, Data and Society, 30 April 2019

Les participants doivent avoir le droit de savoir comment leurs données personnelles sont traitées à toutes les phases de la gestion des données, en commençant par l'acquisition et en terminant par la suppression, selon le Signal Code (Initiative humanitaire de Harvard, 2016).

Le règlement E-transaction, en revanche, ne précise pas ce qui constitue « **un effort qui n'est pas proportionné à l'avantage de la conduite** » (art. 89). En conséquence de cette lacune, les entreprises de traitement de données pourraient profiter du cadre juridique et éviter d'obtenir le consentement clair des personnes.

On déduit que, ceux qui sont déjà marginalisés et vivant dans des situations déplorables sont particulièrement susceptibles de perdre leur agence de données. Ceci n'est pas seulement contraire à l'éthique, mais va également à l'encontre des garanties des droits de la Constitution libanaise.

L'article 7 de la Constitution, garantit que tous les Libanais sont égaux en droit, qu'ils ont les mêmes droits civiques et politiques et qu'ils sont également responsables de leurs tâches civiques.

Selon Dorine Saleh, "La loi sur les transactions électroniques est faible parce qu'elle ne garantit pas que les gens obtiennent l'aide dont ils ont besoin pour comprendre leurs droits en matière de protection des données personnelles ; et elle suppose que tous les citoyens sont également capables de comprendre un texte législatif et autres types de textes juridiques et des documents administratifs comme un formulaire de consentement éclairé.[125]

En effet, plutôt que de créer une agence indépendante pour superviser la collecte, le traitement et l'utilisation des données personnelles, la loi place l'essentiel de l'obligation de protéger les droits des citoyens sur leurs données personnelles entre les mains du ministère libanais de l'Économie et du Commerce.

Étant donné le niveau élevé de corruption dans le secteur public libanais, les observateurs estiment que les droits des citoyens en matière de données seront faiblement protégés et que les entreprises ayant des liens avec le gouvernement aurait la carte blanche pour exploiter les données personnelles de ses clients

[125] ETER Sanaa, The Lebanese e-transaction law in relation with personal data protection law, Data and Society, 30 April 2019

En ce qui concerne l'échange d'informations, la loi 81 confère au pouvoir exécutif un quasi-monopole sur la collecte, le stockage, la modification, l'utilisation et même la publication des données. La concentration d'énormes pouvoirs dans une seule branche du gouvernement sape la légitimité de la loi dans son ensemble en augmentant la possibilité du potentiel d'exploitation et de chantage et d'autres problèmes.

On conclut ainsi que le ministère de l'Économie est habilité à échanger des informations, bien que les critères sous lesquelles il peut le faire ne sont pas claires.[126]

En outre, la loi précise les "procédures judiciaires de diverses natures"[127] comme justification valable au ministre de la Justice d'accorder l'accès à certains types d'informations sur Internet. Ce qui engendre que ces données peuvent être utilisées sans informer le sujet ou obtenir son approbation orale ou écrite.

Une interprétation de l'article 94, nous montre une ambiguïté quant à ce que constitue une cause légitime pour l'acquisition de données. Elle se concentre sur la présentation d'une large liste d'organisations qui sont exclus de l'obligation d'obtenir une autorisation pour collecter et traiter des données à caractère personnel. Ce manque de spécificité rend très facile pour le ministère de l'Économie et Le commerce d'accorder des permis aux organisations qu'il favorise tout en rejetant les demandes de ceux qui ne le plait pas, ce qui ouvre la porte à la corruption pour bien s'installer.

De plus, avec tous les problèmes que survit le Liban, il est incontournable que le ministère de l'Économie et du Commerce manque des ressources nécessaires (personnel qualifié avec suffisamment de temps) pour assurer que tous les aspects de la gestion des données couverts par la loi font l'objet d'un contrôle efficace. Même si des personnes allèguent des abus, leurs demandes seront traitées avec des retards importants, empêchant les citoyens de préserver leurs données personnelles à temps.

Nous pouvons conclure donc que la loi aurait dû créer un organisme spécifique indépendant du gouvernement pour traiter et contrôler les données personnelles à la façon de l'article 8,

[126] Data guidance, comments on Law 81/2018 related to the electronic transactions and data protection, Octobre 2022

[127] Article 97 section 2 de la loi 81/2018

paragraphe 3, de la Charte des droits fondamentaux de l'UE qui affirme que les membres de l'UE établissent des autorités nationales chargées de protéger les données personnelles. Ces corps sont indépendants et autonomes.

En France, l'autorité française de protection des données est la Commission nationale de l'informatique et Libertés (CNIL). En tant qu'établissement public autonome, la CNIL a été investi des pouvoirs de sanction, de contrôle et d'enquête et de réglementation.

Elle n'est sous la direction d'aucune autorité gouvernementale ce qui le rend impartial et efficace contrairement à la loi libanaise sur la protection des données.

De même, l'UE a mis en place le comité européen de la protection des données (EDPB); un organe européen autonome chargé de veiller à ce que les règles de protection des données soient uniformément respectée dans toute l'UE.

Les principales responsabilités de l'EDPB sont de fournir des orientations générales sur les le RGPD et son application, conseiller la Commission européenne sur les données personnelles, les problèmes de confidentialité et les nouvelles lois suggérées dans l'Union européenne, ainsi que la gestion des conflits entre les organes nationaux de contrôle.

À cet égard, non seulement les pays européens ont donné des pouvoirs de protection des données a des organes autonomes indépendants, mais l'intégrité de ces organes était également contrôlée par un comité européen de la protection des données.

La loi libanaise sur les transactions électroniques ne protège pas non plus de manière adéquate le droit à la réparation et à la modification de tout aspect des données recueillies. Les particuliers ont le droit de demander des modifications à des données trompeuses, inexactes ou incomplètes. Cependant, il n'est pas clair si ce droit s'applique pendant la durée de gestion des données personnelles.

Les personnes ordinaires, pour exemple, ne peuvent s'opposer à la collecte et au traitement des données que s'ils n'ont pas préalablement accepté le traitement en vertu de l'art. 101.

En outre, au terme de l'article 102, la loi stipule que si une personne notifie au responsable des données son désir d'avoir ses données supprimées et que le responsable des données ne

prend pas de mesures efficaces, la personne doit déposer une plainte auprès du magistrat de la justice sommaire rendant l'exercice du droit de recours et de rectification extrêmement coûteux et difficile pour les citoyens libanais.

Toutefois, si une seule personne est accusée de nuire à l'intérêt public ou au bien commun du pays, il est permis d'accéder aux données du téléphone portable du suspect. Par conséquent, les données personnelles sont accessibles selon une seule règle, qui est celle du pays et l'intérêt supérieur du public. Les intérêts supérieurs du public comprennent le fait d'infliger des dommages au pays dans son ensemble ou étant lié à des attentats terroristes.

Enfin, la loi comporte un article qui fait référence au droit d'être protéger contre les décisions effectuées à l'aide de traitements automatisés ayant des conséquences juridiques ou administratives. Cependant, la loi mentionne seulement que les individus ont le droit d'examiner et d'objecter, et il ne fait aucune mention de la responsabilité du responsable des données de fournir aux individus une l'explication de la décision et un moyen efficace de la contester.[128]

Section 2 : l'impact du RGPD sur la banque digitale

Le Règlement Général sur la Protection des Données a fait acquérir au client bancaire de nouveaux droits dont il peut bénéficier en tant qu'acteur actif dans l'économie. Cependant les paramètres de la protection demeurent très faibles vu que le principe de la protection des données personnelles est encore timide et n'a pas été intégré dans les opérations quotidiennes de nos jours.

Or ce qui importe tout particulièrement dans notre cas c'est la protection des données a caractère personnel qui est une notion très spécifique et non pas toute la vie privée de la personne concernée, qui est au contraire une notion plus large.

Nous verrons dans cette section les nouveaux droits acquis par le client (P.1) ainsi que les faiblesses des paramètres de la protection (P.2)

[128] Article 86 de la loi 81/2018

P.1 : De nouveaux droits acquis par le client bancaire

Dans ce monde digital, le client bancaire désormais jouit de droits additionnels à ceux dont il jouissait auparavant. Ce privilège est à la base des nouvelles technologies qui ont donné place à de nouveaux droits et obligations vis-à-vis ce client.

Pour développer ce concept, on examinera la protection des données personnelles du client bancaire dans les opérations digitales (A) et les principales droits liés à la protection de ces données (B).

A. La protection des données personnelles du client bancaire dans les opérations digitales

A l'heure du « big data » et de la transformation numérique des services financiers, il est inévitable que les données personnelles massives des clients, facilement accessible, sont au cœur des préoccupations des banques et occupent une importance capitale dans leur vision d'aujourd'hui.

Ces données très spécifiques et critiques sont remplies d'information très confidentielles qui ne doivent certainement pas tomber dans les mains de tout individu. Ils décryptent la situation financière du client, ses revenues, sa profession… Ainsi la banque a une obligation majeure de protéger et de sécuriser les données personnelles de ses clients, ce qui a engendré autant d'opportunité que de risques.

En France, la protection des données personnelles telle que prévue dans le RGPD est devenu impérative avec l'ère du digital peur que ces données soient violées conduisant à des conséquences néfastes pour les clients bancaires. Ainsi, le client bancaire bénéficie d'une grande maîtrise sur ses propres données et il est plus confident et rassuré que ses données sont bien protégées.

En outre, la sécurité des données personnelles des clients vise à sécuriser chaque transaction conduite dans le but de protéger le client de la fraude en ligne et de la cybercriminalité financière surtout avec la digitalisation du secteur bancaire. Ces mesures de sécurité doivent garantir surtout l'accessibilité et la facilité d'utilisation de ces services.

Le RGPD s'est basé sur plusieurs principes dans le domaine bancaire afin de réussir cette protection. On nomme « l'accountability » qui affirme que les banques sont les seules responsables de leur mise en conformité durable. Le « privacy by design » stipule que les banques doivent sécuriser leurs données personnelles dès la conception des biens et services offertes par eux. La « licéité du traitement » qui confirme que ces données seront traitées en se basant uniquement sur un fondement juridique mis en place par le RGPD. « La transparence » ou le traitement de données ne doit être ambiguë et le consommateur bancaire doit pouvoir exercer ses droits dans le respect du RGPD auprès de sa banque. Enfin, la « minimisation et la pertinence », ces données sont collectées dans un but bien définit et répondent au traitement conduit. La conservation de ces données doit se limiter à un temps bien défini.[129]

Ces principes sont d'une importance primordiale pour la bonne préservation de la sécurité des données personnelles et incombe aux banques d'élaborer un registre de traitement des données pour répondre aux défis règlementaires.

La mise en conformité à ce règlement supposait l'adoption d'une stratégie capable de couvrir tout le périmètre d'activité de la banque. Cette stratégie commence par la nomination d'un « Data Protection Officer » (DPO) chargé de traiter les sujets relatifs à la protection des données personnelles de la collecte a la destruction et d'évaluer le niveau de conformité de la banque afin de procéder à la remédiation des sujets non conformes relevant de cette protection.[130]

Dans ce contexte, la CNIL a publié un nouveau livre blanc sur les moyens de paiement et données personnelles. Ce livre aborde des sujets varies et se base sur les points adoptes par la CNIL en matière d'application du RGPD dans le domaine du paiement (l'anonymat, le

[129] Kevin Thomas, protection des données bancaire, quelles sont les nouvelles mesures? 12 Aout 2020, Indice RH date de la visite 27 Octobre 2022 https://www.indicerh.net/protection-des-donnes-bancaires-quelles-sont-les-nouvelles mesures/#:~:text=Loyaut%C3%A9%20et%20transparence%3A%20tout%20traitement,qui%20sera%20fait%20sans%20d%C3%A9viance

[130] Accelerate Collective Intelligence Partner, Le règlement général sur la protection des données RGPD, règlementation et enjeux dans les banques et assurances, 20 Febvrier 2021

choix de paiement, protection de la confidentialité des transactions, la sécurité des données des paiements…).

Suite à la pandémie, à la guerre contre l'Ukraine at aux crises financières mondiale, le secteur bancaire s'est trouvé soumis à une grande pression dans le but d'optimiser ses opérations et répondre aux évolutions et changements de réglementation qui ont spécifiquement touché la conformité juridique des données personnelles des clients bancaires.

Cela a mis une pression sur les banques qui se sont noyées dans l'obligation d'améliorer l'engagement de la clientèle dans les opérations bancaire et l'obligation de bien gérer les risques liés à la protection de leur donnée personnelle.

Pour garantir cette protection, le règlement a défini de nouveaux droits dans le but de protéger la vie privée de la clientèle.

B. Les droits du client bancaire liés à la protection des données personnelles

Au fil du temps, les droits dont disposent Les personnes responsable de la collecte de données personnelles ont été renforcés par le RGPD au fil du temps. On nomme:

Le droit d'accès à l'information, ce droit permet de savoir si les données concernant le client sont traites. Le client peut y accéder à l'aide d'un format compréhensible. Le client ainsi peut contrôler si les données sont exactes.

Ainsi la personne en charge de traiter les données doit renseigner le client du but de l'utilisation des données, les destinataires qui vont accéder ces données, la durée de leur conservation et toute autre information relative à leur source. Alors que **Le droit à la rectification** donne l'avantage au client de rectifier les informations qui ne sont pas exactes (corriger les données personnelles dans le fichier « Know Your Customer » (KYC) comme l'âge, l'adresse…) ou complète (un KYC sans le numéro de téléphone par exemple) car la publication d'informations incorrectes par la banque engendre des pénalités. Ce droit peut avoir lieu soit par courrier ou par voie électronique.

Le privilège de récupérer ces données dans un format lisible par une machine constitue le droit à la portabilité. Ces informations peuvent ainsi être transmis au client pour un usage personnel ou même à une autre banque surtout avec la loi Macron de 2017 qui a facilité la transmission des données de la clientèle lors d'un changement de la banque. Ce droit par conséquence renforce la maitrise du client sur ses propres données.

Le droit à l'effacement ou autrement le droit à l'oubli permet à la banque d'effacer des données personnelles concernant son client.

Dans le monde numérique, le droit à l'oubli est un pilier fondamental car il donne droit au client d'exiger que les informations le concernant ne soient pas conservées pour une durée indéterminée, afin qu'elles ne soient conservées que pour une durée limitée raisonnables, n'excédant pas ceux nécessaires pour atteindre les objectifs pour lesquels la collecte et le traitement ont été effectués.

Enfin le client a **le droit de refuser** l'utilisation de ses données personnelles par la banque en cas de situation particulière. Pour fonder sa demande, ce refus doit être motiver par des justificatifs légitimes. Ce fait reflète le droit d'opposition.[131]

La loi 81/2018 a consacré implicitement les droits précités dans l'article 101 : « Le propriétaire des données à caractère personnel ou l'un de ses héritiers peut demander au responsable du traitement des données de les corriger, les compléter, les mettre à jour

Ou effacés, de même pour les informations qui sont incorrects, incomplets, ambigus, périmés ou incompatibles avec les finalités du traitement ou celles dont il est interdit de traiter, collecter, utiliser, conserver ou transmettre. »

Sur la base de ce qui précède, il est évident que le RGPD place le client bancaire dans une position de contrôle absolu de ses données personnelles, ce qui engendre des garanties suffisantes de sa vie privée.

[131] Article (21) du RGPD

En raison de la nature des données personnelles bancaire et du rythme d'activité interactive sur ceux-ci, qui permet une diffusion et une circulation rapide des données, la meilleure option semble être pour le client de bien ajuster les paramètres et les droits de protection et de sécurisation que la banque place entre ses mains, afin de gérer ses données.

P.2 La faiblesse des paramètres de la protection

Afin de mieux analyser cette faiblesse et de comprendre les raisons pour lesquelles, l'implémentation des provisions relatives à la protection des données personnelles n'a pas bien réussi. Il convient à présent d'explorer la faible conformité au RGPD dans les banques digitales (A) et les conséquences de la non-conformité au RGPD (B).

A. Une faible conformité au RGPD dans les banques digitales

Le Liban fait face à l'une des trois pires crises à l'échelle mondiale depuis 150 ans, selon la Banque de France. [132]

Depuis Octobre, la situation économique continue de se dégrader suite à la crise financière des Banques qui a dévalorisé la monnaie locale de plus de 100%.
Le système de protection ne doit pas se reposer sur des exigences imposées sur la banque seulement, mais également le client doit être impliqué dans ce système.

Le client bancaire jouit d'un accès très restreints à ses comptes bancaires. Les banques ont ainsi priorisé leurs obligations envers le client et par suite la conformité au RGPD n'était pas considéré une priorité ce qui a engendré une grande faiblesse du taux de conformité au RGPD dans le secteur bancaire.

Même si la loi 81/2018 a apporté quelques modifications législatives qui certainement contribueront au développement du commerce électronique et des contrats électroniques, Elle a échoué à résoudre le problème de la protection des données personnelles.

[132] Belhache Pierre, Anytime, Crise Bancaire au Liban: Les épargnants réclament leurs argents, 7 Septembre 2022, https://www.anyti.me/fr/actualites/crise-bancaire-au-liban-les-epargnants-reclament-leur-argent/1370 date de la visit 28 Octobre 2022

Les citoyens libanais semblent être à la merci des entreprises et des organisations dont les politiques de gestion des données ne sont que réglementées par le ministère de l'Économie et du Commerce, qui a déjà beaucoup à faire et n'est pas préparé à ce problème.

Aussi, la suppression de certaines normes et l'ambiguïté de plusieurs dispositions de la loi permet aux entités de continuer à traiter relativement facilement les données personnelles des citoyens libanais sans égard pour leur droit sacré constitutionnel de protection des données personnelles. Surtout que toutes les provisions de la loi font référence à la banque centrale qui jusqu'à nos jours n'a émis les décrets et procédures d'application comme c'était prévu dans la loi.

En effet, à la place de donner aux citoyens plus de contrôle sur leurs données personnelles qui peuvent être utilisées par divers entreprises et organismes publics, la loi donne simplement au gouvernement plus d'autorité sur ces données.

De plus, la BDL circulaire 146 est très laconique du fait que la décision n'a pas imposé des amendes en cas de non-conformité et ne précise pas la responsabilité du secteur financier suite aux exigences strictes placées par le RGPD. Il s'est juste contenté de mentionner que les auditeurs externes doivent vérifier la conformité des banques avec les dispositions de la décision et insérer dans leur rapport annuel toutes les informations détaillant le processus de vérification des mesures adoptées en ce qui concerne la protection des données à caractère personnel, ainsi que leur résultats d'audit et observations pertinentes.

L'interprétation et l'application du règlement donnent du fil à retordre aux banques libanaise. Les banques ne sont clairement pas capables de conformer aux règlements relatives au RGPD. Pour se conformer pleinement au RGPD, il est vital de comprendre le cadre législatif du règlement et de rédiger les procédures adéquates à son application.

On déduit qu'il reste beaucoup de travail à faire en qui concerne la conformité des banques au RGPD. Les banques doivent enclencher un programme basé sur la gouvernance des données bancaires pour jouir d'une vision à 360 degrés des données de leur clientèle.

Aussi, elles doivent êtres très conscients de l'importance des amendes et pénalités qu'elle risque en cas de non-conformité, et notamment les atteintes considérables à leur réputation.

De même, l'automatisation et la digitalisation des opérations bancaire aidera fortement les banques dans leur plan de conformité juridique surtout dans le traitement des données qui jusqu'à aujourd'hui demeure toujours manuel.

Dans la partie suivante, on verra les sanctions pénales comme conséquence directe de la non-conformité au RGPD au niveau national et international.

B. Les conséquences de la non-conformité au RGPD

Se référant aux articles 1240 code civile français et article 122 code des obligations et des contrats libanais, selon ces articles tout acte qui peut causer un dommage à autrui oblige son auteur effectivement à le réparer.

Face aux multiples pratiques illicites, nous sommes à la recherche d'un régime original dans lequel des nouvelles sanctions sont nés jouissant d'un impact réputation ainsi qu'une stratégie qui est adapté à l'ampleur des entraves.

Le principal but visé par la sanction est le respect de la règle de droit. Elle constitue un des critères de la règle légale.

La sanction est définie comme toute mesure qui est justifiée par la simple violation d'une obligation.[133]

Les sanctions sont très variées et s'applique selon l'hypothèse et le contexte en œuvre. Elles doivent atteindre le résultat souhaitable.

Les législateurs doivent se détacher des mesures classiques et recourir à des règles pointilleuses, adaptés à la lecture électronique garantissant une prise de connaissance bien adaptée. Cette adaptation doit ainsi concerner des dispositions spécifiques relatives aux sanctions.

[133] Voire définition sanction in G. Cornu. Vocabulaire Juridique. Association Henri Capitant, Paris, PUF, 11eme édition, 2016, P. 948

La non-conformité au RGPD engendre différents risques sur l'individu ainsi que sur l'entité. Ces risques sont les mêmes pour les banques.

Concernant le risque financier, La CNIL – commission chargée d'adresser les amendes - établit deux catégories d'amendes administratives pour les entités qui recueillent, conservent, échangent ou analysent les données qui pourraient être exploitées pour reconnaître une personne d'un État de l'UE. Les deux sont onéreux.

Niveau 1 : 2 % du revenu mondial annuel, ou dix millions d'euros, selon le montant le plus élevé.

Les violations de données, le défaut d'entreprendre une évaluation de l'impact sur la confidentialité des données (DPIA) et la tenue de registres inadéquate sont autant d'exemples de non-conformité.

Niveau 2 : 20 millions d'euros, soit 4 % du chiffre d'affaires mondial pour la non-conformité dans les domaines tels que le défaut d'obtenir une autorisation ou le défaut de protéger les droits des consommateurs en vertu des normes du RGPD sont des exemples de non-conformité.[134]

Des dommages et intérêts peuvent être récupérer aussi devant les tribunaux physiques. De même, le juge peut prononcer des amendes pénales en cas de manquement des dispositions pénales.

Aussi le non-respect du RGPD peut engendrer une interdiction administrative de la mise en œuvre des traitements des données personnelles ce qui entraîne la suspension de l'activité de l'entreprise reposant sur tel traitement.

Concernant les sanctions pénales, celles-ci peuvent aller jusqu'à 1 500 000 euros d'amendes pour la personne morale et 5 ans de prison et 300 000 euros d'amendes pour les dirigeants. Ce risque s'accompagne du risque juridique dans le cas où le traitement des

[134] CNIL, https://www.cnil.fr/fr/cnil-direct/question/sanctions-quelles-sanctions-peuvent-etre-prononcees-par-la-cnil, date de la visite 26 Octobre 2022

données sert comme preuve dans un contentieux commercial. Dans ce cas, la preuve peur être révoquée si elle est fondée sur un traitement illégal.[135]

Au Liban, il existe des sanctions très similaires de la France. On peut les trouver dans le chapitre 5 de la loi 81. Aux termes des articles 106 à 109 de la loi 81/2018, les amendes varient de 1 million jusqu'à 15 millions, Ils prévoient que tout professionnel qui collecte et traite des données a caractère personnel sans respecter les exigences de protection de ces données, doit être sanctionné d'une amende pénale de 1M a 30M LBP et d'une peine d'emprisonnement de 3 mois allant jusqu'à 3 ans ou par l'une de ces 2 sanctions.
Il en ressort que la sanction applicable en cas de méconnaissance de la loi est d'une utilité limitée ; Les dommages indirects ne sont pas pris en compte. Même chose pour les dommages futurs.

Par exemple, le plafond prévu pour la sanction en droit Libanais n'est pas bien adapté. Ainsi une entreprise touchant des gains très élevés ne sera dissuadée de se comporter déloyalement suite à un montant de 50 000 000 LBP seulement. Le législateur libanais doit prendre compte de ce déficit et imiter son homologue français en imposant une sanction proportionnelle aux bénéfices tirés de ce profit illicite.

Pis encore, le risque d'image et c'est le plus dangereux car il peut avoir des conséquences financières et économique sur l'entreprise et par suite mettre en cause la réputation sa réputation.

En plus des sanctions infligées par la CNIL, s'ajoute la procédure de mise en demeure, ce n'est pas une sanction mais une procédure qui est mise en place après une plainte ou un contrôle. La CNIL a le droit de demander au responsable du traitement d'arrêter une violation constatée au RGPD dans un fixe délai. Le délai de fixation varie entre 10 jours et 6 mois. En cas d'urgence le délai est de 24h pour se mettre en conformité.

[135] Jerome de Mercy, Quels sont les riques en cas de non conformité au RGPD, 4 Mars 2021 https://www.dastra.eu/fr/guide/risques-rgpd/495 date de la visite 28 Octobre 2022

A noter qu'en 2021, la CNIL a imposé près de 3.5 millions d'euros d'amendes pour la violation des législations du RGPD. Alors qu'en 2020, le montant a dépassé les 138 millions d'euros partagés entre 11 amendes.[136]

Revenant à l'année 2021, l'amende la plus élevée durant cette année a été infligée à l'AG2R La Mondiale et équivaut à 1.75 million d'euros. Cette dernière a violé (2) législations vitales du règlement à savoir la limitation des durées de conservation des données et la transmission d'informations à ses adhérents.[137]

[136] CNIL https://www.cnil.fr/fr/thematique/cnil/sanctions - Les sanctions

[137] Alice Vitard ,L'usine digitale, 3 Janvier 2022, en 2021, le total des sanctions inflligées par la CNIL avoisine 3.5 millions d'euros, https://www.usine-digitale.fr/editorial/en-2021-le-total-des-sanctions-infligees-par-la-cnil-avoisine-3-5-millions-d-euros.N1172692 date de la visite 15 Decembre 2022

Partie 2 : La banque digitale : un outil stratégique au service de la cybercriminalité

En intégrant les innovations électroniques technologiques dans leurs systèmes, les banques doivent fondamentalement renforcer leurs dispositifs en matière de sécurité, surtout après l'émergence de nouvelles techniques de cybercriminalité. Cela ne s'applique que si la banque a élaboré de nouvelles solutions et politiques dans la lutte contre cette affliction.

En fait, toute cette métamorphose implique un risque énorme sur la banque; celle – ci doit prévoir un cadre de sécurité plus élevé pour s'assurer de l'identité de son client et protéger ses renseignements confidentiels.

La digitalisation et la numérisation étant conçues comme un support incontournable d'une gigantesque quantité d'informations d'où l'importance de prendre certaines mesures lors de son utilisation notamment en terme de sécurité afin de protéger la banque de la criminalité bancaire. Ainsi s'avère l'importance d'éduquer le client et de le sensibiliser aux cyber crimes, aux sanctions qui y sont relatives, mais aussi à l'utilisation et à la gestion des services bancaires en ligne.

Dans ce cadre, nous exposerons l'utilisation abusive des services digitales dans la banque (titre 1) pour passer à l'importance d'installer un dispositif de cyber protection bancaire (titre 2).

Titre 1 – L’utilisation abusive des services digitales bancaires

Les cyberattaques font généralement référence à des activités criminelles menées via Internet.
En fait, La criminalité financière digitale, également appelée criminalité en col blanc, couvre un large éventail d'infractions pénales qui sont généralement de nature internationale car l'activité criminelle elle-même ne connaissent pas de frontières par nature. Ainsi, émerge la nécessite de renforcer l'application des réglementations en matière de cybercriminalité.

Dans le même sens se pose la question de l’étendu de la responsabilité pénale en matière de cybercriminalité vu que les cyber crimes sont commis dans le cyberspace ce qui évoquent le problème de l’extranéité et le principe de la territorialité, notion pertinente dans un espace ouvert sans frontière.

Afin de mieux comprendre ces notions, nous évoquerons la règlementation de la cybercriminalité bancaire (chapitre 1) et les conséquences de l’atteinte à la sécurité des opérations digitales (chapitre 2).

Chapitre 1: La règlementation de la cybercriminalité bancaire

Comme on a susmentionné, les établissements bancaires sont soumis à multiples lois et règlements qui encadrent partiellement ou totalement la gestion de leurs opérations. En effet, le cadre juridique qui règlemente les banques constitue un point de départ crucial pour protéger celui-ci contre toutes les formes de non-conformité légales et règlementaires des lois en vigueur.

Dans ce chapitre, nous exposerons le cadre législatif régissant le caractère multiforme de la cybercriminalité (section 1) et les actions criminelles découlant de l’abus de l’utilisation des banques digitales (section 2).

Section 1: Le cadre législatif régissant le caractère multiforme de la cybercriminalité

Le domaine bancaire est depuis longtemps soumis à une grande variété de législations pour combattre notamment les crimes qui pèsent considérablement sur la clientèle.

Avec l'utilisation intensive des techniques informatiques, les incidents de nature cyber se sont indéniablement accélérés. En effet, le risque de cybercriminalité est considérablement très supérieur dans le secteur bancaire s'étalant des sanctions pénales à la détérioration de l'image de la banque et d'autres conséquences néfastes.

Les législations qui encadrent la cybercriminalité diffèrent d'un pays a un autre. Nous verrons les principales législations à l'échelle internationale (P.1) et à l'échelle nationale (P.2).

P.1: Au niveau international

En ce qui concerne les principales règlementations en matière de cybercriminalité sur le plan international, on entamera les lois européennes (A), mais aussi les organisations européennes compétentes (B) qui font partie intégrante dans la règlementation de la cybercriminalité vue qu'elles jouissent du pouvoir d'imposer des sanctions en la matière.

A. Les Lois européennes relatives à la cybercriminalité

Le problème de la sécurité des systèmes informatiques des entreprises financières en générale et des banques en particulier constituent, de nos jours, une préoccupation majeure.

Du côté règlementaire, le risque lié à la cybercriminalité a été appréhender dans un cadre très large récemment après qu'en 2022, Dalloz a publié sa première édition du code de la cyber sécurité pour anticiper et répondre aux cyberattaques.

Ce code a exposé dans un livre premier la sécurité des systèmes d'information, la lutte contre la cybercriminalité dans un livre deuxième et enfin la cyberdéfense dans un livre

troisième. Ces sujets ont été traité selon les règles internes, les règles européennes et les règles internationales.[138]

En effet, il n'est pas question que les banques doivent se conformer aux exigences nationales et internationales relatives à la lutte contre la cybercriminalité par la mise en place d'un système de contrôle interne qui prend en considération la sécurité des systèmes d'information.

Dans ce sens, le règlement 97-02, daté 21 Février 1997[139], du comité de la règlementation bancaire et financière a donné une base juridique pour s'assurer de l'existence d'un programme de contrôle des systèmes d'information dans le secteur bancaire. Les provisions du règlement ont été par la suite enrichies suite à la directive CRD IV[140].

En France, à côté de ces exigences, les accords de 2006 de Bâle II, qui ont entré en vigueur avec l'arrêté du 20 Février 2007 ont introduit des exigences relatives aux risques opérationnels notamment les pertes relatives à la cybercriminalité et plus explicitement les cas de chute du système informatique et les cas de fraude portant atteinte au systèmes d'information.

Concernant les moyens de paiement et la monnaie électronique, des exigences très spécifiques en matière de sécurité ont été envisagé dans le but de limiter les risques de fraude dans ce sujet notamment la directive sur les services de paiement (DSP2).[141]

Le CPF a évoqué la problématique de la sécurité des technologies informatiques dans les articles 226-17 et 226-17-1 relatives aux atteintes aux droits de la personne résultant des

[138] Edouard Fernandez Bollo, Institution financière et cybercriminalité, Revue d'économie financière, 2015/4 N. 120 P. 181 – 198
[139] Règlement n° 97–04 du 21 février 1997 relatif aux normes de gestion applicables aux entreprises d'investissement autres que les sociétés de gestion de portefeuille
[140] Directive 2013/36/UE du Parlement européen et du Conseil européen du 26 juin 2013 concernant l'accès à l'activité et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, dite en anglais « CRD IV » (Capital Requirements Directive IV).
[141] Entrée en vigueur le 13 Janvier 2018, la directive comporte un ensemble de dispositions règlementaires visant à renforcer la sécurité des paiements, et relevant du champ de compétences de la Banque de France au niveau national.

fichiers ou traitements informatiques. La peine varie de 5 ans d'emprisonnement et de 300 000 € d'amende si la violation n'a pas été notifié à l'intéressé ou à la commission nationale de l'informatique et des libertés.[142]

Sur le champ international, la convention du conseil de l'Europe sur la cybercriminalité – convention de Budapest du 23 Novembre 2001, rédigée par le conseil de l'Europe, est le premier traité international qui envisage les crimes informatiques ainsi que les crimes sur internet.

Le deuxième protocole ajouté à la convention de cybercriminalité est relatif au renforcement de la coopération et divulgation de la preuve électronique et vise à répondre à toutes questions pénales en matière d'attaques contre les systèmes d'information ainsi qu'aux crimes impliquant des preuves électroniques, comme on verra ci-après.

Les réglementations précitées ne sont pas les seuls responsables d'empêcher la criminalité dans le monde cyber, des organisations spécialisées ont joué aussi un rôle primordial.

B. Les Organisations européennes compétentes en matière de cybercriminalité

Innombrables malfaiteurs bénéficient, de nos jours, de l'internet et sa vaste accessibilité pour se livrer aux activités criminelles qui représentent une réelle menace pour le monde entier et spécifiquement la clientèle bancaire vu la relation très spécifique entre le client et la banque et l'octroi de ce dernier d'information très confidentielles. Dans ce sens, plusieurs organisations internationales ont joué un rôle essentiel dans le domaine de la cybercriminalité.

L'Organisation International de Police Criminelle (International Criminal Police Organization ou INTERPOL) a mis en œuvre multiples dispositifs pour lutter contre la cybercriminalité, proposant des technologies de lutte innovante et une assistance aux pays dans le traitement des éléments de preuves électroniques. Aussi l'INTERPOL a joué un

[142] Voir CPF – Article 226-17 – 226-17-1

rôle dans la sensibilisation des personnes concernées à travers la réalisation de formations et la communication de renseignements dans ce domaine.[143]

Cette organisation relie les polices de divers pays suite à une gestion de plusieurs bases de données policières qui incluent des données sur les criminels et les infractions relatives, ce qui facilite la lutte contre la cybercriminalité.

Ajoutons à l'INTERPOL, le centre européen de lutte contre la cybercriminalité (EC3) qui a été établi par L'UE en 2020 à la Haye, dans le but de prévenir et combattre la cybercriminalité en Europe.

La création de ce centre a pour finalité principale la protection des citoyens contre les cybercriminels. Ainsi, il vise surtout les fraudes en ligne, les activités illicites menées par des criminels et spécialement les attaques conduites contre les activités financières et services bancaires. A côté de ce rôle, le centre s'occupe des recherches dans le domaine de la cybercriminalité et du traitement des données internationales dans ce domaine, ainsi que de l'analyse des rapports relatives aux menaces contre les systèmes d'information.[144]

Aussi, il est important de mentionner le rôle de la Task Force nationale de lutte contre les arnaques. Crée en 2020, à l'initiative du ministère de l'Economie et du Finance, cette structure vise à combattre, sanctionner et prévenir les pratiques frauduleuses tel que les arnaques, et les escroqueries.

Cette Task Force a publié en juillet 2022, un guide pour la prévention de l'escroquerie en ligne appelant à prendre toutes les mesures de vigilance contre ces types de fraude largement observées ces dernières années. Ainsi, le guide vient en réponse à l'utilisation accrue des outils numériques par les entreprises, les banques et la clientèle et traite les cyber arnaques associés essentiellement au vol de coordonnées bancaire, détournement de

[143] INTERPOL, www.interpol.int

[144] EC3, Le centre européen de lutte contre la cybercriminalité, 11 Février 2013, https://www.guidedetectives.fr/articles/ec3-le-centre-europeen-de-lutte-contre-la-cybercriminalite, 7 Novembre 2022

virement bancaire et fraudes par chèque en proposant les mesures de préventions associes.[145]

Après avoir exposer les principales réglementations et organisations spécialisées dans le domaine de la cybercriminalité sur le stade international. Nous entamerons le cadre législatif au Liban ainsi que les organisations spécialisées en la matière.

P.2 Au niveau national

A- Les Lois Libanaises relatives à la cybercriminalité

En raison de la croissance rapide des technologies de la communication et de l'information, qui ont positivement contribué au développement de la vie humaine, un aspect négatif de ces technologies s'est apparu ; L'émergence de nouveaux types d'atteintes aux droits et même de nouveaux crimes.

Malheureusement les lois et règlements en vigueur, sont restés déficients et absurdes dans le domaine du digital et par la suite les auteurs de ces atteintes impunis dans certains cas en raison de l'absence des moyens de dissuasion juridiques appropriés.

Pratiquement, beaucoup de textes du code pénal libanais peuvent être appliqués aux crimes électroniques, et plus particulièrement dans les crimes traditionnels qui se produisent par des moyens électroniques.

Citons l'article 281 du code pénal libanais qui puni d'emprisonnement quiconque qui pénètre ou tente de pénétrer un lieu interdit dans l'intention d'obtenir des choses, des documents ou des informations qui doivent rester étouffé pour la sécurité de l'État.

De même, les textes des articles 282 et 283 du code pénal punit quiconque qui vole ou détient des documents ou informations tels que ceux mentionnés à l'article 281 dans l'intention de les divulguer. Ces dites informations ou documents peuvent être enregistrés

[145] Selon le guide, les détournements de virement sont estimés à 157 millions d'euros de préjudice en 2020 d'après l'Observatoire de la sécurité des moyens de paiement, les escroqueries au chèque sont estimées à 538 millions d'euros de fraude au chèque en 2020 d'après le même Observatoire.

sur des bandes électroniques ou sur des disques utilisés à l'aide d'un ordinateur et peuvent donc être considérés un matériel criminel.

Il est également possible, à travers les dispositions du code pénal, de punir de nombreux crimes électroniques ayant lieu en publiant des documents, des photos ou en envoyant des e-mails sur internet ayant comme but d'affaiblir le sentiment national ou attiser les conflits racistes ou le sectarisme en temps de guerre (article 295 code pénal) ou contenir une diffamation ou un outrage à une personne de l'autorité publique (articles 383 à 389 code pénal) ou à une personne physique (articles 582 à 589 code pénal), ou une menace d'un crime ou d'un délit (articles 574 à 578 code pénale).

Notons que l'internet est aujourd'hui un réseau public qui peut être considéré comme l'un des moyens automatisés visés à l'article 209 du Code pénal.

De plus, le texte de l'article 635 code pénal et ce qui suit, incrimine les vols de tous genres effectués sur des ordinateurs physiques et leurs accessoires (hardware).

La falsification et l'utilisation de cartes de crédit bancaires électroniques peuvent également être punies sur la base des articles 454 et 471 du code pénal.

En outre, conformément à l'article 655 du code pénal, les infractions d'escroqueries peuvent être punies si des manœuvres frauduleuses ont eu lieu par voie électronique.

D'un autre côté, la loi sur la protection de la propriété littéraire et artistique N. 75 du 13 Avril 1999, est une réussite dans ce domaine, compte tenu que pour la première fois certains délits d'information sont punis par un texte explicite ; Ainsi, l'article 1 de cette loi a défini le programme informatique comme un ensemble de commandes exprimées en mots, phrases, symboles ou toute autre forme pouvant être lus lorsqu'ils entrent dans du matériel qu'un ordinateur peut lire, et capable de demander à l'ordinateur d'effectuer une tâche ou de donner un résultat.

L'article 1 définit également la question de la transmission d'informations au public qui peuvent faire l'objet d'une responsabilité s'ils portent sur des actes protégés et s'il a été réalisé par des moyens filaires ou sans fil et mis, par exemple, sur Internet.

Dans son article 2, la loi précitée a considéré parmi les œuvres couvertes par la protection

« Les programmes informatiques quelle que soit leur langue, y compris les travaux préparatoires. »

D'autre part, la loi 81/2018 a développé dans le titre (باب) 2 relatif au commerce et contrat électronique, chapitre (فصل) 3, les services financières et bancaires électroniques. Ce chapitre a compris (5) sections (جزء) ; les opérations liées aux paiement et transferts électroniques d'argent, les cartes bancaires, les monnaies électroniques et numériques et enfin les chèques électroniques et numériques.[146]

Le titre 6 de la loi précitée relatif aux infractions liées aux systèmes d'information, aux données informatiques et cartes bancaires et les règles de procédure relatives à la saisie et à la conservation des éléments de preuve informationnels énonce dans son chapitre 1 les crimes relatifs aux procédures et données informatiques.

Ainsi l'article 110 punit toute personne qui, dans l'intention de commettre une fraude, accède au système informatique en tout ou en partie. De même, si le but du criminel est d'entraver ou corrompre le système d'information. La punition s'accentue s'il résulte d'un tel fait la suppression, copie ou modification de données numériques ou de programmes d'information.

L'article 112 relatif à la violation de l'intégrité des données numériques, punit toute personne ayant introduit des données numériques dans un système d'information, avec l'intention de commettre une fraude, et toute personne ayant annulé ou modifié les données numériques incluses dans un système d'information.

L'article 113 punit aussi toute personne qui obstrue ou désactive intentionnellement, par quelque moyen que ce soit, l'accès au service ou l'accès aux appareils, programmes, sources de données ou information.

[146] Voir article 41 à 64 – Loi 81/2018

Dans le même sens, quiconque importe, produit, présente, dépose, cède ou publie, sans motif légitime, un appareil, un programme informatique ou des données d'équipement, dans le but de commettre l'un des délits précités est puni selon l'article 114.

Le chapitre (2) lié à la falsification et contrefaçon des cartes bancaires, de la monnaie et du chèque électronique et numérique stipule aux termes de l'article 116, l'incrimination de toute personne qui imite ou falsifie une carte bancaire, utilise une carte bancaire imitée ou falsifiée en connaissance de cause, falsifie la monnaie électronique ou numérique. La même punition s'applique en cas de cheque numérique ou électronique falsifié ou imitée.

Dans le même contexte, la loi 81/2018 a modifié l'article 453 du code pénal dans sa chapitre (5) lié à la falsification électronique en affirmant que « la falsification est une déformation délibérée de la vérité, dans les faits et les données, prouvée par un instrument, manuscrit, support papier ou électronique, ou tout autre support d'expression constituant un document, dans le but de causer un préjudice matériel, moral ou social. »

Après cette présentation, il nous apparaît claire que les lois libanaises en vigueur ne suffisent pas à criminaliser les infractions résultant du développement rapide des technologies de l'information et de la communication et n'englobent certainement pas de nombreux nouveaux types de crimes connus aujourd'hui sous le nom de cyber crimes.

B- Les Organisations Libanaises spécialisées en matière de cybercriminalité

En matière de cybercriminalité, la direction générale des forces de sécurité intérieure a annoncé que, conformément au développement technologique notamment dans le domaine de la TIC et au besoin urgent de sensibiliser les personnes aux menaces liés à l'internet, **le bureau de lutte contre les délits informatiques et de protection de la propriété intellectuelle**[147] a été créé en Mars 2006, affilié au Département spécial d'enquêtes criminelles dans l'unité de police judiciaire et travaillant sous la supervision du ministère public financier et du ministère public d'appel dans les gouvernorats.

[147] مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية

À cet égard, une décision récente a été rendue par la Cour de cassation libanaise, la neuvième chambre examinant une demande d'appel dans le procès des publications, 1/2014, dans laquelle cette cour a clarifié « l'identité et le rôle de ce bureau ».

Pour en revenir aux fonctions de ce bureau, il ressort clairement de son nom qu'il est chargé de lutter contre la cybercriminalité.

En effet, après cette révolution technologique, de nouveaux crimes basés sur l'exploitation des technologies ont vu le jour dans le but de commettre de nouveaux types de criminalités à l'exemple du vol des données personnelles ou d'autres connus mais par des techniques modernes comme le vol des mots de passe.

Le bureau entreprend également des missions de lutte contre les cyber crimes et les cyber-attaques mais aussi contre la fabrication et le commerce de CD illégaux. Il protège de même les productions intellectuelles, littéraires, artistiques et musicales, et lutte contre divers délits informatiques et enfin réfère les contrevenants aux autorités judiciaires compétentes.

Le bureau mène ses enquêtes soit sur la base d'informations privées, soit sur la base de plaintes de citoyens. Et il se déplace selon le signal du. النيابة العامة المختصة.[148]

La Direction générale des forces de sécurité intérieure (ISF) a comme mission aussi d'avertir les citoyens de ne pas être victimes d'actes d'extorsion, d'indécence ou d'exploitation via Internet, et de ne pas communiquer avec des inconnus par le biais des médias sociaux. En cas d'exposition à de tels actes, la victime doit contacter la Direction Générale des Forces de Sécurité Intérieure - le Bureau de Lutte contre les cyber crimes et de la Protection de la Propriété Intellectuelle - ou de porter plainte auprès de la personne compétente.

Dans ce sens, la BDL a mentionné dans son circulaire intermédiaire 605 daté du 23 Décembre 2021 l'obligation de se référer à la liste publiée par L'ISF en ce qui concerne

[148] هانيا محمد علي فقيه، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لواقع الحماية وتحديات العصر، دراسة منشورة في مجلة الحياة النيابية، المجلد المائة وخمسة، كانون الأول/ديسمبر ٢٠١٧، لبنان، ص ٧٨.

les noms inscrits sur la liste nationale associés aux personnes physiques, morales ou entités se livrant aux crimes financiers et au financement du terrorisme.

Il est important de noter aussi que l'ISF coopère toujours avec la Commission d'investigation spéciale (SIC) qui est une cellule de renseignement financier multifonctionnelle à statut judiciaire. C'est une plateforme de coopération internationale qui joue un rôle vital dans la protection du secteur bancaire contre les crimes illicites tel que les cyber crimes et le blanchiment d'argent.

La SIC reçoit les déclarations d'opérations suspectes (STR) et les demandes d'assistance pour enquêter sur les opérations bancaires soupçonnées et prendre à cet égard la décision adéquate, notamment les mesures de précaution spécifiques. [149]

Ainsi, elle possède le pouvoir d'exiger des personnes et parties concernées, publiques ou privées, qu'elles prennent les mesures nécessaires pour empêcher l'utilisation de biens mobiliers ou immobiliers appartenant à toutes dénominations désignées ou à désigner sur les listes nationales délivrées par les autorités libanaises compétentes tel que l'ISF ou toute autre liste qu'elle diffuse concernant le terrorisme et les actes illicites. [150]

Notant que les personnes et parties concernées, qu'elles soient publiques ou privées, doivent se conformer sans délai aux exigences de la SIC.

Section 2: Les actions criminelles découlant de l'abus de l'utilisation des banques digitales

Suite à la croissance du recours au numérique et l'augmentation des technologies du digital qui a donné place aux divers services et opérations électroniques notamment dans le secteur bancaire. Ces services sont malheureusement devenus de plus en plus vulnérables aux cyberattaques. Eventuellement, ces cyberattaques se sont transformés en des cyber crimes qui visent à nuire à la réputation de la banque, à un gain financier et à d'autres motifs.

[149] Special Investigation Commission, https://sic.gov.lb/en/about-us 8 November 2022
[150] Special Investigation Commission, Circular 25, national ML and TF risk assessment https://sic.gov.lb/en/laws-and-regulations/1 30 November 2022

Ces crimes commis peuvent êtres des crimes qui utilisent les tactiques novatrices de l'informatique (ordinateur, réseau...) (P.1) ou des crimes financiers visant les biens dans le but de gagner de l'argent d'une manière illégale (P.2).

P.1 Les différents types de cybercriminalités

On discutera ci-après les activités criminelles traditionnelles facilitées par la technologie (A) et les activités criminelles sophistiquées utilisant la technologie moderne (B).

A. Les activités criminelles traditionnelles facilitées par la technologie

Les crimes ayant lieu sur les opérations bancaires ne sont pas récentes. Cependant, avec l'augmentation de la technologie spécifiquement le « mobile Banking », les outils à l'aide desquels ces crimes sont commis se sont accentués.

Le chèque par exemple est connu comme un instrument de paiement très utilisé. Cependant, cet usage s'est reculé avec l'apparition des moyens de paiement électronique comme la carte et le virement bancaire.

Les fraudeurs peuvent fabriquer eux-mêmes de faux chèques en les falsifiant (modifier le bénéficiaire, la date, le montant.). Les criminels visent à tromper la banque en encaissant les chèques à l'aide de jeunes personnes vulnérables (appelés mules) séduites dans l'espoir de gagner facilement l'argent suite à cet encaissement ou par exemple faire croire à la victime qu'elle peut aider une association en encaissant le chèque à sa place[151], tout en invoquant son inaptitude pour l'encaisser pour des raisons fallacieux (nécessité d'être discrètes sur certaines opérations bancaires). Une fois encaissés sur son compte, la victime va restituer les fonds au criminel sous différentes formes comme le virement.

La deuxième directive européenne sur les services de paiement (DSP2) de 2019, stipule que les opérations par carte bancaire sont soumises à une authentification du payeur pour vérifier la légitimité de la transaction[152] et empêcher par la suite la fraude aux paiements

[151] Cabinet Phénix, qu'est-ce qu'un chèque falsifié, https://www.cabinetphenix.fr/quest-ce-quun-cheque-falsifie/ 12 Décembre 2022

[152] Protocole appelé 3-D Secure, deux éléments que seul le payeur peut mobiliser: il s'agit d'un élément de connaissance (mot de passe, code…), d'un élément de possession

en ligne par l'intermédiaire de la carte bancaire. La principale solution d'authentification est l'application mobile bancaire à l'aide de laquelle le client insère un code spécifique pour ses achats en ligne ou présente son empreinte biométrique au vendeur.

Le criminel, dans ce cas, va collecter des données à caractère personnel notamment en volant les coordonnées bancaires par des opérations frauduleuses comme l'attaque informatique. Suite à la récupération de ces données et coordonnées, le fraudeur aura un accès facile à la carte bancaire pour effectuer des achats ou retirer de l'argent.

Cette fraude peut avoir lieu aussi à l'aide de l'usurpation de l'identité de la banque. Dans ce dernier cas, le fraudeur utilise les données bancaires notamment le numéro mobile du client, il le contacte en usurpant l'identité de la banque[153] connue sous la technologie de « spoofing », prétendant être un employé de la banque, pour le faire confiance. Il va ainsi, par exemple prétendre demander des éléments spécifiques pour bloquer les tentatives de fraudes. Une fois la victime valide les opérations requises à travers les moyens d'authentifications forte, la fraude aura lieu.

Notant que l'usurpation d'identité moderne est dite usurpation numérique. Elle a lieu, en ligne, sur les sites web et les courriers électroniques à l'aide de la technique de « phishing » ou hameçonnage et se résume par le fait d'effectuer des opérations et des activités bancaires à l'insu du client.

On déduit qu'il est incontournable qu'il ne passe un peu de temps sans qu'un nouveau logiciel malveillant « malware » menace la clientèle bancaire d'aujourd'hui grâce à la technologie sophistiquée qui s'accroit très vite. Quels sont ces technologies sophistiquées et comment il s'adresse à la banque ?

(téléphone, clé USB, carte…) et/ou d'un élément biométrique (empreinte digitale, biométrie faciale…).

[153] L'article 264-4-1 du CPF stipule que Le délit d'usurpation d'identité suppose qu'il soit fait usage de l'identité d'un tiers en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération.

B. Les attaques criminelles informatiques utilisant la technologie sophistiquée

Ces attaques sont très avancées et évoluent constamment par rapport à d'autres attaques suite à la croissance et mutation technologique très rapide. Par exemple l'hameçonnage « phishing » consistant à frauder le client pour le pousser à communiquer ses données personnelles bancaires (le mot de passe, les cartes de crédit/débit et autres). Ainsi, il peut s'agir d'un message erroné, d'un appel téléphonique de la banque comme précité, d'un lien sur un faux site web entrepris par un hacker pour accéder d'une manière illégale aux comptes bancaires de la victime.

De même le rançongiciel est un logiciel malveillant qui infiltre l'ordinateur et prend en otage des données sensibles ou rend ses fichiers personnels inaccessible. Après avoir infecter l'ordinateur par la manière de chiffrement infecte des fichiers de l'utilisateur, il demande une rançon financière normalement en crypto monnaie en échange d'une clé qui permet de les déchiffrer. Le criminel peut même menacer le client de publier ses données personnelles ou de détruire ses fichiers s'il ne paye pas.[154]

Aussi, un nouvel type de fraude qui vise les banques effectuant des transferts de fonds est la fraude du courriel d'entreprise compromis. Ce nouveau type de fraude vise les entreprises qui effectuent les transferts de fonds ou celles qui ont des fournisseurs en dehors de leurs pays. Ce crime dépend largement de l'accès au courrier électroniques des directeurs exécutifs ou ceux responsable notamment du département de finance.

Cette technologie cible la création de courrier, géré par le cybercriminel qui ressemble aux courriers des personnes susmentionnées par la simple technique d'hameçonnage, ce qui permet au criminel de prendre l'identité du directeur exécutif par exemple dans le but de frauder l'employé pour autoriser des opérations financières normalement à l'étranger.

[154] Terranova security, qu'est-ce qu'un rancongiciel, https://terranovasecurity.com/fr/quest-ce-quun-rancongiciel/ date de la visite 14 Décembre 2022

Le cheval de Troie « Trojans » est un programme doué pour voler les informations bancaires sensible en ligne de la clientèle. Pour la première vue, le programme semble légitime, cependant, il jouit de la capacité de chiffrer, de manière inaperçue, les informations volées sur plusieurs comptes bancaires (mot de passe et autres) alors que cette dernière était transmise des ordinateurs infectés envers des serveurs spécifiques, rendant le système plus vulnérable à une future entrée.[155]

Le législateur libanais a stipulé le crime d'intimidation dans l'extrait du chapitre 2 relatif à « la prise de l'argent d'autrui » du code pénal dans la section liée aux crimes financiers.

La désignation commune de l'intimidation en France s'appelle le chantage.

Il est incontournable que l'un des effets négatifs de la digitalisation est sa contribution à la propagation de ce crime qui est devenu un phénomène qui soulève de multiples questions juridiques.

Sur le plan législatif, le législateur libanais a défini le chantage dans l'article 650 du code pénal : « le chantage est le fait de menacer une personne en exposant ou en divulguant des nouvelles la concernant si cela porterait atteinte à la dignité de cette personne ou son honneur, ou le sort ou l'honneur de l'un de ses proches, pour l'inciter à apporter un avantage illicite à l'auteur ou à autrui. »[156]

En reprenant le texte de l'article 578 code pénal libanais, nous constatons que le législateur a sanctionné la menace du seul fait de nuire à la personne quel que soit le but de l'acte lui-même tant qu'il affecte gravement la victime. Donc vu que le législateur a défini

[155] Kaspersky, Le cheval de Troie et les dégâts qui peut causer, https://www.kaspersky.fr/resource-center/threats/trojans date de la visite 16 Décembre 2022

[156] Ce texte ressemble au texte français qui définit le chantage dans l'article 312-10 du CPF, à l'exception que ledit article à spécifier la nature de l'avantage illicite requis par le criminel. « Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque ». (L'Art 312-10 du CPF, modifie par Ordonnance n. 2000-916 du Septembre 2000).

l'intimidation comme étant « un chantage », cela requiert une distinction entre l'intimidation et le chantage.

En conséquence, si le fait constitue une menace qui infligera un préjudice, l'acte est considéré une intimidation. Par contre, si l'auteur a l'intention d'apporter un bénéfice illégal dans son propre intérêt ou au profit d'autrui, l'acte est un chantage.

Notant que le législateur libanais n'a pas explicitement fait référence à l'intimidation électronique ou cyber harcèlement, mais l'article 650 code pénal relatif à l'intimidation n'a pas distingué entre un moyen et un autre pour le perpétrer. Ainsi, tous les moyens disponibles - y compris les moyens électroniques - sont autorisés dans ce domaine. La plus célèbre est le fait de porter atteinte à la victime à travers des messages harcelants pour l'intimider et le pousser à divulguer des informations sensibles.

Ces crimes précités sont très graves normalement et ouvrent la porte à multiples autres activités financières illégales commises contre les biens et constituant des crimes financiers.

P.2 Les formes de crimes financiers à l'ère digital

A l'ère des nouvelles solutions technologiques, les crimes financiers peuvent prendre différentes formes et se produisent surtout dans le secteur bancaire compte tenu que ce dernier est basé sur l'échange de la monnaie.

On étudiera principalement le cyber blanchiment d'argent (A) et d'autres crimes financiers résultant de la digitalisation. (B)

A. Le cyber blanchiment d'argent

Vu que le Liban a fait partie des 15 pays inclus sur la liste des pays non coopératifs en matière de lutte contre le blanchiment d'argent issu par le Groupe d'Action Financière (GAFI), le gouvernement libanais s'est pressé pour publier la loi 318/2001 du 10 Avril 2001 qui a été modifié par la loi 547 du 20 avril 2003. Cette dernière a modifié l'article 1 de la 318/2000, concernant les fonds illicites destinés au blanchiment d'argent.

Enfin, la plus récente loi régissant le blanchiment d'argent est la loi 44 daté du 24 Novembre 2015 relative à la lutte contre le blanchiment d'argent et la corruption, accompagnée de diverses circulaires et décisions de la BDL.

Selon l'article 2 de ladite loi, le blanchiment d'argent est tout acte commis dans le but de dissimuler la véritable source des fonds illicites ou donner, par quelque moyen que ce soit, une fausse justification concernant ladite source, tout en étant conscient du caractère illicite de ces fonds, ou bien transférer ou transporter des fonds, ou substituer ou investir ces derniers dans l'achat des biens mobiliers ou immobiliers ou dans la réalisation d'opérations financières aux fins de dissimuler ou déguiser la source illicite de ces fonds, ou aider une personne impliquée dans la commission de l'une quelconque des infractions qui constituent une infraction de blanchiment d'argent pour éviter les poursuites, bien que la personne est consciente du caractère illicite de ces fonds.

Malheureusement, la loi ne détaille pas spécifiquement les crimes résultant d'un accès illégal à un système informatique ayant comme but le blanchiment d'argent. Cette problématique demeure essentielle dans le cadre juridique des crimes sur l'internet et de la technologie avancée.

A son tour, la BDL a aussi publié des circulaires pour lutter contre le blanchiment d'argent dans les opérations financières, notamment la circulaire basique 83 du 18 Avril 2001 relatif au contrôle des opérations financières et bancaires dans la lutte contre le blanchiment d'argent et le financement du terrorisme.

Mais quelle est la relation entre les différentes formes de crimes sur internet et le blanchiment d'argent ? En effet, le principal motif des cybercriminels est le gain financier. Ce motif fait face à un défi majeur que confronte le criminel après chaque attaque réussie ; l'encaissement de l'argent sale volé sans pouvoir être détecter par la banque. En effet, Ces fonds illicites générés des crimes commis doivent bien sûr être réinjectés dans le secteur financier principalement pour être légitimement utiliser dans le marché.[157]

[157] Cybersouth project, situation report on cyber crime and money laundering on the Internet, in Lebanon, Novembre 2020

La principale méthode pour réussir ce but est les mules de transfert ou « money mules ».

Elle consiste à ouvrir multiples comptes bancaire qui vont recevoir les fonds illégitimes, avec des fausses ou vraies identités. Indirectement ces mules de transfert vont blanchir l'argent au nom de ces personnes qui ignorent ce qui se passe. Ces complices-victimes sont normalement vulnérables, repérés à l'aide des réseaux sociaux. Les criminels les promettent de gagner facilement de l'argent à condition d'ouvrir ces comptes. Face à cette tournure complexe, les fonds entrent dans un circuit sophistiqué, qui inclue multiples transferts entre comptes bancaires, pour brouiller leur trace.[158]

B. Autres cyber crimes financiers

Selon l'article 1 de la loi 44/2015, les fonds illicites comprennent les actifs corporels et incorporels, meubles et immeubles, y compris tout document ou instrument juridique attestant un titre ou un intérêt dans ledit actif résultant du fait de commettre ou de la tentative punissable de commettre ou de participer à des infractions spécifiques que ce soit au Liban ou à l'étranger.

Le blanchiment d'argent est une infraction distincte qui ne nécessite pas d'accusation auprès d'une infraction principale sous-jacente. La loi cite les infractions sous-jacents du blanchiment d'argent qui comprennent le terrorisme et le financement du terrorisme, et la fraude fiscale. Les criminels font largement recours à ces crimes spécifiquement puisque les TIC ont facilité largement leur commission.

Le terrorisme a fait l'objet de la loi 44/2015 susmentionnée. En effet l'ancienne loi 318/2000 comprenait des provisions consacrées uniquement pour la lutte contre le blanchiment d'argent, cependant la loi 44 est venue ajouter le terrorisme à la lutte contre le blanchiment d'argent.

[158] Mourad Karim, Suivez l'argent : comment les cybercriminels blanchissent le fruit de leurs vols à grande échelle 04 Septembre 2020, https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/suivez-largent-comment-les-cybercriminels-blanchissent-le-fruit-de-leurs-vols-a-grande-echelle/ date de la visite 10 Novembre 2022.

L’utilisation de l’internet pour des fins terroristes a augmenté durant les dernières années laissant une place à l’apparition d’une nouvelle terminologie ; le cyber terrorisme. En effet les terroristes utilisent de plus en plus l’internet et les TIC pour soutenir leurs actes terroristes. Cette utilisation est gérée de façon directe ou indirecte. Les fonds réinjectés dans le secteur bancaire seront ainsi utilisés pour financer les actes terroristes.

A l’aide de ces technologies, les terroristes utilisent les sites web pour demander au public de faire des dons. Ces sites peuvent contenir des enregistrements audio, des livres informatives pour inciter le public à s’engager dans ces organisations ou simplement une demande pour faire un don. Normalement, ces transferts interviennent à l’aide d’une carte de crédit ou par virement électronique. Ces terroristes peuvent utilisés tous les moyens précités dans le but de gagner de l’argent au services de leurs actes terroristes comme le vol des coordonnés et le vol de la carte de crédit.[159]

Encore, l’accessibilité d’une gigantesque quantité d’information dans le cyberspace, a permis d’abolir les frontières et les distances facilitant aux terroristes la planification de leurs attentats et actes terroristes.

La messagerie électronique a permis aussi de masquer les messages envoyés entre terroristes où l’expéditeur et le destinataire sont anonymes simplifiant ainsi toute sortes d’interaction.

Concernant la fraude fiscale, cette infraction est principalement régie par la loi 144 sur les procédures fiscales. En outre, la décision du ministre des Finances 2487/2019 du 30 Aout 2019 réitère que les mesures juridiques nécessaires seront prises, y compris le renforcement du secret bancaire, pour lutter strictement contre l'évasion fiscale.

L'évasion fiscale selon l’alinéa 1 de décision est définie comme volontairement s'abstenir de déclarer les impôts et taxes dus aux autorités qui résultent d'un revenu ou d'un patrimoine d'une personne, et ne pas payer les impôts et taxes qui doivent être déduits, collectés, annulés ou réduits illégalement par des méthodes illégitimes ; tel que l’enregistrement

[159] United Nations Office of Drugs and Crime, Utilisation de l’internet a des fins terroristes, NY, 2014

d'obligations financières fictives ou différentes de son objet réel ; l'utilisation de faux documents ; la démolition volontaire des pièces comptables avant la date requise par la loi ; le fait de pratiquer la déduction ou le remboursement d'impôt de manière illégale; le défaut d'émission de factures ou de documents similaires.

Signalons qu'en 2014, suite à la publication de la norme « Common Reporting Standard » (CRS) élaborée par l'Organisation de Coopération et de Développement (OCDE) visant à échanger automatiquement des information relative aux taxes entre les pays partenaires dans le but de lutter contre l'évasion fiscale[160], le Liban a issu la loi 55 daté 27 Octobre 2016, sur l'échange de renseignements fiscaux définissant l'échange de renseignements fiscaux et l'importance de cet échange sur le stade international.

Selon l'article 4, section 1, l'autorité compétente assiste l'État requérant conformément aux termes de la convention. Lorsque l'autorité compétente constate, suite à la réception d'une demande, que ce dernier respecte les dispositions de la convention conclue avec l'Etat concerné, l'Autorité compétente procède alors à la réponse à la demande conformément aux dispositions tant de ladite convention que de la présente loi.

Ainsi le CRS impose aux banques localisés dans un pays engagé dans le CRS d'identifier tous les clients non-résidents et de les déclarer par suite à l'administration fiscale nationale située dans le pays engagé dans le CRS. Dans notre cas c'est le ministère des finances (MOF).

Suite à la technologie numérique, les fraudes liées à l'évasion fiscale demeurent facile à exécuter avec les nouveaux techniques dans le monde cyber.

Les papiers « Pandora » par exemple sont la plus grande et récente mine de données offshore divulguées en 2021, exposant le secret des paradis fiscaux dans l'histoire.

[160] Société Générale, Comprendre le common Reporting Standard, https://www.societegenerale.com/fr/le-groupe-societe-generale/ethique-et-conformite/common-reporting-standard-crs 14 Nov. 2022

Il s'agit d'une série de fuites au cours des dernières années, suite à la « FinCen Files » (2020), les « Paradise Papers » (2017), les « Panama Papers » (2016) et « wikileaks » (2013).

En effet, Plus de 12 millions de documents ont été publié, le plus grand vidage de données, provenant de 14 offshore fournisseurs de services. La fuite, qui est à l'origine de plusieurs cyberattaques, a révélé les comptes bancaires, transactions secrètes et réseaux complexes de paradis fiscaux incriminant des politiciens et milliardaires bien connus et la façon dont ces derniers ont caché les argents et éludé les impôts de manière à ce que l'état ne pourrait pas les détecter[161].

Chapitre 2 : La spécificité des crimes commis dans le monde cyber en matière pénale

En tant que crimes commis par biais de l'internet dans le monde digital, ces derniers sont soumis, selon leur nature, à certaines procédures spécifiques en matière pénale, différentes des crimes commis hors internet.

Nous exposerons dans les sections qui suivent les moyens d'accusation et de poursuite dans ces types de crimes (section 1) et les procédures liées à la preuve électronique (section 2).

Section 1 : les moyens d'accusation et de poursuite

Tant que le droit applicable en matière de crimes commis par l'intermédiaire de l'internet est le droit pénal et spécifiquement les règles de la procédures pénale, il convient au Ministère Public d'Affaire النيابة العامة الاستئنافية avec l'assistance de la police judiciaire, الضابطة العدلية d'enquêter sur ces crimes dans un stade préliminaire, et référer les personnes impliquées devant la justice pénale compétente, le cas échéant, tout en reconnaissant le droit de la personne lésée d'acquérir la personnalité juridique, et réclamer son droit selon le droit applicable.

[161] Définition des papiers Pandora, 8 Octobre 2021, https://thepressfree.com/definition-des-papiers-pandora/ 14 Novembre 2022

En pratique, certaines problématiques se posent, notamment l'instance juridique compétente pour réclamer devant elle le crime, en d'autres termes le conflit de compétence (P.1) ainsi que la problématique des nouvelles compétences conférées à a des organes spécifiques dans ces types de crimes (P.2)

P.1 Le conflit de compétence dans les accords internationaux

Si les crimes ordinaires commis sur le territoire national ne pose aucun problème quant à la compétence des juridictions nationales pour incriminer le contrevenant, c'est pas du tout le cas en ce qui concerne les crimes cyber qui créent de nombreux problématiques concernant l'identification de la juridiction chargée de s'engager dans les procédures pénales requises dans de tels crimes contre les criminels surtout si ce crime était qualifié de transfrontière.

Ainsi, la justice pénale se trouve confrontée à d'innombrables graves problèmes étant donné que ces crimes vont au-delà des limites géographiques et critères traditionnels adoptées pour déterminer la compétence normalement.

Dans ce cadre, nous verrons les règles de la compétence juridique dans les accords internationaux (A) mais aussi les règles de la compétence juridique au niveau interne puisque ces crimes se heurtent à des obstacles procéduraux au niveau de la juridiction nationale applicable dans de tels crimes (B).

A- Les règles de compétence dans les accords internationaux

Les conventions internationales exigent que la compétence en matière de crime électronique appartienne au pays dans lequel le crime a été commis en tout ou en partie, ou dans lequel le crime a été réalisé, que ce soit sur le territoire de l'état partie, ou à bord d'un navire battant pavillon de l'État partie ou commis par un ressortissant de l'État partie si le crime est punissable selon le droit interne du lieu où il a été commis, ou si l'infraction ne relève de la compétence territoriale d'aucun état, de sorte qu'en se référant à la Convention de Budapest concernant la lutte contre la cybercriminalité.[162]

[162] مجلة مستقبل العلوم الاجتماعية، العدد الرابع، نيسان ٢٠٢١

On constate que la troisième partie, a consacré dans son article 22 la problématique de la compétence[163].

Cette problématique a aussi été évoqué dans la convention arabe sur la lutte contre les crimes liés aux technologies de l'information. Le Conseil des ministres arabes de la justice et de l'intérieur a approuvé cet accord dans sa réunion conjointe au siège du Secrétariat Général de la Ligue des États arabes convoqué en Egypte le 21 Décembre 2010. Ainsi le chapitre 4 a été consacré à la coopération juridique et judiciaire et spécifiquement l'article 30 a adressé la problématique de la compétence.[164]

Nous constatons que la jurisprudence pénale a abordé la question de la détermination de l'état compétent dans la poursuite des criminels, en s'appuyant sur deux critères, à savoir[165] :

Le premier critère : la loi la plus appropriée, c'est-à-dire la compétence du pouvoir judiciaire de l'État dont la loi est la plus vulnérable à la violation due à l'acte criminel, car les propriétaires de cette tendance dépendent de l'étendue des dommages résultant du cyber crime. Dans le cas où le crime s'étend pour inclure plus d'un pays, la disparité du ratio du dommage entre les états concernés doit être examiné et la compétence sera pour l'état le plus endommagé.

Le deuxième critère est le préjudice attendu : c'est-à-dire le préjudice causé par le crime commis sur internet peut avoir lieu dans n'importe quel pays connecté à l'internet, parce que la destination du préjudice n'est pas nécessairement précisée, ce qui peut nuire à de nombreux pays. Dans ce cas, nous sommes confrontés à une situation dans laquelle il est impossible d'appliquer les lois des pays victimes de l'incident, dans ce cas, la compétence appartient aux tribunaux du pays dans lequel le crime est commis.[166]

B- Le conflit de compétence au niveau interne

[163] Voir article 22 – Convention de Budapest

[164] Voir article 30 - convention arabe sur la lutte contre les crimes liés aux technologies de l'information

[165] الصغير، جميل عبد الباقي، ٢٠٠٢، أدلة الإثبات الجنائية والتكنولوجيا الحديثة، دار النهضة العربية، ط ١، القاهرة. ص. ٢٠٧

[166] حجازي، عبد الفتاح بيومي، ٢٠٠٩، الدليل الجنائي والتزوير في ج ا رئم الكمبيوتر والإنترنت، دراسة مقارنة، منشأة المعارف، ط ١، الإسكندرية، صفحة ٥٢.

La compétence régionale selon la législation pénale libanaise intervient lorsqu'un crime est commis sur le territoire libanais (Article 15 - Paragraphe 1 du Code Pénal)[167].

Le crime est considéré comme tel aussi si une personne a commise sur ce terrain les éléments qui le compose, ou un acte d'un crime indivisible, ou un acte primaire ou subsidiaire, ou si le résultat s'est produit sur ce terrain ou devait s'y produire (article 15 - deuxième alinéa – code pénal Libanais).

Dans le contexte des cyber crimes, il existe deux tendances différentes:

Après la publication de la loi 81/2018, le législateur est supposé être conscient de la non territorialité de ces moyens.

Selon le code pénal, le législateur libanais attribue la compétence personnelle à la législation pénale nationale pour tout crime commis à l'étranger tant qu'il affecte les intérêts essentiels de l'Etat[168] quel que soit la nationalité de l'auteur de l'infraction et la nature de sa participation au crime (auteur, co-auteur, instigateur ou intervenant).

Par conséquence, tout crime qui affecte, par exemple, la situation financière de l'État ou perturbe la sérénité entre les éléments de la nation ou autres commis par des moyens électroniques ou via l'internet, le code pénal libanais est compétent pour examiner l'affaire qui s'y rapporte.

Il en va de même pour la compétence personnelle, qui confère la compétence au code pénal libanais concernant tout libanais qui a commis un crime hors du territoire libanais.[169]

Il est utile de mentionner ici que le législateur ne requiert pas le contrevenant à retourner au Liban pour être poursuivi et jugé, comme il peut être juge par contumace (غيابياً).[170]

Cela justifie la prononciation de plusieurs jugements pénaux par la justice libanaise par contumace durant ces dernières années contre des personnes résidant ou présents dans d'autres pays selon les dispositions de la compétence réelle الذاتية ou personnelle الشخصية,

[167] Voir Art. 16 et 17 du CPL
[168] Voit Art. 19 du CPL
[169] Voir Art. 20 – 21 CPL
[170] سمير عالية وهيثم سمير عالية، الوسيط في شرح قانون العقوبات-القسم العام، الطبعة ٣٧٠-الأولى، مجد المؤسسة الجامعية للدارسات والنشر والتوزيع،٢٠١٠، ص ١٦٢

lorsque les conditions de chacun d'eux sont remplies à la suite de leur commission d'une infraction pénale commise dans le monde cyber.

P. 2 Les pouvoirs conférés à des organes spécifiques

L'augmentation rapide du pourcentage des crimes commis via internet a posé un nouveau défi aux autorités chargées d'enquêter sur ces crimes et de traquer leurs auteurs, ce qui a poussé la plupart des pays à créer des agences spécialisées pour faciliter la lutte contre ces crimes. Ainsi des organes spécifiques ont été formés jouissant d'une formation spécialisée prenant en considération la technologie et la complexité des crimes de ce type.[171]

Au Liban, cette tâche a été confiée au Bureau de lutte contre la cybercriminalité et de protection de la propriété intellectuelle qui exerce un rôle primordial dans la lutte contre la cybercriminalité (A).

Le processus de lutte contre la cybercriminalité n'a pas été limitée à la création d'un dispositif spécialisé

جهاز ضابطة عدلية متخصص، mais aussi le ministère public النيابة العامة a été conféré de nouveaux pouvoirs selon la loi 81/2018. (B)

A. La force du pouvoir conféré au bureau de la cybercriminalité et la protection de la propriété intellectuelle (مكتب مكافحة الجرائم الإلكترونية والملكية الفكرية)

Le bureau de la cybercriminalité et de la protection de la propriété intellectuelle a été créé conformément à la note publiée par la direction générale de la sécurité intérieure N.

[171] Dans l'Amérique, plusieurs organismes ont été crée pour lutter contre les crimes électroniques comme le WEB police et le centre de plainte contre la criminalité sur l'internet IC3 crée par la FBI. En France, c'est l'office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication – police nationale OCLCTIC responsable de tel crimes. Dans les pays arabes, il y a l'organisme responsable de la lutte contre les crimes des comptes et réseaux informatiques en Egypte, et une section spécialisée pour la lutte contre la criminalité informatique de la direction de sécurité en Jordanie, et le centre de lutte contre la cybercriminalité de la gendarmerie nationale en Algérie.

204/609 CH2 daté du 8 Mars 2006, annexée au Service Spécial de Recherches Criminelles de la Police Judiciaire.

En effet, la création de ce bureau contredit la loi 17 datée du 06 Septembre 1990 relative à la création du bureau de sécurité intérieure qui stipule dans son article (8) : « Est déterminé par un décret pris par le conseil des ministres, sur proposition du ministre de l'intérieur, après avis du conseil de direction : A- L'instauration des divisions et la détermination de leur appellation ». Ainsi l'illégitimité de la création de cet office soulève automatiquement des interrogations sur la légalité des tâches qu'il exerce.

Dans tous les cas, le bureau se déplace - conformément aux règles générales procédurales - sur le signal du ministère public, pour enquêter sur les crimes faisant l'objet d'une plainte et des rapports qui lui sont conférés dans ce cas. Ainsi , il commence ses investigations et convoque le suspect pour entendre ses paroles.[172]

Une fois l'investigation finie, le dossier est transmis au ministère public النيابة العامة qui prend sa décision de poursuivre l'affaire (en portant plainte devant l'autorité pénale compétente) ou de conserver le dossier.

Le rôle principal du bureau est d'apporter une assistance au ministère publicالنيابة العامة sur tous les aspects techniques informatique de l'affaire[173]. Ce bureau tire son autorité du fait que les crimes commis via l'internet ou dans le monde cyber sont des crimes électroniques faisant partie des crimes informatiques.

Notant les crimes informatiques inclus tout crime dans lequel la technologie avancée est le cible du crime, et tout crime dans lequel la haute technologie est un moyen de commettre le crime.[174]

---

[172] Voir articles 25, 27, 38, 40 et 47 modifiés par la loi 191 du 16 Octobre 2020 (visant à renforcer les garanties fondamentales et activer les droits de la défense) du CPL

[173] غيده فرنجية، مكتب مكافحة الجرائم المعلوماتية: رقابة غير منظمة على المساحات الإلكتروني مقال منشور على موقع مجلة "المفكرة القانونية في ٢٠١٣/١١/٣ -www.legal agenda.com date de la visite 16 Novembre 2022

[174] https://www.marchlebanon.org/wp-content/uploads/2020/03/know-your-Rights-1.pdf Date de la visite 16 Novembre 2022

Cependant, dans la pratique, le ministère public العامة النيابة ne se contente pas de confier au bureau de lui fournir ce qu'il a besoin d'expertise et d'information liés aux technologies informatiques utilisées pour commettre un crime, mais même il lui confère des plaintes des crimes commis sur internet pour s'engager dans une enquête pénale complète. Comme ses fonctions n'étaient pas clairement organisées législativement, ils ont dépassé les limites des pouvoirs de la police judiciaire organisésالضابطة العدلية dans le code de la procédure pénale et ce bureau s'est transformé en une autorité d'enquête, « d'accusation » et « d'exécution.[175]

B. Le pouvoir conféré au ministère public en matière de crimes électroniques

Le chapitre 7 de la loi 81/2018 lié aux règles de procédures relatives à la saisie et à la conservation des preuves informatiques a affirmé l'importance du pouvoir conféré au ministère public.

Selon l'article 121 « les règles mentionnées dans le présent chapitre doivent être suivies lors de la saisie des preuves informatiques sur la base de la décision du ministère public ou de l'autorité judiciaire compétente. »

Lors de la saisie des preuves informatique, le ministère public ou l'autorité judiciaire saisie de l'affaire peut décider que le téléchargement, le transfert ou la copie de données ou de programmes s'effectuent en présence de la personne concernée ou en présence d'une personne technique spécialisée en informatique désignée par cette personne en vertu d'une autorisation écrite.

Le cas échéant et aux termes de l'article 124, est scellé à la cire rouge, le lieu où se déroulent les opérations, ou le support électronique où se trouvent les données et les programmes, jusqu'à la présence de cette personne technique dans le délai imparti, et jusqu'à ce que le processus soit terminé dans les présence de deux proches de la personne concernée, de son représentant ou de deux témoins. Notant que la présence de toutes ces personnes peut être écartée sur décision de l'autorité judiciaire compétente.

[175] محمد علوش، رسالة لمكتب جرئم معلوماتية: أوقفوا مخالفة القانون أوعدّلوه، مقال منشور على موقع "النشرة www.elnashra.com le 11 Aout 2018. Date de la visite 16 Novembre 2022

Parmi les pouvoirs conférés au ministère public, ce dernier peut décider de suspendre des services électroniques, de bloquer des sites internet ou de bloquer temporairement des comptes sur ceux-ci pour une durée maximale de 30 jours, renouvelable une fois par décision motivée, sous réserve que l'effet de cette procédure s'expire du fait de l'expiration du délai prévu.

L'autorité judiciaire peut revenir sur sa décision si des circonstances nouvelles le justifient.

Le nouveau pouvoir du ministère public peut être défendu parce que c'est visible qu'il respecte l'élément de célérité que doit caractériser le déroulement des procédures dans les affaires liées à des crimes informatiques commis par voie électronique dans le monde cyber.

Ainsi, au lieu de confiner au juge d'instruction, au juge pénal ou au juge des référés cette autorité compte tenu qu'il est l'autorité compétente pour prendre des mesures pour supprimer l'atteinte manifeste et implicite aux droits impliquant un danger imminent ou dommage imminent[176], le ministère public prend ces mesures immédiatement lors de la phase d'enquête initiale, ce qui évite la pertes de temps qui se manifeste en référant le plaignant à la justice civile compétente pour prendre les mesures nécessaires, ou en attendant que l'affaire atteigne le stade de l'enquête initiale ou l'étape du procès.

Section 2 : Les procédures liées à la preuve électronique

Il ne fait aucun doute que l'objectif des poursuites pénales est de porter l'affaire au stade du procès et de prononcer un jugement qui condamne le contrevenant et le tient responsable de son acte criminel en lui infligeant la peine appropriée.

À cette fin, la phase d'enquête est centrée sur l'obtention de preuves prouvant l'imputation du crime à l'auteur. Ces preuves présentées doivent être suffisantes pour convaincre le juge de statuer équitablement sur l'affaire.

[176] علي مصباح إبراهيم، الوافي في أصول المحاكمات المدنية – الجزء الأول، الطبعة الأولى، الناشر غير مذكور، ٢٠١١ صفحة ٦٠-٦١

Dans le contexte des crimes commis par l'intermédiaire d'un moyen électronique ou dans le monde cyber tel que les cyber crimes, la nature de ces crimes affecte nécessairement la nature des preuves obtenues à partir de celle-ci, d'où un nouveau genre de preuve est apparu appelé "preuve électronique "ou encore "preuve numérique".

La jurisprudence a défini les preuves électroniques comme des preuves qui prennent la forme de champs magnétiques ou d'impulsions ou de l'énergie électrique qui peut être collectée et analysée à l'aide de programmes, d'applications et de technologies spéciaux. Elles constituent un composant numérique pour présenter des informations sous diverses formes telles que des textes écrits, des images, des sons et des graphiques qui peuvent être adopter devant les forces juridiques.[177]

On conclut de cette définition que les données existantes dans le monde cyber prennent la forme de nombres avec un codage spécifique. Ces symboles peuvent être transformé en contenu clair, en utilisant des moyens scientifiques.

Le législateur libanais a fait référence à ce type de preuve pénale en vertu de la loi 81/2018.

Le chapitre 7 du titre 6 à exposer les dispositions des « règles de procédure relatives à la saisie de la preuve informatique et sa conservation ».

Ainsi l'article 121 alinéa 1 a stipule : « Les traces informationnels, qui sont des preuves numériques ou informationnelles, sont des données que les gens laissent volontairement ou involontairement sur les systèmes, bases de données, services d'information et réseaux d'information. »

Devant l'énorme volume de données où résident les preuves informatiques, ainsi que son caractère invisible, non palpable ou non sensuelles,[178] il a fallu que le législateur tienne

[177] ممدوح عبد الحميد عبد المطلب، استخدام بروتوكولTCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على موقع، www.arablawinfo.com

[178] سامر أبو شقرا، الدليل الرقمي بين الضابطة العدلية والقضاء لبنان نموذج ، رسالة لنيل دبلوم الدارسات العليا في القانون الجزائي، الجامعة اللبنانية - كليّة الحقوق والعلوم السياسية والإدارية، الفرع الثاني ، ص ٦

compte de certaines considérations pour traiter ce type de preuve[179] en consacrant des principes régissant le processus de son obtention (P.1) facilitant les procédures particulières entreprises pour mener à bien le processus mentionné (P.2).

P.1 Les principes régissant l'acquisition de preuves électroniques

Du fait que le crime est commis par voie électronique ne signifie pas qu'il ne peut être prouvé qu'à l'aide des preuves électroniques. En fait, la preuve traditionnelle ne se limite pas aux crimes traditionnels et la preuve dans le pénal est libre. Ainsi nous discuterons dans ce qui suit les moyens de preuves récentes tel que présentées par la loi 81/2018.

Les articles 121 à 127 de la dite loi ont réglementé les conditions d'obtention de la preuve électronique mettant en relief 2 principes de bases régissant les procédures dans de tel cas spécifiques; le principe de la spécialisation (A) et le respect de la vie privée et des droits des parties de bonne foi. (B)

A- Le principe de la spécialisation مبدأ التخصص

Nous avons mentionné précédemment que le Liban est l'un des pays qui ont été créé en 2006 un bureau spécialisé dans la lutte contre les délits informatiques et la protection de la propriété intellectuelle, affilié au tribunal pénal spécial au sein de l'unité de police judiciaire, composé d'officiers et de personnel, y compris des opérateurs techniques spécialisé dans le domaine ou au moins ont suivi des formations intensives dans ce domaine.[180]

La jurisprudence libanaise avait précédemment confirmé que ce bureau est une section de la police judiciaire. Il travaille sous la tutelle des parquets de cassation, du parquet financier et des parquets d'appel dans les provinces.

Ainsi en réponse au motif d'appel relatif à la nullité de l'enquête préliminaire menée par ce bureau, se basant sur le fait que "le but de sa création est la nécessité de comprendre les

---

[180] هانيا الحلوه، الجرائم السيبارنية بين مشروع القانون الصادر بالمرسوم رقم ٢٠١٢/٩٣٤١ لنيل شهادة الدراسات العليا في القانون الجزائي، الجامعة اللبنانية – كلية الحقوق والعلوم السياسية والإدارية، الفرع الثاني، ٢٠١٧، ص ٧١؛

technologies de l'information qui sont utilisées dans le vol des cartes bancaires (...) et que son travail se limite à l'expertise technique et à la réalisation d'une enquête. » Le tribunal s'est appuyé sur l'article 37 du code de procédure pénale, qui stipulait :

Qu'il: "(...) assiste le Ministère Public et travaille sous son contrôle dans l'exercice des fonctions de la police judiciaire, chacun dans les limites de sa compétence stipulée dans la présente loi et dans les lois qui s'y rapportent, comme suit : (...) Assiste le Ministère Public et travaille sous sa direction dans l'exercice des fonctions de Police Judiciaire, dans les limites de leur compétence stipulées dans la présente loi et dans les lois qui s'y rapportent, les personnes comme suit : (...) 2- Le directeur général des forces de sécurité intérieure, les officiers des forces de sécurité intérieure, la police judiciaire et les sous-officiers travaillant dans les secteurs régionaux et chefs de postes de sécurité intérieure », pour conclure en affirmant le bien-fondé de l'enquête préliminaire menée par le bureau en tant que rattacher à la Cellule de Police Judiciaire[181]. Ainsi, toutes les plaintes comprenant des preuves électroniques pour être enquêter lui sont transmises, et les tribunaux lui envoient des preuves qui nécessitent un examen minutieux.

Avec la publication de la loi 81, le législateur a stipulé dans l'alinéa dernier de l'article 121, « Doit accompagner la police judiciaire dans la saisie et la conservation des preuves informatiques, un bureau spécialisé ». Dans ce contexte, l'organisme dont la formation et l'objectif sont compatibles avec les exigences requises dans de tels crimes commis par moyens électroniques est le bureau précité de "Lutte contre la cybercriminalité et la protection de la propriété intellectuelle".

Dans une étape ultérieure, selon la note de service émise par ISF N 246/204 daté le 01 Novembre 2016, le Service d'Investigation Scientifique s'est doté d'un laboratoire criminalistique numérique spécialisée dans le traitement et l'analyse des preuves numériques. De nouvelles branches ont été créées afin d'activer le traitement des preuves numériques, ces branches sont : Branche Informatiques - Branche Smartphones – Branche audios – Branche vidéos et images et branche diapositives électroniques.

[181] ت.ج، غ ٩، القرار رقم ١، تاريخ ٩ /١ ٢٠١٤ منشور على موقع المعلوماتية القانونية – الجامعة اللبنانية، date de la visite 17 Novembre 2022 www.legiliban.edu.ul.edu.lb

La mission de ce bureau est d'extraire et d'analyser les implications juridiques numériques qui existent dans tous les systèmes numériques.[182]

Dans un contexte connexe, nous mentionnons la « Branche technique de la Division de l'information » annexée à ISF, autorisée à analyser les communications numériques et le trafic de données dans les systèmes et à déterminer la localisation géographique.[183]

En pratique, tous ces organismes susmentionnés se soutiennent mutuellement dans le cadre d'une coopération mutuelle lorsque l'enquête nécessite de telle intervention, dans le but de s'assurer que les procédures nécessaires sont prises pour accéder aux preuves électroniques.

B. Le principe du respect de la vie privée et des droits des parties de bonne foie

Il est bien connu que les procédures de recherche de preuves sont en elles-mêmes des procédures qui pose la problématique du respect de la vie privée dans l'intérêt d'enquêter sur les criminels et de les traduire en justice. Mais cela ne signifie pas que le suspect est déchu de son droit, surtout dans la sphère cyber, où il a une vie privée parallèle à sa vie privée dans le monde réel.

En ce sens, il est nécessaire de concilier avec la nécessite de l'investigation et le droit à la vie privée consacré en faveur du suspect, en définissant le périmètre du champ d'information ciblé et en le limitant avec l'affaire pénale en question. Dans ce sens, l'article 121, alinéa 4 de la loi 81 a affirmé que « la vie privée doit être respectée en termes de preuves électronique, en particulier les données et images non liées à une affaire pénale."

Cependant, dans la pratique, one ne peut nier qu'il est difficile au moment de la distinction entre les informations pour déterminer ceux qui sont liés à l'affaire et ceux qui ne le sont pas, d'être conformes à ces principes vus que les fichiers sont généralement entrelacés sur l'appareil ou son logiciel, et qu'ils tombent tous sous l'œil vigilant ou sous les mains de l'enquêteur dès qu'il accède à l'appareil ou au logiciel où se trouvent les données.

[182] سامر أبو شقرا، الدليل الرقمي بين الضابطة العدلية والقضاء .لبنان نموذج، المرجع السابق، ص ١٢
[183] سامر أبو شقرا، الدليل الرقمي بين الضابطة العدلية والقضاء .لبنان نموذج، المرجع السابق، ص ١٣

Il appartient donc à la personne concernée d'adopter certaines normes qui respecte la vie privée tel qu'énoncé dans l'alinéa susmentionné, et de limiter l'atteinte au monde virtuel du suspect.

Parallèlement, le législateur n'a pas négligé l'importance de tenir compte des droits des parties de bonne foi et a de ce fait exigé dans l'alinéa 1, article 124 de prendre en considération les droits des personnes de bonne foi et les droits de la personne concernée en copiant les données et programmes saisis et sans saisir les matériels informatiques sur celles-ci surtout si ces dernières sont utilisées à d'autres fins légitimes.

P.2 Les procédures d'obtention de la preuve électronique

Le processus d'obtention de la preuve électronique diffère normalement des autres types de preuves vu sa spécificité et son caractère transfrontière.

Les alinéas (3) et (5) de l'article 121 de la loi 81/2018 stipulent respectivement :

- Les règles contenues dans le présent chapitre doivent être suivies lors de la saisie des preuves informatiques sur la base de la décision du ministère public ou du ministère public de l'autorité judiciaire compétente ;
- La police judiciaire exerce les procédures de saisie et de conservation des preuves informatiques prévues au présent chapitre sur décision de l'autorité judiciaire compétente.

Cela indique la consécration de nouvelles dispositions supplémentaires concernant les procédures de recherche relatives à l'obtention de la preuve et d'autres renouvelées concernant les procédures de saisie résultant de l'inspection.

Dans ce contexte, il convient de distinguer deux types de preuves numériques ou informatiques, conformément à l'article 123 de la loi 81/2018 :

- Les données disponibles sur un support électronique transférable tel qu'un CD-ROM ou un ordinateur sont soumises aux dispositions du code de procédure pénale relatives à l'inspection et à la saisie des preuves, notamment ses articles 33 et 41 sous réserve des autres dispositions contenues dans ce dernier à cet égard.

- Les données et les programmes en tant que composante morale du système informatique sont soumis aux dispositions de la loi 81 en ce qui concerne les procédures d'accès et de saisie qui s'appliquent dans le cas du crime sans témoin dans lequel la police judiciaire se déplace sous commande du ministère public, ainsi que le dans le cas du crime témoigné, où il est obligatoire que l'huissier de justice, qui se rend immédiatement sur le lieu de sa survenance et en informe le procureur de la république compétent, « maintient les traces, repères, preuves qui peuvent s'estomper, et tout ce qui aide à clarifier la vérité, y compris les preuves électroniques en prenant en considération la loi 81/2018 concernant les données personnelles.[184]

Dans un premier temps, nous aborderons les modalités de recherche de la preuve informatique (A), puis nous passerons à la présentation des procédures de saisie (B).

A. Les modalités de recherche de la preuve électronique

A l'instar du criminel qui laisse des traces physiques sur la scène du crime, ce dernier laisse aussi des traces sur la scène du crime dans le monde cyber, et ces traces sont les données qui représentent la preuve. La présence de ces données constitue l'objet de l'inspection, en d'autres termes, la source de la preuve numérique ou informatif.

Dans ce sens, le législateur libanais a énuméré dans l'alinéa 2 de l'article 121 de la loi 81, les sources de la preuve en affirmant que « Les preuves informatiques comprennent : les équipements informatiques, les programmes, les données, les applications, les traces informatiques et autres. »

Ici, une distinction peut être menée entre deux scènes de crime. Une scène virtuelle qui est le cyberspace et une autre réelle tangible représenté par les composants de la machine (ordinateur, smartphone...).

[184] Art. 41, Al. (2) CPL modifié par la loi 191/2020

D'autre part, toute donnée ou preuve numérique stockée dans un système informatique existant sur le terrain Libanais peut être saisi tant qu'il est possible d'y accéder depuis le système informatique à inspecter, selon l'alinéa (3) de l'article 124 de la loi 81/2018.

Ainsi, l'autorité judiciaire n'aura pas besoin d'obtenir un permis ou un nouveau mandat de perquisition auprès de l'autorité judiciaire compétente.

Il est également possible d'accéder aux données stockées dans un système informatique que ce soit à l'intérieur ou à l'extérieur du territoire Libanais, tant qu'il a été mis à la disposition du public ou en cas d'approbation de la personne légalement autorisée à générer ces données via un système d'information sur le territoire libanais.[185]

Notant que ces 2 cas ont été déterminés en vertu de l'article 32 de la convention approuvée par le Conseil européen du 23 Novembre 2001 lié à la cybercriminalité (Convention de Budapest)[186], dans le cadre de l'établissement d'une norme appropriée pour le principe de la souveraineté de l'État afin qu'il ne soit pas violé en permettant le piratage du système informatique à distance sans contrôle restreint.

En effet, nous estimons qu'il est très logique de ne mettre aucun obstacle à l'accès aux données lorsqu'il est facile et gratuit d'y accéder parce qu'elle est mise à la disposition du public ou parce que la personne qui a le pouvoir légal de le révéler a volontairement accepté de le faire.

Il reste à noter que l'autorité judiciaire peut « demander à toute personne disposant de données ou programmes pouvant faire l'objet d'une preuve informatique, d'en faire une copie et de la conserver auprès de lui jusqu'à ce qu'elles en soit saisi »[187] pour éviter toute tentative d'endommagement ou de modification.

L'un des modes de preuve utilisés devant les juridictions pénales, qui revêt une grande importance, est la preuve expertise. Elle consiste à se référer à une personne ayant une

[185] Voir Art. 124 Al. 4 de la loi 81/2018
[186] Convention de Budapest disponible sur https://rm.coe.int/budapest-convention-im-arabic/1680739173 -
[187] Voir Art. 124, Al. 8 de la loi 81/2018

compétence scientifique ou technique pour donner son avis dans son domaine d'expertise.[188]

Avec l'avancée de la technologie, le degré d'expertise dans le domaine des enquêtes criminelles s'est élevé. En effet, le processus de formation de la police judiciaire pour traiter les preuves informationnelles ou numériques et les schémas criminels innovant, ne signifie pas nécessairement que l'enquêteur est un expert dans tous les appareils et systèmes électroniques. En fait, il lui suffit de connaître les procédures à suivre sur la scène virtuelle pour sécuriser correctement les preuves[189].

Par conséquence, l'alinéa (7) de l'article 124 de la loi 81 stipule que « l'autorité juridique peut demander à toute personne ayant connaissance des méthodes de fonctionnement d'un système d'information ou des moyens de protection qui lui sont appliqués de fournir la personne en charge de l'enquête les informations nécessaires pour accéder aux données et aux programmes requises. »

En ce qui concerne la présence du criminel, l'article 33 du code de la procédure pénale impose sur le ministère public ou la police judiciaire[190], d'effectuer l'inspection en présence du suspect ou de l'accusé.

S'il a refusé de se présenter ou s'il s'est caché, l'inspection doit être effectuée en présence de son représentant et de deux membres majeurs de la famille ou deux témoins choisis par le Procureur de la République, sous peine d'annulation de la procédure de recherche.

En revenant à la loi 81, nous constatons que cette dernière n'a inclus aucune limitation dans le temps concernant l'obtention de la preuve informatique, ce qui nous revoit aux textes généraux à cet égard.

---

[188] نصر يواكيم فيلومين، أصول المحاكمات الجزائية، الطبعة الأولى، المؤسسة الحديثة للكتاب، ٢٠١٣ص. ٤٧٠.

[189] سامر أبو شقرا، الدليل الرقمي بين الضابطة العدلية والقضاء، مرجع سابق صفحة ٨٠-٨١

[190] Voir Art 47 Al. 2 CPL

En ce qui concerne le moment de la perquisition, l'alinéa 5 de l'article 33 du code de procédure pénale a déterminé ce moment, interdisant la pénétration dans les habitats pour la mener sauf entre 5h du matin et 8h du soir et sauf accord contraire du propriétaire, dans l'intérêt de réduire le champ de la violation de la liberté personnelle et de l'inviolabilité du domicile résultant de la perquisition.

Pour revenir à la loi 81/2018, on remarque que cette dernière n'a pas évoqué cette problématique, ce qui renvoie aux textes généraux à cet égard.

Cependant, dans notre avis, eu égard à la vulnérabilité de la preuve informatique aux tentatives de destruction ou de modification et la nécessité d'agir vite dans le stade de la perquisition, ce qui fait de la limitation de l'inspection à la date légale qui lui est fixée un obstacle au bon déroulement de celle-ci.[191]

Donc il est souhaitable de stipuler explicitement la non-restriction a un délai précis, dans le domaine de l'inspection dans les preuves électroniques.

B- Les procédures de saisie

La preuve informatique notamment les données et programmes se caractérisent par la possibilité de les reproduire de manière à ce que la copie soit identique à la preuve originale et ait la même valeur scientifique, selon la correspondance de la méthode de copie avec la méthode de création[192], aux fins de la soumettre à l'autorité judiciaire compétente, ce qui n'est pas disponible dans les preuves criminelles traditionnelles.[193]

En ce sens, l'alinéa 2 de l'article 123 de la loi 81/2018 a stipulé que « dans tous les cas, une copie originale des données et programmes doit être conservée telle qu'elle a été capturée dans le manuel numérique, des scellés sont apposés sur le support électronique sur lequel il est conservé, pour qu'elle soit ensuite déposée auprès de l'autorité judiciaire. »

---

[191] شهرزاد شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكملة لنيل شهادة الماسترفي الحقوق، جامعة العربي بن مهيدي أم البواقي– كلية الحقوق والعلوم السياسية - قسم الحقوق،.٢٠١٧ الجزائر ، ص ٣٩

[192] خالد خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩ ص ١٨١

[193] شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق، ص ١٦

L’alinéa 6 de l’article 124 a son tour affirme qu’on peut y accéder par une décision de l’autorité judiciaire qui a décidé de faire une copie des données et programmes informatiques saisis en faveur de la personne concernée.

On déduit que l’acceptation de la preuve est limitée sur (2) critères :

D'une part, il y a la fiabilité du système informatique, source de la preuve. L'article 124 alinéa 2 de la loi en a fait référence en stipulant que : « Lors de la saisie, en cas de téléchargement de données ou de preuves électroniques ou sa transmission à partir d'un site Web ou d’un ordinateur, ses sources doivent être indiquées. »

D'autre part, il y a le facteur responsable de sauvegarder des données ou des programmes et de ne pas les manipuler jusqu'à ce qu'ils soient exposés devant la justice.

Nous stressons ici sur la difficulté de se débarrasser des preuves numériques, car les données peuvent être récupérer après avoir été effacées, réparer après avoir été détruit, et révéler après avoir été caché[194].

Il révèle ainsi nécessaire que les personnes responsables aient le pouvoir de conserver ces preuves afin de préserver la validité et la fiabilité de la preuve numérique, pour que cette dernière ait une autorité de preuve suffisante au stade du procès.

Le procès المحضر est une déclaration écrite officielle qui doit être délivrée par l'huissier de justice pour documenter les procédures d'enquête prises en rapport avec un crime.

Ce procès reste impératif dans le cadre du contrôle des preuves électroniques, en effet, l’article 123 alinéa 1 de la loi 81/2018 a explicitement exigé l'établissement d'un procès pour chaque opération de saisie, ainsi que pour chaque processus de sauvegarde, d'analyse, de transfert ou autre d'une référence à une autre, à n’importe quelle preuve électronique.

Conformément aux dispositions du présent article, le procès doit comporter une présentation détaillée de toutes les procédures et actions effectuées; les autorités dont la preuve était en leur possession, la manière de transférer la preuve, notamment les

[194] شهرزاد حداد ، الدليل الإلكتروني في مجال الإثبات الجنائي، المرجع السابق ص. ١٥

procédures qui assurent son intégrité et qui empêche sa modification à partir du moment de sa saisie.

Ainsi, Le procès-verbal est organisé selon les normes précitées, puis déposé auprès de l'autorité judiciaire spécialisée.

Enfin, il est important de mentionner les effets de la violation des procédures de saisie qui ont été déterminé dans l'article 127 de la loi 81/2018 affirmant que « la preuve saisie ou conservée sera invalide dans le cas où elle viole les principes énoncés dans le présent chapitre. Par conséquence, les procédures d'enquête qui lui sont attribuées seront invalide aussi. »

Le deuxième alinéa ajoute que: « La nullité n'empêche pas à la prise des informations disponibles utiles pour l'investigation à la suite d'une saisie ou d'un traitement, si des preuves valides les soutenaient. »

Titre 2 – L'installation d'un dispositif de cyber protection bancaire

Dans l'usage courant, il est inévitable que la cybercriminalité dans le secteur bancaire constitue désormais une grande menace qui pèse lourdement sur le secteur financier et suscite de ce fait une attention élevée de la part des personnes concernées sur plusieurs niveaux.

En effet, les différentes formes de cyberattaques et les programmes informatiques massifs exploités à des fins malveillantes qui ont envahi le secteur économique ont amplifié les craintes dans ce secteur. Evidemment, les acteurs financiers craignaient le vol des données, les atteintes à la continuité de l'activité bancaire et d'autres conséquences graves que pourraient engendrés de tels actes.

Dans ce sens, s'avère nécessaire de développer un processus de lutte contre la cybercriminalité au sein des banques (chapitre 1) et de mettre en œuvre cette stratégie dans le monde réel ou en d'autre terme incarner un système de cyberdéfense bancaire (chapitre 2)

Chapitre 1 : Le processus de lutte contre la cybercriminalité bancaire

Garantir la sécurité des systèmes informatiques est au cœur de la lutte contre la cybercriminalité. Cet enjeu est majeur vu que le secteur bancaire joue le principal rôle dans le fonctionnement de l'économie au point que n'importe quel genre d'attaque peut endommager toutes les opérations du secteur.

Dans ce cadre, il est essentiel de comprendre les règlementations spécifiques qui régissent le domaine de la cyber sécurité dans les banques et répondent aux problématiques créer par cet environnement menaçant (Section 1) ainsi que les éléments essentiels qui ont renforcé la lutte contre la cybercriminalité dans les banques et ses différents impacts (Section 2).

Section 1 : Le cadre règlementaire régissant la cyber sécurité bancaire

On évoquera dans cette section les règlements relatifs à la lutte contre la cybercriminalité dans le code pénal et les conventions au niveau international (P.1) mais aussi au niveau national dans le cadre de la stratégie libanaise de cyber sécurité. (P.2)

P.1 Le cadre législatif de la lutte contre la cybercriminalité au niveau international

Au niveau international, comme on a déjà mentionné, les règlements et lois issues dans le domaine de la sécurité informatique ont augmenté progressivement depuis le milieu du XXème siècle, pour former de nos jours un cadre pénal stricte et conforme et contribuer à la publication du code de la cyber sécurité en 2022. Ce code qui a consacré le livre deuxième à la lutte contre la cybercriminalité a stipulé les règles internes, européennes et internationales relatifs à ce sujet.

Dans ce contexte, nous entamerons les règles européennes (A) et les règles internationales (B) qui ont consacré la problématique de la cyber sécurité.

A. Les règles européennes

Avant la publication récente du code de la cyber sécurité, la lutte contre la cybercriminalité a été abordée dans la loi informatique et liberté en 1978[195]. Ensuite, la loi Godfrain de 1988[196] a évoqué ce sujet mais a précisément parlé de la fraude informatique qui a permis de punir la suppression et la modification des données mais aussi les atteintes majeures aux systèmes informatiques.

Cependant, l'évolution constante et rapide des différentes formes de cybercriminalité suivie de la croissance de la technologie a encouragé le législateur a publié d'autres lois mais aussi revoir et compléter les lois anciennes par des jurisprudences pour mettre à jours

[195] Loi n.78-17 du 6 Janvier 1978 relative à l'information, aux fichiers et aux libertés
[196] Loi n. 88-19 du 5 Janvier 1988 relative à la fraude informatique

ces règlements à l'exemple de la loi 2001[197] relative à la sécurité quotidienne et la loi 2003[198] consacré à la sécurité intérieure. Aussi, les provisions relatives à la lutte contre le terrorisme et le vol des données évoquées dans la loi du 13 Novembre 2014[199] et la loi relative au renseignement[200].

Plus récemment, vu que les types des infractions commises ont évolué et les personnes visées par ces crimes ont aussi augmenté, le cadre juridique relatif à la cyber sécurité a subi des renouvellements constants et a évolué à son tour dans le but de s'adapter aux nouvelles formes de cyberattaques.

En effet, dans le nouveau code de la cyber sécurité, des dispositions générales liées au régime des peines, aux crimes et délits contre les personnes et les biens et contre la nation, l'Etat et la paix publique ont été stipulé dans le volet correspondant au code pénal.

Ces dispositions énumérés contiennent des lois relatives à l'escroquerie[201], on nomme la qualification de la fraude à la carte bancaire, le « skimmer », les manœuvres frauduleuses à distance ainsi que les sanctions relatives.

Aussi, le code a consacré une partie aux précisions techniques relatives à la professionnalisation du cyber crime, des ventes sur le « blackmarket » et des exemples sur le crypto virus et « ransomware » ainsi que des dispositions liées à la cyber association des malfaiteurs. Dans son dernier livre, le code traite les atteintes aux intérêts fondamentaux de la nation y compris le blanchiment et les actes de terrorisme.

Cette présentation non exhaustive des règlements européennes, met l'accent sur l'importance des divers règlements constituant le cadre juridique pénal dans la lutte contre la cybercriminalité et ses résultats atroces.

B. Les règles internationales

[197] Loi n 2001-1062 du 15 Novembre 2001 relative à la sécurité quotidienne
[198] Loi n 2003-239 du 18 Mars 2003 relative à la sécurité intérieure
[199] Loi n 2014-1353 du 13 Novembre 2014 relative à la lutte contre le terrorisme et le vol des données
[200] Loi n 2015-912 du 24 juillet 2015 relative au renseignement
[201] Code de la cybersécurité, Chapitre 3 de l'escroquerie et des infractions voisines

Dans le contexte international, la plus célèbre convention est la convention de Budapest du 23 Novembre 2001. Cette convention est considérée comme une loi type sur la lutte contre la cybercriminalité. C'est le premier traité au niveau international qui entame les crimes informatiques et les crimes de l'internet.

Cette convention a été rédigé par le conseil de l'Europe avec la participation active de plusieurs pays. Elle vise à combattre les cyber crimes et répondre aux enjeux de la cybercriminalité dans le monde.

Le Liban malheureusement n'a jusqu'aujourd'hui ratifié la convention. Cependant, la France a ratifié la loi no 2005-493 du 19 mai 2005 qui a autorisé l'approbation de ladite convention et ses deux protocoles additionnels à savoir le protocole additionnel à la convention sur la cybercriminalité du 28 Janvier 2003[202] et le protocole additionnel à la convention du 5 Avril 2022[203.] Jusqu'à nos jours 66 pays ont ratifié la convention.[204]

En effet, la convention a réussi à renforcer et à harmoniser le cadre législatif des pays relatif à la cybercriminalité et à améliorer la coopération des pays au niveau international surtout dans le cadre des enquêtes et poursuites liées aux cyber crimes[205].

De même qu'harmoniser les provisions du droit pénal concernant les infractions commises par le biais de l'informatique et les dispositions connexes dans le monde de la cybercriminalité en prévoyant les règles de procédures pénales dans le domaine de l'enquête et la poursuite.

Aussi, la convention facilite le recueil de preuves numériques relatives à des infractions qui ne sont pas commises dans le cyberspace.

---

[202] Protocole relatif à l'incrimination d'actes de nature racistes et xénophobe commis par le biais de systèmes informatique.
[203] Protocole relatif au renforcement de la coopération et de la divulgation de preuves électroniques.
[204] Augouard Marc Watin –Convention de Budapest, un deuxième protocole pour lutter contre la cybercriminalité https://incyber.org/convention-budapest-deuxieme-protocole-lutter-contre-cybercriminalite/ date de la visite 13 Décembre 2021
[205] Howard Solomon, La convention de Budapest sur la cybercriminalité a 20 ans, 11 Novembre 2021 https://www.directioninformatique.com/la-convention-de-budapest-sur-la-cybercriminalite-a-20-ans/90060 date de la visite 25 Novembre 2022.

En 2003, un protocole a été issue dans le but de compléter la convention en matière d'incrimination des actes de nature raciste et xénophobe, commis par le biais de systèmes informatiques. En 2022, le deuxième protocole additionnel à la convention a vu le jour, visant à moderniser la convention initiale pour être bien adapté aux défis contemporains liés à la croissance de la technologie et des crimes de l'internet.

Ce deuxième protocole a été issue vu l'importance croissante de la preuve numérique dans les faits criminels. Il ne concerne pas seulement les preuves dans les crimes cyber mais aussi toutes genres de preuves se présentant sous forme électronique.

Le protocole harmonise les éléments relatifs au droit pénal avec les dispositions liées aux infractions dans le domaine de la cybercriminalité notamment relatifs aux données et systèmes informatiques ou même des infractions qui implique des preuves numériques, mais qui ne sont commises à l'aide d'un système informatique.

Ainsi, le protocole conçoit les règles de procédures pénales vitales connexes aux enquêtes et aux poursuites et concernant les infractions qui visent les systèmes informatiques en trouvant un cadre solide pour l'obtention efficace des preuves numériques dans le cyberspace[206].

P.2 La stratégie nationale libanaise de cyber sécurité

Face à la mutation du cyberspace, l'évolution de ses usages et la croissance des cyberattaques sophistiquées, le Liban s'est trouvé face à un grand défi au milieu de cette transformation numérique.

Une stratégie nationale de cyber sécurité s'est ainsi imposée dans le but de sécuriser le cyberspace des utilisateurs et de diminuer les cyber risques qu'ils peuvent confrontés.

[206] InCyber, Convention de Budapest, Un deuxième protocole pour lutter contre la cybercriminalité https://incyber.org/convention-budapest-deuxieme-protocole-lutter-contre-cybercriminalite/, date de la visite, 31 Janvier 2023

Dans ce cadre, nous entamerons les efforts nationaux du Liban en matière de cyber sécurité (A) pour passer à la création d'une agence Nationale de la Cyber sécurité et des Systèmes d'Information (B).

A. Les efforts nationaux en matière de cyber sécurité

Comme nous avons déjà évoqué, le Liban n'a pas issue des lois protégeant les entreprises en général et les banques en particulier dans le monde numérique.

Cependant, le Liban a travaillé avec des organisations internationales comme l'INTERPOL et les organisations des nations unies et d'autres institutions européennes dans le but de renforcer la coopération internationale en matière de cyber sécurité.

Le pays aussi partage des informations avec des entités internationales sur les cyber crimes actuelles et naissante à travers la SIC.

Publié en 2009, la stratégie nationale de cyber sécurité a été conçue pour mettre en œuvre un cadre de défense contre les cyberattaques dans le but de protéger les entreprises du risque cyber et de protéger en même temps la vie privée des utilisateurs.

Ainsi, la stratégie a visé plusieurs objectifs qui doivent se transformer en actions opérationnelles dans le but de transformer le Liban en un pays capable de confronter les cyber crimes dans le monde numérique.

De même, elle a stressé sur le fait que le Liban doit appliquer un mécanisme rapide et efficace de notification dans la gestion des incidents et risques dans le cyberspace, développer les moyens techniques pour répondre à ces incidents majeurs et fournir une assistance aux organisations spécialisées dans le domaine de sécurité[207].

Ces incidents doivent ensuite être signalés rapidement à l'autorité nationale de la cyber sécurité pour évaluer la gravité des menaces.

[207] Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019, P 8-21

Selon cette stratégie, la cybercriminalité doit être mesurer en se référant à des statistiques fiables, et en établissant une base de données sur les cyber crimes pour pouvoir bien identifier les solutions convenables en matière de sécurité.

La stratégie a mis en relief le rôle que joue l'état pour faire réussir la stratégie vue que le gouvernement est responsable de protéger ses citoyens et leurs intérêts nationaux ainsi que leurs droits fondamentaux. Toutefois, lorsqu'il s'agit de la cyber sécurité, une collaboration bien équilibrée entre les différents organismes de l'état est primordiale pour lutter contre la cybercriminalité.

Dans un contexte diffèrent, la stratégie à insister sur l'importance de promouvoir la capacité éducative en matière de sécurité informatique par la mise en place de programmes spécialisés de haut niveau qui visent les personnes concernés dans le domaine de cyber sécurité.

En ce qui concerne le secteur bancaire, la stratégie a considéré que ce dernier est le plus important secteur dans l'économie libanaise. Ainsi, les organismes de règlementation de ce secteur sont un facteur essentiel de l'équipe responsable de la réglementation des lois en matière de cyber sécurité. Les banques doivent être indépendant concernant les décisions opérationnelles qui leur affectent. Ces décisions doivent êtres alignées avec la stratégie vue que le secteur bancaire travaille à la normalisation de la cyber sécurité, qui est un défi majeur pour ce dernier[208].

Dans le même sens, la loi 81/2018 a inclut diverses provisions affirmant la nécessité de sécuriser les opérations et transferts électroniques exécutés par le client.

Concernant les procédures de sécurité relatives aux paiements et transferts électroniques de fonds l'article 44 affirme que les banques doivent notifier le client, par écrit, avant 30 jours au moins dans le cas de la modification des conditions du contrat. Les banques doivent adopter un système technique leur permettant d'identifier l'émetteur de l'ordre de

[208] Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019, P.22-35

paiement ou de transfert électronique et de prouver que le client a transmis cet ordre à la banque.

Selon l'article 46, le client n'est responsable d'aucune opération exécutée sur son compte à la suite d'un transfert ou d'un paiement électronique s'il a notifié la banque, sans délai, durant les 90 jours qui suivent un tel acte de la possibilité d'autrui d'accéder à son compte sans autorisation ou de connaitre le mot de passe.

A son tour, la banque doit vérifier ces faits proclamés par le client et notifier ce dernier par écrit du résultat de l'audit entrepris par la banque. Dans tous les cas, il incombe à la banque de prouver le contraire de ce que le client a affirmé.

Dans le cas où l'une des conditions énumérées à l'article 46 précitée est réalisée, la banque doit entreprendre toutes les procédures convenables pour protéger le compte du client, de corriger la faute ou l'opération illégitime ou de compenser les pertes subies sur son compte.

Concernant les cartes bancaires, l'article 54 affirme que la banque doit fournir au client tous les moyens lui permettant de déclarer la perte de la carte ou son vol et d'empêcher toute utilisation de la carte une fois le client déclare sa perte ou son vol.

De sa part, le client doit prendre toutes les mesures de diligence pour protéger la carte et les informations d'identification lui permettant de l'utiliser.

B. L'agence Nationale de la cyber sécurité et des systèmes d'information (NCSIA)

Après la création du Bureau de la Police Judiciaire des Forces de Sécurité Intérieure (FSI) chargé de la cybercriminalité précitée ayant comme mission de lutter contre les crimes liés à la technologie, la cyber sécurité est devenu de plus en plus une préoccupation nationale vu que les cyberattaques ne cessent d'infliger de terribles dommages à la nation.

Face à ce danger, le Liban devrait mettre en œuvre un système national de défense contre cette technologie informatique.

Ainsi l'Agence Nationale de la Cyber sécurité et des Systèmes d'Information est une agence gouvernementale libanaise rattachée au Secretariat Général du Conseil Supérieur de la Défense, qui tire sa légitimité d'un mandat national définissant ses tâches.

La stratégie vise à centraliser l'ensemble des décisions prises au niveau des services étatiques dans le monde de la cyber sécurité renforçant ainsi la résilience du Liban aux risques numériques.

Elle met en œuvre les politiques et procédures du système libanais lié à l'informatique conformément à la stratégie nationale libanaise tout en évaluant les vulnérabilités et en identifiant les menaces[209].

La stratégie fournit également les bonnes pratiques et mécanismes technologiques en matière de cyber sécurité et crée un modèle libanais pour bien gérer les situations urgentes dans le monde numérique mais aussi offre un soutien dans le domaine du cyber terrorisme.

A côté de cette défense, la stratégie a un but préventif, elle construit un système de détection des incidents en réponse aux menaces confrontées et conduit des campagnes de sensibilisation à la cyber sécurité tout en offrant le soutient et les recommandations aux entreprises publiques et privées sur les cyber menaces.

Ses démarches préventives englobent aussi les mesures appropriées permettant aux particuliers et aux entreprises de notifier à l'agence la nature et l'origine de ces cyber menaces pour se protéger contre les cyberattaques.

Notons que la stratégie devra suivre l'évolution technologique dans le but de proposer les innovations requises en matière de cyber sécurité pour pouvoir réussir sa mission[210].

[209] Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019, P.42 - 44
[210] Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019, P. 45-46

D’un autre côté, il est incontournable que la construction d’un cadre juridique solide dans le domaine de la cyber sécurité nécessite que de tel agence soit expérimentée et collabore avec des agences internationales dans le cadre du respect de la constitution Libanaise.

Dans ce contexte, l’agence prépare le cadre normatif pour bien accueillir les services numériques et élabore les règlements en matière de cyberdéfenses pour protéger les systèmes d’information et réseaux informatiques.

De même, elle coordonne avec les homologues étrangers pour assurer la réussite des négociations internationales en matière de cyber sécurité.

Pour finir avec l’agence, cette dernière veille à protéger les informations qualifiées comme confidentielles et personnelles liées spécifiquement au gouvernement Libanais contre le cyber fraude et les cyberattaques. Compte tenu que c’est une agence gouvernementale, elle joue le rôle essentiel de facilitateur entre toutes les agences gouvernementales et les ministères concernés d’où l’importance de son rôle sur ce niveau[211].

Après avoir exposer la mission et le rôle essentiel que joue l’Agence Libanaise Nationale pour la cyber sécurité, on verra comment la crise sanitaire a renforcé l’importance de la cyber sécurité dans le monder numérique et comment les banques ont été affecté par le télétravail, une conséquence directe de la crise sanitaire.

Section 2: La lutte contre la cybercriminalité : un enjeu critique de survie des banques digitales

De nos jours, le secteur bancaire est confronté à une énorme explosion de logiciels malveillants dans un but d’exploiter les systèmes informatiques utilises par les banques. En effet, les cybercriminels visent en priorité les banques. Selon le rapport publié par Boston consulting group en 2021, les banques courent 300 fois plus de risques que les autres institutions financières d’être la cible d’une cyberattaque.

[211] Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019, P. 47-49

Ce défi s'est malheureusement accentué durant la pandémie de COVID 19, suite à l'accélération au recours aux programmes numériques et systèmes digitales pour faire face aux conséquences de la crise sanitaire en matière de continuation des services surtout dans les banques.

Dans cette optique, nous étudierons la prise de conscience de la cyber sécurité en réponse é la pandémie dans les banques (P.1) et la position du secteur bancaire dans le monde cyber dans la lutte contre la cybercriminalité (P.2)

P.1 Une prise de conscience de la cyber sécurité en 2019

La crise sanitaire a dû accélérer l'évolution des services bancaire utilisant des moyens numériques digitales. Ainsi, l'utilisation de la carte bancaire pour les achats en ligne a augmenté entraînant des transactions bancaires sans contact, de même pour le recours à l'ATM et d'autres moyens électroniques.

Ces usages accentués en réponse à la pandémie ont contribué à l'explosion des cyberattaques bancaires et risques relative à la cybercriminalité bancaire surtout pendant la période de confinement dans laquelle les gens étaient obligé de ne pas sortir de leur milieu pour des raisons sanitaires (A) ce qui a par la suite aboutit au renforcement des contrôles et mesures pour protéger la banque du risque cyber et lutter contre les fraudes et les cyberattaques (B).

A. Explosion des cyberattaques bancaires pendant le confinement

Publié le 28 juin 2021, La Banque de France souligne dans son rapport le rôle qu'a joué la crise sanitaire sur l'évolution grandissante de la cybercriminalité.

Elle affirme ainsi : "La crise sanitaire a accéléré l'exposition importante du secteur financier au risque cyber à travers un basculement massif et rapide des activités financières vers le télétravail et la prestation de services à distance."[212]

[212] Rapport de la banque de France, Évaluation des risques du système financier français, publié le 28 Juin 2021

Selon Moody's, l'agence de notation financière, le nombre de cyberattaques contre les institutions financières dans le monde a triplé entre Février et Avril 2020 (+238%).

En effet, dû aux conditions particulière du confinement les employés était forcés de travailler de leur maison afin de poursuivre les activités bancaires, cette accélération massive non anticipée du recours au télétravail a rendu les systèmes informatiques bancaires exploitables par les pirates selon Moody's.

Dans ce contexte, les clients ont eu recours largement à l'utilisation massive des moyens digitaux dans le but de se connecter à leur banque. Ces derniers devaient répondre aux problématiques confrontées par la clientèle mais ce sont trouvés mois vigilants face aux risques de cyberattaques.[213]

L'environnement dans lequel les banques évoluent a radicalement changé suite aux attaques dans le monde numérique. Selon le membre du comité exécutif de la Banque Centrale Européenne, Fabio Panetta, une entreprise sera attaquée par un logiciel de rançon toutes les 11 secondes d'ici 2021.

En effet, ce recours soudain au digital accompagné du développement technologique a constitué une base solide aux cybercriminels pour planifier leurs attaques.

Dans ce cadre, les clients des banques se sont tombés victimes de failles internes et d'hameçonnage ou « phishing », leur mot de passe était volé grâce aux faux SMS demandant un accès au compte bancaire[214]. Aussi, l'utilisation des applications mobiles bancaire était la source de plusieurs attaques, notamment l'exploitation des transactions à distance. Le secteur bancaire s'est présentée comme une cible de choix pour les pirates informatiques surtout les hackers et les programmes malveillants.

[213] MC2I, les banques face aux risques de cybersecurité en période de crise sanitaire, 18 Fevrier 2021, https://www.mc2i.fr/articles/les-banques-face-aux-risques-de-cybersecurite-en-periode-de-crise-sanitaire date de la visite 10 Janvier 2023

[214] Timothee Talbi, les cyberattaques contre les banques ont triplé pendant le confinement, publié dans les ECHOS, 15 Juillet 2020.

Les cybercriminels se sont infiltrés facilement dans le secteur et ont exploité suite aux attaques, les données personnelles sensibles de la clientèle à l'exemple des codes pin et des numéros de cartes bancaires qu'il utilisent régulièrement.[215]

Parmi les autres vulnérabilités, on peut nommer aussi, la possibilité de la distraction des employés qui travaillent en mode télétravail dû aux restrictions sanitaires, les systèmes informatiques non protégés et les menaces internes qui surgissent lors de l'utilisation des systèmes. Ces risques constituent une menace dommageable pour la fiabilité et la réputation du secteur.

Selon le rapport de la SIC publié en 2022, les cyber crimes commises entres les années 2017 et 2022 constituent le plus grand pourcentage (25%) de l'ensemble des crimes commises durant cet intervalle de temps tel que le terrorisme, la corruption, l'escroquerie etc. Durant l'année 2022, 39 cas de cyber crimes ont eu lieu dans le secteur bancaire libanais[216].

Cela a soulevé de plusieurs faiblesses face à la fraude bancaire en terme de sécurité nécessitant la mise en œuvre des meilleurs pratiques liées à la cyber sécurité.

Cette progression continue des différents types d'attaques a progressé son évolution après la pandémie de manière constante et de plus en plus sophistiquée dans l'infrastructure bancaire[217]. On ne peut nier que les systèmes gérés par les acteurs bancaires et les matériels utilisés sont légitimement accessibles aux employés et à la clientèle ce qui permet d'accroître le risque des cyberattaques.

La sécurité bancaire s'est avérée ainsi essentielle avec l'augmentation significative de la cybercriminalité à laquelle était exposé particulièrement le secteur bancaire depuis le début de la crise sanitaire.

---

[215] ITnation, La cyber sécurité dans les banques de demain: sécuriser le réseau de services numérique, 30 Aout 2021 https://itnation.lu/news/la-cybersecurite-dans-les-banques-de-demain-securiser-le-reseau-de-services-numeriques/ date de la visite 15 Janvier 2023

[216] Rapport publie par la SIC en 2022, https://sic.gov.lb/en/publications/10

[217] ITNationLa cyber sécurité dans les banques de demain: sécuriser le réseau de services numérique, réference précédente

On se demande ici, si les banques sont bien armées pour faire face à ces risques ?

En effet, les banques devaient dans une période courte et rapide renforcer les mesures de cyber sécurité pour faire face à ces nouveaux types de cybercriminalité dans le but d'éviter les perturbations et la perte de confiance dans le secteur.

B. Renforcement des contrôles et mesures au service de la cyber sécurité bancaire avec l'expansion du télétravail

Il est incontournable que le développement de la digitalisation a augmenté l'exposition des banques au risques cyber et avec l'avènement de la crise sanitaire, la situation s'est malheureusement aggravés.

Les mesures prises dans le domaine de la cyber sécurité se sont radicalement bouleversés durant les dernières années, sous l'impulsion de la crise sanitaire et le progrès de la technologie dans le secteur bancaire surtout que les cybercriminels tentent a amélioré toujours leur prouesse technologique pour contourner les mesures de cyber sécurité.

Si les méthodes des cybercriminels évoluent, la banque doit à son tour efficacement évoluer ses techniques pour faire face aux attaques.

En Europe par exemple, les banques ont développé des cadres de protection basés sur la AI. Cette dernière repose sur l'analyse des cyber incidents et le comportement des clients pour identifier leur rythme habituel d'utilisation des opérations bancaires[218]. Ainsi, une fois qu'un comportement suspect est déterminé par l'AI, une alarme est déclenchée pour permettre à la banque de contacter son client et s'assurer de la légitimité de l'opération.

Une autre façon de réduire les risques dans le monde cyber est celle relative au risque lié à la fraude sur la carte bancaire, les entreprises responsables de transmettre les données bancaires issus des cartes de paiement doivent se conformer à la règle PCI DSS.

[218] Cheshta mann, comment proteger son entreprise contre les cybermenaces, 22 mars 2023 https://www.cibc.com/fr/business/advice-centre/articles/how-to/safeguarding-your-business-from-cyber-attacks.html date de la visite 23 Mars 2023

Elle constitue un ensemble de normes qui visent à sécuriser les transactions bancaires et garantir que les données personnelles ne seront pas utilisés de manière abusive[219].

En effet, ces techniques incombent une tâche sur la banque de régulièrement détecter les menaces et vulnérabilités liés à la technologie surtout dans une période de crise vu que les attaques augmentent significativement dans un tel contexte.

Les banques se trouvent ainsi obliger de procéder à une amélioration continue des outils et méthodes qui leur permettent de lutter contre la cybercriminalité notamment la création des programmes informatiques relatives à la cyber sécurité.

En matière de cyber sécurité, pour faire face aux attaques de plus en plus virulentes, les banques doivent construire une stratégie stipulant les actions à entreprendre en cas d'attaques pour renforcer leur positionnement dans la lutte contre la cybercriminalité.

Une telle stratégie garantit la conformité de la banque aux règlementations internes et internationales, permet d'identifier rapidement les risques à grande échelle et contribue à une réussite dans la détection des fraudes.

Dans ce sens, l'Interpol a publié un document sur la cybercriminalité : impact du COVID 19. Elle souligne la nécessite de mettre en œuvre une stratégie de lutte contre la cybercriminalité en réponse à la pandémie, surtout qu'il y a une hausse constante de la cybercriminalité avec l'existence continue du télétravail et les vulnérabilités qui y sont relatives. Une telle stratégie vise à combattre efficacement les cyber menaces et protéger les personnes concernées contre la violation des données[220].

Signalons que l'instabilité de la situation économique générée par la pandémie multiplie les attaques dans le monde numérique. En parallèle, la grande dépendance de la technologie surtout dans le secteur bancaire renforce les attaques informatiques. Ainsi, il est nécessaire que les banques prennent toutes les mesures appropriées pour aider les acteurs bancaires et

[219] Pour plus d'information, veuillez voir https://www.expert-line.com/norme-pci-dss-obligatoire-sur-la-securite-bancaire/
[220] Interpol, la cybercriminalité : impact du COVID 19, Aout 2020

la clientèle à se préparer et être conscient des menaces et des moyens qu'utilisent les fraudeurs pour une meilleure résilience aux éventuels incidents.

P.2 La banque digitale : un maillon faible dans la lutte contre la cybercriminalité

Après avoir plongé dans la cyber sécurité en se basant sur un contexte qui reflète l'environnement dominant de nos jours et après cette remise en action de la notion relative à la lutte contre la cybercriminalité, nous dédions cette dernière partie de ce titre à l'exposition de l'impact de la cybercriminalité en cas d'échec de lutte programmée.

En effet, le Liban est en retard par rapport à l'échelle mondiale de la lutte contre la cybercriminalité et l'installation d'un dispositif fort de cyber sécurité bancaire.

Le pays est classé au rang 118 sur 164 selon l'indice mondial de cyber sécurité de l'Union internationale des télécommunications[221].

Malgré qu'intense effort ont été déployé, ces efforts sont éparpillés et ne se sont pas concentrés dans le secteur bancaire principalement d'où la nécessité de présenter l'impact de la faillite de lutte contre la cybercriminalité. Cette dernière aura un impact égale sur la banque en elle-même (A) ainsi que sur sa clientèle (B).

A. L'impact sur la banque

Selon le rapport publié par la FBI en 2021 relatif à la criminalité sur l'internet, 847 000 plaintes ont été déposées et 6,9 milliards de dollars de pertes ont été enregistrés en raison de la cybercriminalité dans le monde entier.

Précisément, entre Mars 2020 et Mars 2021, les attaques contre les institutions financières généralement ont augmenté de 38% dans le monde.

[221] Justin Babin, Cyber sécurité : "les systèmes d'information au Liban regorgent de données sensibles", alerte Lina Oueidat, 1 Mars 2019, Le commerce du Levant, https://www.lecommercedulevant.com/article/28913-cybersecurite-les-systemes-dinformation-au-liban-regorgent-de-donnees-sensibles-alerte-lina-oueidat date de la visite 24 Novembre 2022

Dans le milieu bancaire, la cybercriminalité constitue une menace pour la stabilité financière[222]. Grâce aux fortes interconnexions financières, et la digitalisation des activités bancaires, la cybercriminalité est devenu une menace pour les banques.

Dans son évaluation des risques majeurs du système financier français, issue le 10 Janvier 2022, la Banque de France présente la cybercriminalité comme l'un des principaux dangers pour les acteurs de la finance en 2022.

Nous constatons ainsi que l'une des conséquences financières majeures se traduit par le coût de la cybercriminalité qui est relativement très élevé. En effet, une seule attaque cyber au sein de la banque peut entraîner une pénétration frauduleuse au sein du système de sécurité bancaire qui peut aboutir à une fuite d'informations confidentielles et par la suite à un vol de fonds, constituant une atteinte réelle aux actifs de la banque.

Dans ce contexte et dans le but d'éviter la croissance des cyberattaques et leurs conséquences drastiques, la Banque Centrale Européenne (BCE) a développé en 2018 des tests d'intrusions dans les systèmes de l'informatique des banques[223]. Ces tests visent à identifier les lacunes majeures dans le secteur bancaire et bien préparer les employés pour être prêts à confronter de tels attaques.

Une conséquence très grave aussi est la mauvaise réputation de la banque. En effet, le risque d'image est un élément très dangereux dans la vie de la banque puisque la bonne réputation est basée sur la crédibilité ou la notoriété de la banque auprès du marché. Le risque d'un attaque cyber pourrait tenir la réputation de la banque et par suite ses perspectives et profits futurs[224].

A noter également que la cybercriminalité entraîne une paralysie des systèmes bancaires et par suite des opérations bancaires. A la suite d'un cyber attaque, la banque se trouvera alors

[222] Antonin Celine et Nadia, la cybercriminalité coute cher aux banques, https://variances.eu/?p=6431#:~:text=Le%20co%C3%BBt%20financier%20de%20la%20cybercriminalit%C3%A9&text=Elles%20entra%C3%AEnent%20des%20dommages%20li%C3%A9s,%C3%A0%20la%20fuite%20de%20donn%C3%A9es 11 Aout 2022, date de la visite 24 Novembre 2022
[223] Christoph Chloé, La cybercriminalite bancaire, référence précédente, P.18
[224] Christoph Chloé, La cybercriminalité bancaire, référence précédente, P.20

paralyser, ce qui conduit à un arrêt des activités bancaire quotidienne affectant directement le travail de la banque.

La banque n'est pas la seule affectée par ces attaques, le client à son tour est menacé par de tels risques et subit des pertes majeures.

B. L'impact sur le client bancaire

L'impact de la cybercriminalité sur la banque affecte directement le client bancaire. En effet, la relation banque - client demeure un enjeu essentiel pour les banques.

La gestion des avoirs des clients est le devoir de la banque. Ce dernier est donc obligé de préserver leurs fonds[225].

Une des conséquences grave de la cybercriminalité est le manque de confiance de la clientèle envers sa banque.

En fait, cette dernière compromet cette confiance établie entre la banque et son client puisque le client aura tendance a fermé son compte à la banque et ouvrir un autre compte dans une banque compétitive pour se sentir en sécurité.

L'enjeu pour les banques consiste à créer un climat de confiance pour sa clientèle suite à la mise en place de contrôles concrètes et à la communication transparente avec son client.

Une autre conséquence significative est la perte des informations personnelles sensibles des clients suite à un vol des coordonnées par exemple (état civil, adresse, numéro de téléphone…), ce qui laisse le client inquiet quant à la sécurité de ses argents. En effet, les données personnelles sont aujourd'hui protégées sous le RGPD et la violation de ce droit aboutit à des sanctions très élevés pour la banque menacée comme on a déjà précité mais aussi à ce que le client soit exposé à des crimes tel que le chantage par exemple ou le ransomware.

[225] BankObserver, Cyber sécurité: que craint réellement le client. 01 Juin 2017 https://www.bankobserver-wavestone.com/cybersecurite-craint-reellement-client/ date de la visite 24 Novembre 2022

Dans ce dernier cas, le criminel demande au client une rançon suite à la prise en otage des données sensibles. La banque serait ainsi obligée de payer une indemnité au client et de payer les honoraires de l'avocat et les frais de justice en cas de procès.

D'autre part le vol des données contribue à un sentiment de doute chez le client sur la capacité de sa banque de mettre en œuvre des systèmes de défense efficaces et opérationnels.

Il est important également d'ajouter un volet relatif au temps nécessaire pour que la banque traite les conséquences de l'attaque cyber surtout que certaines données impactées par le vol ne sont jamais récupérées ce qui peut aggraver la situation du client.

Toutes ces conséquences fatales de la cybercriminalité et les attaques informatiques sur le secteur bancaire ne sont qu'une preuve de la nécessité de mettre en œuvre une stratégie claire basée sur des objectifs, actions et ressources bien déterminée ainsi qu'une démarche méthodique et coopérative pour la réussir.

Chapitre 2 : La Cyberdéfense : Une mise en œuvre de la stratégie de lutte contre la cybercriminalité bancaire

Pour lutter efficacement contre la cybercriminalité face à la multiplication des cyberattaques, une stratégie de cyber protection et de sécurité bancaire est vitale au sein de la banque mais aussi la banque doit renforcer ses armées de contrôle internes. En effet, une telle stratégie de sauvegarde des systèmes informatiques rend le système bancaire plus capable de confronter ces risques.

Dans ce contexte, on verra le processus de prévention, de détection et de correction relatif aux cybercriminalités dans le secteur bancaire (section 1) pour développer la nécessité du renforcement de certains contrôles au niveau de la banque (section 2).

Section 1: Un processus de prévention, de détection et de correction relatif aux cybercriminalités dans les banques digitales

Avec l'essor de la banque digitale, le processus de prévention, de détection et de correction des cyber crimes a connu une ampleur rapide vu la nécessité accrue d'identifier les risques qui s'adaptent rapidement avec l'évolution de la technologie. Ainsi les banques doivent continuellement se tenir à jour dans toutes les matières relatives aux cybercriminalités.

Dans ce sens, L'ISF a intégré dans son livret différents modalités de défense contre les cyber crimes bancaires (P.1). Cependant cette défense ne peut réussir sans une solide politique de gouvernance intégrée dans la culture de la banque et dédié à la sécurité des systèmes informatique mais aussi à la protection contre les cyberattaques (P.2).

P.1 Le modèle Libanais de cyberdéfense selon L'ISF

Comme nous l'avons déjà mentionné, au niveau national, l'ISF a publié le livret de sensibilisation aux cyber menaces. En terme de lutte contre la cybercriminalité, ce livret propose des modalités de prévention contre les cyber crimes (A) et des modalités de traitement des cyber crimes bancaires (B). Ces modalités contiennent des dispositions spécifiques au secteur bancaire qu'on verra dans ce qui suit.

A- Les modalités de prévention contre les cyber crimes bancaires

L'ISF a consacré dans son manuel une section liée aux mesures de protection des transactions électroniques et financières sous l'égide de la prévention des cyber crimes bancaires.

Ainsi, elle a énuméré une liste de mesures qui aident les clients à préserver leurs fonds dans la banques et l'intégrité de leur carte de crédit mais aussi protéger leur transactions financières conduites sur l'internet.

Tout d'abord, le client bancaire doit faire preuve de prudence et de vigilance. Compte tenu que la création et la gestion du mot de passe sont devenu un art, le client doit bien choisir

le mot de passe qui lui donne accès à son compte bancaire surtout que la plupart des opérations de nos jours ont lieu par la voie « e-banking » [226].

Ainsi, le mot de passe doit être conforme au prototype suggéré de mot de passe à l'exemple de l'utilisation des nombres, des symboles et des caractères spéciaux. Surtout éviter les mots de passe qui contiennent les informations personnelles comme le prénom, le numéro de téléphone, l'adresse et ne jamais utiliser le même mot de passe pour tous les comptes compte tenu que normalement le client possède plusieurs comptes dans sa banque.

De même, Le client doit périodiquement changer son mot de passe et choisir un nouveau totalement diffèrent de l'ancien surtout en cas de suspicion de piratage et ne jamais l'insérez devant une personne étrangère.

Concernant les transactions bancaires électroniques, l'utilisateur doit s'assurer que les opérations bancaires électroniques sont dotés de logiciels qui combattent le virus comme les programmes anti-virus.

Il ne doit jamais divulguer les détails du compte ou de la carte bancaire vue que ces informations si révélées peuvent être facilement voler. Ainsi, le client doit être très attentif quant au partage de ces détails surtout le mot de passe (PIN) et le One Time Password (OTP) [227]. En fait, le livret insiste sur le fait que l'employé de la banque ne demandera jamais ses informations confidentielles.

Concernant l'utilisation de l'ATM, le PIN code doit être bien caché lorsque le client le tape. Alors que pour la carte bancaire, ce dernier doit toujours couper les cartes périmées en morceaux très petites pour que la bande magnétique soit définitivement détruite[228].

[226] ISF, livret de sensibilisation aux cybercmenaces, P.14 - 22
[227] ISF, livret de sensibilisation aux cybercmenaces, p. 25
[228] Norton Life Lock, 5 pratiques sur Internet qui peuvent vous exposer à la cybercriminalité, 2021, https://fr.norton.com/blog/online-scams/5-online-habits-that-could-expose-you-to-cybercrime-are-you-doing-them date de la visite 10 Decembre 2022

Il est important de noter ici que le client doit revoir toujours ses comptes bancaires pour s'assurer de la véracité des transactions exécutées sur le compte par exemple l'exactitude des montants de transferts d'argent.

A son tour, l'employé doit vérifier tout paiement qui dépasse une certaine limite placée par la banque et ne jamais répondre à un email qui demandent des informations confidentielles sur le client ou qui demande un transfert avant de s'assurer par un appel téléphonique que c'est le client lui-même qui ordonne la demande[229].

Dans le même sens, le client ne doit pas répondre à des messageries qui prétendent prévenir de la banque demandant des numéros confidentiels tel que les numéros d'identification personnels ou les numéros d'identification fiscales.

Concernant les mesures de protection contre la fraude financière par email (Business Email Compromis), le livret insiste sur l'importance d'analyser les messages électroniques surtout les demandes de virements de comptes et tout comportement inhabituelle du client par email.

L'employé doit vérifier minutieusement le courriel de l'expéditeur par exemple les emails qui comportent des fautes d'orthographes, les demandes de modification aux modes de paiements ou n'importe quel changement dans les détails de paiement[230].

Enfin, le client doit éviter toute opération s'il est connecté à un réseau public ou sur des sites n'utilisant pas le protocole préventif http, le site doit être fiable et le réseau doit être privé.

On déduit ainsi que la prévention contre la cybercriminalité est un devoir et une obligation qui nécessite une coopération mutuelle entre le client et la banque pour réussir cette protection.

Si le client ne prend pas en compte ces mesures préventives, ce dernier sera évidemment exposé au de tels crimes. Alors comment ce dernier doit il agir dans ce cas ?

[229] ISF, livret de sensibilisation aux cybercmenaces, P. 44
[230] ISF, livret de sensibilisation aux cybercmenaces, P. 45

B- Les modalités de traitement des cyber crimes bancaires

Le livret stipule qu'en cas de perte, de vol ou de piratage de la carte de crédit ou même de son utilisation sans le consentement de la personne concernée, le client doit contacter directement le service clientèle puisque la banque est en charge de l'émission de la carte. Cette dernière doit immédiatement suspendre la carte et la remplacer par une autre (nouveau code, nouveau PIN) et surtout prendre les mesures de sécurité et de diligence nécessaire.

Parallèlement, le client doit accéder à son propre compte pour s'assurer qu'aucune opération illégitime n'a été exécuté sur ce dernier y inclut des frais inhabituels ou des coûts supplémentaires. Dans l'affirmative, la banque doit être informée pour essayer de récupérer l'argent[231].

Dans le cas où la carte qui est perdue, volée ou piratée est utilisée sur des sites d'achat (e-commerce), le client doit mettre à jour ses comptes bancaires sur ces sites.

En cas de fraude bancaire sur internet, la victime doit signaler directement à la banque – le département concernée par les opérations frauduleuses – pour prendre les mesures nécessaires et directement changer le mot de passe du compte bancaire ou de l'application mobile.

La victime doit aussi enregistrer la date et l'heure de la découverte de cette opération ainsi que toute autre information qui peut se révéler pertinente dans l'enquête[232].

La victime doit pouvoir estimer les pertes encourues et les pertes potentielle pour demander les dommages et intérêts.

Enfin, le client doit identifier toutes les preuves liées directement à l'opération à l'exemple de la fracture et de l'ordre de l'achat.

[231] ISF, livret de sensibilisation aux cybercmenaces, P. 47
[232] Glenny Misha, Cyber arnaques, comment les hackers piratent vos cartes bancaires, 10 Janvier 2013

Dans le cas d'infection par un « malware » – logiciel malveillant – l'employé doit mettre en œuvre le programme anti-virus pour effacer ces infections, le cas échéant, il doit installer un autre programme fiable d'où l'importance que les programmes installés sur les ordinateurs de la banque soient originaux et mises à jour[233]. L'employé ou le client peut aussi transférer les informations sur un disque interne ou même une USB et enfin formater l'ordinateur infecté.

Selon une étude menée en France en février 2022, cette dernière a le taux d'attaques par ransomware le plus grand dans le monde entier. 81 % des industries interrogées dans l'étude ont malheureusement été confrontées à au moins une infection par rançongiciel.

En effet, une infection de l'ordinateur de la banque par le logiciel du « ransomware » engendre beaucoup de risques. Ainsi, il est important que l'employé n'exécute pas les instructions des hackers et de notifier le département responsable tout de suite car la récupération des données n'est pas garantie vue que le but du criminel est seulement de gagner de l'argent[234].

Dans ce cas le département doit déterminer le type du virus qui peut être un virus de cryptage des fichiers pour accéder aux données personnelles des clients et prendre les mesures correctives selon la procédure entamée par la banque dans de tels situations.

Enfin, il est primordiale de mentionner que la banque ou même le client peuvent solliciter l'assistance des Forces de Sécurité Intérieure qui possèdent la capabilité de résoudre le problème[235].

[233] ISF, livret de sensibilisation aux cybercmenaces, P. 53-54
[234] Rocoveo, Livre blanc, Cyberattaques par ransomware
[235] Le signal aux Forces de Securite Interieure s'effectue par l'un des moyens suivant : Bureau de la lutte contre la cybercriminalité et de Protection de la Propriété Intellectuelle: +961 1 293293 ou à l'aide Service " بلغ " Sur le site des Forces de Sécurité Intérieure : www.isf.gov.lb

P.2 La nécessité de conformité entre les bonnes pratiques en matière de gouvernance et la cyberdéfense comme moyen de prévention

Face aux cyber menaces en constante progression, la coopération entre les différents acteurs de la banque est plus que jamais indispensable pour renforcer le processus de prévention. Cette coopération est à la base de la bonne gouvernance qui revêt aujourd'hui une valeur stratégique plus que jamais. La période de crise qu'a vécu le monde entier a renforcé à son tour le principe de l'autoregulation.

On veut dire par autorégulation, le processus qui implique le respect par les acteurs concernes des principales règles formulées par eux-mêmes et dont ils assurent la bonne application (à l'exemple du code de conduite et du code des bonne pratiques)[236]. Notant que ces bonnes pratiques seront modifiées périodiquement eu égard a l'évolution rapide de la technologie.

On songe tout particulierement aux défis divers posés par les cyber crimes qui requiert des réponses rapides et multiples rassemblant tous les responsables acteurs de la banque afin de répondre principalement aux enjeux de la gouvernance de la cyber sécurité et lutter d'une manière efficace contre ce développement accéléré des actes cyber et de l'utilisation malveillante de l'internet.

C'est dans ce contexte qu'une action énergique était vitale pour promouvoir à la banque un cyberspace plus stable.

Nous entamerons dans ce sens les différents concepts de la gouvernance classique qui affecte surtout la performance des banques (A) pour découvrir comment ce principe de la gouvernance a évolué dans la transformation digitale suite aux progressions informatiques et technologiques. (B)

A- Une corrélation entre la gouvernance et la performance des banques

[236] B. Du Marais "Regulation de l'internet: des faux semblant du retour a la realité", revue francaise administration publique 2004/1, n. 109, P 83

En Septembre 1999, le document consacré à la gouvernance des banques a été publié par la comite de Bale «Enhancing Corporate Governance for Banking Organisations »[237] y compris des recommandations sur plusieurs sujets tel que la transparence et le rôles des auditeurs internes et externes.

Au Liban, le concept de la gouvernance bancaire a été évoqué pour la première fois dans la circulaire 106 de la BDL daté du 26 Juillet 2006. La BDL a requis aux banques de fournir tous les efforts pour bien se conformer aux principes de la bonne gouvernance.

Ainsi les banques opérant au Liban doivent préparer un guide de gouvernance claire qui inclut notamment un organisme administratif avec un partage de responsabilité efficace et cohérent, le mécanisme de communication adoptée entre le conseil d'administration et la direction générale et une charte organisationnelle cohérente qui définit la relation entre les différentes filiales et la banque mère[238].

Aussi la banque doit publier sur son site électronique et dans son rapport annuel le guide de gouvernance d'entreprise comme un signe de transparence.

Le circulaire aussi met en évidence l'importance d'une coopération mutuelle entre les personnes responsables de gérer les opérations bancaire quotidiennes comme les directeurs généraux, les comités spécialises et le président du conseil d'administration[239].

On constate que la gouvernance est un élément essentiel pour le bon fonctionnement de la banque en particulier et l'économie en général. Elle joue un rôle crucial dans la résistance des banques aux crises externes vu qu'elle détermine les responsabilités et la manière dont les pôles de décision de la banque (actionnaires, dirigeants…) sont censés travailler au sein des différentes instances.

[237] Esther Jeffers, Asma Abidi, La gouvernance des banques à l'épreuve de la crise : comment concilier intérêt général et intérêts des parties prenantes ? Revue d'économie financière 2018/2 (N° 130), pages 277 à 287
[238] BDL circulaire principale 106 – Art. 2
[239] BDL circulaire principale 106 – Art. 1

En effet ces organes disposent de principes, de pouvoirs et de mécanismes pour faciliter l'analyse, la détection et l'évaluation des risques liés aux activités de la banque.

La gouvernance vise à préserver l'intérêt social en déterminant les pouvoirs des différents organes chargés du bon fonctionnement de la banque, spécifiquement les autorités de contrôle, afin de renforcer implicitement leur responsabilité. Cela n'est possible que si la gouvernance définit sa stratégie et ses objectifs dans un cadre sain et intègre[240] qui respecte les lois et règlements en vigueur.

Un dysfonctionnement de la gouvernance peut donc engendrer de graves défaillances tel que la prise de décisions non contrôlée qui affecte le fonctionnement optimal de la banque et ses organes structurels et même engendrer des sanctions qui peuvent compromettre la réputation de celle-ci sur le marché.

Avec la croissance et le développement des systèmes d'information dans le monde cyber durant les dernières années, les banques ne pourraient plus se limiter à la gouvernance classique et devaient ainsi passer à une vision plus contemporaine utilisant des techniques et concepts récents qui font face aux enjeux, problématiques et défis posés par le monde numérique. Une évolution surprenante est apparue dans ce cadre ; la gouvernance numérique.

B- L'évolution du principe de la gouvernance dans la transformation digitale

Dans le contexte récent de la gouvernance et la transformation digitale des banques, il incombe au conseil d'administration de surveiller les outils de conformité au sein de la banque et d'approuver les procédures de détection et de prévention du risque de non-conformité dans le but d'optimiser les bonnes pratiques de gouvernance. Ainsi, les dirigeants de la banque ont évolué de manière drastique leur gouvernance au fil du temps pour mieux appréhender cette transformation numérique et les risques graves qui l'accompagne.

[240] Banques des règlements internationaux, Comité de bale sur le controle bancaire, principe de gouvernance des entreprises a l'intention des banques, Juillet 2015 P. 3

La gouvernance numérique consiste à gérer de manière efficace les systèmes d'information dans un cadre flexible et dynamique surtout que les TIC sont en perpétuelles mutation et par suite la manipulation de ces technologies par les criminels s'aggrave jour après jour.

Vu que le monde digitale est très risqué surtout après l'émergence rapide des cyber crimes, le rôle requis par la gouvernance doit être exercés avec la plus grande diligence.

Grâce à une agile gouvernance de l'information, la gouvernance numérique favorise le développement du digital et améliore la performance des banques dans la lutte contre les crimes bancaires dans ce nouvel espace propice de comportements illégitimes tel que la violations des données confidentielles[241].

De nos jours, les banques ont un rôle primordial dans la prévention des cyber crimes, Cette défense ne peut se faire à titre personnel. Des efforts concertes doivent être mises en place par les responsables exécutifs à la banque pour développer une connaissance de ces risques, et les moyens de les prévenir basé sur une culture de l'éthique dans la conduite des opérations bancaires récentes suivant les nouvelles technologies et une connaissance approfondie des obligations de contrôle des divers acteurs.

Ainsi, la fraude fiscale, le blanchiment d'argent et tous les crimes commis à l'ère du digital peuvent compromettre la continuité et la stabilité de la banque si celle-ci n'a pas mis des moyens pour les combattre. Les pratiques de bonnes gouvernance contribuent largement à préserver et sécuriser un sain système bancaire[242] dans le but d'accroître la transparence et la vigilance entre les actionnaires et dirigeants concernés et lutter contre la corruption considérée comme un échec de la gouvernance.

On constate que la gouvernance en matière cyber sécurité consiste à mettre en œuvre une série de contrôles appropriés, ainsi que les responsabilités et les rôles de chaque organe afin de mettre en conformité les normes applicables, protéger les actifs de la banque et

---

[241] Le centre pour la gouvernance du secteur de la securité, guide pour la bonne gouvernance de la cybersecurité, Genève 2019 P.40

[242] Giovanella Polidoro, La gouvernance face à la conformité, https://www.giovannellapolidoro.com/la-gouvernance-face-a-la-conformite/ date de la visite 30 Novembre 2022

sécuriser les systèmes informatiques opérationnelles associés aux opérations bancaires pour détecter et prévenir les crimes.

Au Liban, la vitesse des innovations technologiques est contrastée malheureusement avec la lenteur des processus législatif qui traite de tels problématique. C'est la raison pour laquelle la gouvernance dans le domaine de la technologie et l'informatique n'est pas règlementée de manière adéquate[243]. La croissance des cyber crimes dans le secteur bancaire surtout après la crise sanitaire constitue un exemple emblématique de ce vide règlementaire.

Ce déficit dans la règlementation doit absolument être compenser par l'élaboration d'un rigide contrôle exercé par les organismes compétents au sein de la banque, capable de détecter et de prévenir les cyberattaques.

Section 2 : La nécessité d'intégrer certaines mesures de protection au sein de la banque

Il est incontournable que les banques les plus avantageuses de demain seront celles qui déploient beaucoup d'effort en matière de prévention, de détection et de correction des cyber crimes. L'ampleur du défi est énorme et la non-conformité aux instructions et règlements de détection et de prévention coûte relativement chère aux banques.

Ceci implique à ce que les banques prennent l'initiative pour introduire de nouveaux services afin de combattre ces genres d'attaques. Ainsi les comités créent à cet égard au sein de la banque jouissent d'une autorité énorme grâce à leur pouvoir de contrôle (P.1) mais aussi la banque a un devoir de sensibiliser ses employés en intégrant une culture de cyber risques au niveau de ses personnels (P.2).

P.1 Le renforcement des pouvoirs des comités spécialisés

La détection et la prévention des faillites dans les systèmes informatiques de la banque dépendent notamment de l'existence d'une structure interne bien organisée.

[243] Guide pour la bonne gouvernance de la cybersecurité, référence précédente, P.66

Les comités de la banque sont au cœur des dispositifs entrepris pour l'évaluation des contrôles intégrés et de leur efficacité. En effet, ces comités peuvent édicter des normes et des directives selon la situation confrontée et ont pour objectif de renforcer la fiabilité dans le secteur bancaire.

Dans le cadre de la cyberdéfense des crimes de l'internet, le comité d'audit jouit d'une autorité de surveillance sur toutes les branches de la banques (A) mais aussi d'autres comités ont été intégrées pour gérer les risques qui peuvent être confrontés par la banque (B).

A. Le comité d'audit : Une mission de contrôle et de surveillance

Les unités d'audit internes jouent un rôle vital au niveau du contrôle exercés dans la banque.

Selon la BDL circulaire principale 106, l'audit de la banque doit s'assurer que les services effectués notamment à la clientèle sont conformes aux procédures établies par la direction générale ainsi qu'aux principes des gouvernances susmentionnées.

L'unité doit aussi évaluer de manière appropriée les règlementations et politiques de la banque et donner son opinion sur le degré d'efficience et d'efficacité, notamment quand la banque s'engage dans de nouveaux produits[244].

A côté de cette unité, le conseil d'administration de la banque doit constituer un comité d'audit [245]. Ce comité doit être indépendant, choisi parmi les membres non exécutifs du conseil et formé de (3) personnes au moins.

Le circulaire stipule que ce comité doit superviser les activités de l'audit interne et examiner ses rapports afin de pouvoir évaluer la performance de l'unité et donner des recommandations[246].

[244] BDL circulaire 106 Art. 3
[245] BDL circulaire 118 Art.4
[246] BDL circulaire 118. Art. 6 Al. 1

De même, cette unité doit revoir l'ensemble des procédures de lutte contre le blanchiment des capitaux et le financement du terrorisme dans le but de s'assurer de leur efficience et efficacité et vérifier que la direction traite les recommandations liées aux faiblesses constatées dans son contrôle[247].

En effet, la fonction d'audit interne constitue la principale ligne de défense du système de contrôle interne puisqu'elle impose le respect des normes de la banque et possède le pouvoir de demander à la direction de remédier efficacement les problèmes confrontés et de réaliser une évaluation régulière des fonctions de conformité[248].

On remarque que les circulaires de la BDL précités bien qu'ils ont développé le rôle de l'unité de l'audit et du comité de l'audit, n'ont rien mentionné sur le rôle majeur de cette unité et son importance dans le cadre de l'évaluation et la prévention des cyberattaques au sein de la banque vu qu'elle exerce le devoir de contrôle et de conformité.

Selon un rapport publié par Deloitte sur la cyber sécurité et le rôle de l'audit interne, l'audit interne doit évaluer la capacité de l'organisation à aborder les cyber risques.

L'importance croissante que les banques accordent de nos jours aux cyber menaces ont attisé les craintes des comités d'audit[249].

En raison des cyberattaques croissantes, les banques doivent s'adapter rapidement à l'évolution des cybers incidents pour faciliter la détection des activités malveillants liées à la cyber sécurité et les mécanismes de défense et de surveillance des organismes responsables.

L'unité de l'audit doit ainsi intégrer ces risques dans les règlements et procédures de contrôles interne et inclure dans leurs rapports et réunions périodiques les faiblesses associées à ce genre de contrôle et les recommandations constatés[250] ainsi que mettre en place des procédures permettant de confronter la situation et leurs points de vue et résultats

[247] BDL circulaire 118. Art. 6 Al. 2
[248] BDL Circulaire 106 – Art. 1
[249] Banques des reglements internationaux, référence précédente P. 34
[250] Deloitte, cybersecurité et role de l'audit interne: un appel urgent à l'action, 2020 P.3

objectifs pour assurer la continuité du travail et garantir une évaluation approfondie des cyber risques.

En ce qui concerne le rôle de l'audit interne dans le renforcement de la cyber sécurité, cette comité joue un rôle crucial en soutenant la banque dans sa lutte contre la cybercriminalité et en fournissant des rapports conformes aux procédures en jeu. De cette façon, l'audit renforce ses mécanismes de contrôle en matière de cyber sécurité en visant principalement les risques associés au monde digitale.

Cependant le rôle de l'audit n'est pas suffisant à lui seul pour exercer le contrôle dans le but de la prévention et la détection des cyber crimes dans la banque digitale. Le comité des risques et de la sécurité de l'informatique (InfoSec) doivent à leur tour intervenir, comme lignes de défense essentielles, pour supporter ce rôle.

B. Instauration d'autres système de contrôle : le comité des risques et le comité d'Info Sec

Selon la BDL circulaire principale 118, le conseil d'administration doit constituer un comité de risque. Ce comité doit être choisi parmi les membres de ce conseil et formé d'au moins (3) personnes[251].

Le rôle du comité est de superviser l'application des règles relatives à la gestion des risques selon les règlements publiés par la BDL et la BCCL[252].

En effet, cet article est très restrictif et n'énumère pas les différents contrôles que le comité de risque est en charge.

En effet, le comité des risques est en charge du risque opérationnel, risque financier, risque humain… Cependant, il existe aussi le risque informatique qui occupe une place énorme de nos jours. Le risque informatique concerne tous les éléments informatiques gérés par les employés et les risques liés au mauvais usage de ces derniers.

[251] Deloitte, cybersecurité et role de l'audit interne: un appel urgent à l'action référence précédente P.5
[252] BDL circulaire 118 – Art.7 -8

En matière de cyber sécurité, le comité des risques doit identifier ces risques et définir toutes les politiques et procédures destinées à les maîtriser[253].

Le risque informatique est vitale de nos jours, il a comme vocation de déterminer la tolérance de l'établissement bancaire à ce genre de risque, mais aussi mettre en œuvre les stratégies et les politiques de sécurité pour respecter cette tolérance.

Le comité des risques est en charge aussi de contrôler les mesures prises par le comité d'audit en matière de sécurité et doit coordonner avec lui et le comité de l'Info Sec, le maillon essentiel de la lutte contre la cybercriminalité à la banque, pour une bonne mise en œuvre et un suivi conforme aux règlements dans le cadre de la gestion des risques.

A l'instar du comité d'audit et du comité des risques, le comité d'info Sec joue le rôle le plus important dans ce processus de contrôle. En effet, les personnes concernées doivent suffisamment connaître et comprendre de manière approfondie leur rôle et responsabilité. Ils doivent avoir l'expertise et les compétences compatibles à ce type de contrôle vu la complexité des cyber crimes et leurs graves résultats.

Le comité de l'Info Sec doit coordonner avec le département de l'info Sec pour identifier et promouvoir les meilleures pratiques de l'industrie en matière de sécurité de l'information et de cyber sécurité ainsi que les nouveaux risques ciblant le système informatique.

Il est en charge de mener des évaluations régulières des risques sur le système informatique afin d'identifier les faiblesses potentielles de sécurité et définir un plan d'action pour remédier aux risques identifiés.

Parallèlement, le comité doit s'assurer que la banque coopère avec les régulateurs locaux et les auditeurs internes/externes concernant les sujets de sécurité de l'information et doit surveiller la conformité avec les réglementations et circulaires liées à la sécurité de l'information de la BCCL et de la BDL.

[253] Marc ANDRIES, David CARTEAU, Sylvie CORNAGGIA, Pascale GINOLHAC, Cyril GRUFFAT, Corinne LE MAGUER, le risque informatique, ACPR Banque de France, Janvier 2019, P.3

Il est chargé d'initier et de promouvoir des activités non conventionnelles pour diffuser la sensibilisation à la sécurité de l'information au sein de la banque et participer activement aux projets émergents en fournissant des exigences de sécurité conformes aux politiques de sécurité de l'information et aux meilleures pratiques en matière de sécurité.

Ainsi le comité doit offrir un soutien au département de l'Info sec pour assurer l'utilisation efficace des systèmes et des ressources informatiques et développer, surveiller et maintenir le cadre de performance, de disponibilité et de sécurité du système d'information de la banque pour les incidents de sécurité suspects ou potentiels.

Personne n'est à l'abri, même l'employé de la banque. De ce fait, la banque joue un rôle énorme quant à la sensibilisation de ses employés à la cybercriminalité compte tenu que ces derniers sont les premières victimes de tels crimes et le manque d'une telle sensibilisation augmentera les risques et les conséquences de ces attaques.

P.2 L'intégration d'un processus de sensibilisation des employés répondant à la pénurie d'expertise humaine

Selon Jean-Charles Duquesne, membre du Mouvement des Entreprises de Taille intermédiaire (METI), directeur général de la Normandie, près d'un incident sur deux est imputable au facteur humain[254].

D'après un sondage réalise en 2019[255], 82 % des répondants ont ignoré ce qu'est un pare-feu, 76 % ne connait pas ce qu'est un malware, 71 % n'ont pas réussi à définir le HTML,

73 % ne comprennent pas le terme VPN.

[254] Temoin donné à la table-ronde organisée par la Délégation aux entreprises le 25 mars 2021

[255] Réalisé pour le compte de l'éditeur en sécurité Specops Software qui a interrogé 2 445 personnes ayant entre 20 et 40 ans.

Malheureusement, ce handicap est particulièrement aggravé dans les banques et ce déficit de compétence était bien visible durant la pandémie de la COVID-19 vu que les cybercriminalités ont connu une forte croissance durant cette période.

Dans cette dernière étude, on verra la pénurie de culture des employés de la banque en matière de cyber sécurité (A) et la nécessite d'intensifier les formations sur la sécurité (B) comme solution à ce déficit de compétence.

A. Manque de culture des cyber risques auprès des employés et clients

Selon Matthieu Bonenfant, Directeur Marketing Stormshield, « Un utilisateur relativement averti peut à lui seul éviter beaucoup de risques.» [256]

Ainsi, le plus vulnérable domaine de toute organisation n'est pas nécessairement technique, mais plutôt humain et l'humain dans notre cas est simplement l'employé de la banque.

L'employé est la clé magique d'une cyber sécurité efficace.

Aujourd'hui, le digital s'impose sur tous les domaines. La cyber sécurité constitue une menace pour la banque mais elle permet aussi de développer le marché financier de plein de produits électroniques sécurisés.

Selon l'observatoire de la confiance numérique, la sécurité numérique et la cyber sécurité employaient 67 000 personnes[257].

Malgré le travail de sensibilisation conduit dans le marketing par les moteurs de recherches, les employés et les clients maîtrisent mal le domaine informatique.

[256] Poitevin Victor, comment insufler une culture de cybersecurite dans l'entrepise, 01 Janvier 2020 https://www.stormshield.com/fr/actus/comment-insuffler-culture-cybersecurite-dans-entreprise/ 5 Decembre 2022

[257] MM. Sébastien MEURANT et Rémi CARDON, rapport d'information fait au nom de la delegation aux entreprises relatif à la cybersecurité des entreprises, 10 Juin 2021, N. 678 11 Aout 2022

Pour pouvoir incorporer une culture de cyber sécurité, il est nécessaire de commencer par le conseil d'administration de la banque et les exécutifs compte tenu que ces derniers constituent un exemple.

L'émergence d'une telle culture de cyber sécurité nommée « tone on the top » énonce l'environnement culturel, le climat éthique général et les valeurs de la banque et n'est qu'une des différentes réponses qui se posent face à la multiplication des menaces sophistiques.

En effet sensibiliser les employés aux risques informatiques ne se définit pas par l'application des règlements seulement, une vraie culture rigide de cyber sécurité doit être développer à l'intérieur de la banque et les employés doivent se sentir concernés par ce rôle. Cela englobe la sensibilisation à la détection, prévention et correction des incidents commis sur l'internet.

Notons que les employés doivent être aussi motiver pour apprendre sur la cyber sécurité et prendre ce risque au sérieux. Dans ce cadre, la banque doit promouvoir l'importance de la sécurité et les conséquences néfastes en cas de violation ou non-conformité aux règles de sécurité[258] pour éviter que ces règles ne soient contournés.

Ainsi, favoriser une culture de cyber sécurité représente un atout redoutable contre les cyberattaques. Une forte et active culture de cyber sécurité influencera énormément le comportement des employés et leur vision vis-à-vis des attaques. Ce qui aidera à mettre en œuvre les meilleurs pratiques pour lutter contre les incidents de sécurité et faire face aux problèmes principalement techniques confrontés dans les banques.

B. Intensification des formations sur la sécurité du digital

Une culture de cyber sécurité n'est établie et une responsabilité envers la sécurité informatique n'est renforcée, que si une collaboration est bien réalisée entre les différents acteurs de la banque.

[258] Fabien Lebargy, la culture de la cybersecurité en entreprise, l'enjeu majeure de 2020, 20 Janvier 2020 https://www.extern-it.fr/la-culture-de-la-cybersecurite-en-entreprise-lenjeu-majeur-de-2020/ date de la visite 20 Décembre 2022

En fait, une seule session informative de cyber sécurité n'est jamais suffisante. La banque doit entreprendre plusieurs sessions continues interactives pour que les employés assimilent la cyber sécurité surtout que ce domaine est encore difficile pour plusieurs.

La banque doit surtout mettre l'accent sur les risques majeurs impliqués dans de tel sorte de cyber crimes et souligner comment la réduction de ce risque sauvera la banque des failles de sécurité.

Les employés jouent un très grand rôle dans la lutte contre la cybercriminalité lorsqu'ils adhèrent à ces formations et assimile bien le concept de cyber sécurité. Ainsi, l'enregistrement des employés dans de tels types de formations et leur prise de conscience sur l'importance de la cyber sécurité de nos jours, facilite leur assimilation de la culture de sécurité.

En effet, éduquer les employés constituent le facteur n.1 pour diminuer les cyberattaques, puisque le criminel cible toujours le maillon faible qui est dans notre cas l'employé. Dans le cas où ce dernier n'est pas suffisamment impliqué et éduquer sur les différentes formes d'attaques, il facilite la mission du criminel pour réussir sa mission[259].

Parallèlement, les mesures de sécurité seront plus efficaces lorsqu'ils sont partagés entre différents employés de différents départements, les tâches de sécurité seront ainsi déléguées ce qui permet de partager la responsabilité et de diffuser la cyber conscience sur tous les cadres de la banque.

D'un autre côté, ces formations peuvent aussi être suivies par des mails de sensibilisation de la part du département concerné. Celui-ci joue un rôle majeur dans la minimalisation des menaces. Ainsi, les personnes concernées peuvent établir un programme de sensibilisation qui attaquera multiples facettes de la cyber sécurité durant une certaine période mettant en relief les précautions à entreprendre dans de tels cas et leur permettant de proposer des solutions pour se protéger des risques adaptés à leur travail quotidien.

[259] Insights for professional, 5 façons de développer une culture de sécurité informatique, 3 Janvier 2017 https://www.insightsforprofessionals.com/fr-fr/it/leadership/develop-an-it-security-culture date de visite 5 Decembre 2022

Selon cyberSensitiz[260], les programmes contre les attaques cyber doivent au moins contenir (4) phases ; une phase préparatoire qui définit les divers types de scenarios de cyber attaques, les objectifs visés et les personnels concernés.

Ensuite, il y a la phase opérationnelle qui consiste à la diffusion des différentes tentatives de menaces. Puis, la phase de synthèse, cette phase collecte et décrypte les résultats obtenus et prépare le compte rendu approprié à présenter.

La dernière phase est la phase de restitution qui constitue le véritable atelier de sensibilisation à la cyber sécurité. Cette dernière définit les différents étapes d'attaques et les bonnes pratiques à entreprendre pour faire face aux multiples risques contournés.

On déduit que les séminaires et programmes sur la protection des cyber menaces doivent ainsi être la première préoccupation de la banque pour assurer une protection maximale pour le client mais aussi les personnels de la banque.
En faite, un comportement responsable de la part du client preuve une pensée consciente de sa part aussi

La solution la plus efficace pour prévenir ces attaques demeure celle de la gestion des séminaires dans le domaine de la sécurité dans le cyberspace. Ces programmes, accessibles aux personnels de la banque, éveille leur conscience et diminue le risque associé aux enjeux critiques des systèmes informatiques.

[260] FC Micro, programme de sensibilisation à la cybersecurité https://fcmicro.net/programme-sensibilisation-cybersecurite/ date de visite 6 Décembre 2022

Conclusion

Nous échappons du Moyen âge! La fonction du digital est dès lors très différente selon les domaines. On réclame l'internet comme un outil capable de réparer les déséquilibres.

La démarche globale entretenue durant cette recherché a consisté à privilégier une analyse approfondie du système bancaire digital actuel tout en mettant en œuvre la particularité de l'environnement dans lequel s'exécute ces opérations afin de relever les lacunes du règlement actuel eu égard à l'opacité des stratégies adoptés dans le droit libanais et leur complexification.

Malgré la difficulté de donner une vision précise du monde numérique, il est incontournable que, de nos jours, le digital nous libère dans un univers où nous ne sommes pas pleinement conscients de ses résultats surtout qu'il est au cœur des différentes réformes légales contemporaines et que les activités bancaires entrepris dans ce monde se développe au-delà des proportions et des attentes jour après jour.

Cependant, l'évolution du digital ne s'oppose définitivement pas à la préservation de l'autorité de droit pénal auxquels les crimes résultants d'une utilisation abusive des systèmes informatique doit y être soumise.

A travers notre étude et dans un premier volet, on a clarifié l'encadrement juridique de la banque digitale et l'apport essentiel de ces banques aux activités bancaires surtout avec la mutation de modèle bancaire traditionnel à l'ère du digital et les divers défis et fragilités qui menacent ce cadre législatif.

Ensuite, on a exposé les principales droits protégés liés à l'utilisation des services de la banque digitale notamment les droits liés aux principes de la protection de la clientèle et ceux relatives la protection des données personnelles soumise au règlement général de la protection des droits personnelles avec une présentation détaillée des législations européennes principalement les législations françaises surtout lorsqu'on se heurtait à un vide dans la législation libanaise

Dans un second volet, on a entamé les risques liés à la banque digitale traduites principalement par le risque de la cybercriminalité bancaire. Dans ce sens, on a discuté les lois et règlements applicables régissant le caractère multiforme de la cybercriminalité et les différents types de crimes facilités par la technologie. On a présenté aussi les principes appliques dans ces crimes et les procédures connexes dans la mise en œuvre des moyens d'accusation et de poursuite de même que pour les procédures spécifiques liées à la preuve électronique dans de tels crimes en matière pénal.

Enfin, on a analysé les raisons pour lesquels il est primordial d'installer un dispositif de protection bancaire pour faire face aux différents types de cybercriminalités. Ainsi on a rapporté le cadre législatif de la cyber sécurité bancaire comme une stratégie essentielle de lutte contre la cybercriminalité et la mise en œuvre de cette stratégie représentée par la cyberdéfense bancaire.

Cette analyse se concrétise par la protection des acteurs de la banque qui doit se baser sur une collaboration transnationale et ne pas se limiter au seul droit national servira pour proposer des bases essentielles de réforme.

Sur la base de ce qui précède et étant confronté aux évolutions infinis résultant des innovations juridiques et techniques dans ce domaine, nous sommes parvenus à des résultats que nous présenterons d'abord ainsi que des recommandations indispensables pour une amélioration efficace du droit libanais.

L'analyse du droit Libanais a prouvé que ses dispositions sont inadaptées et insuffisantes. On s'interroge ici sur la vraie efficacité des règles existantes qui semblent incapable d'assurer leur fonction réelle.

La BDL a un rôle majeur dans le soutient de l'économie locale en générale et les opérations électroniques en particulier car l'expérience montre que cette institution est l'une des institutions les plus compétentes travaillant dans le pays à travers les prérogatives accordées à son gouverneur.

La structure règlementaire au Liban en matière des services électroniques et les innombrables circulaires issus par cet organisme suivent une optique spécifique et échouent a résoudre l'integralité des problématiques soulevées car ils n'abordent pas l'origine du

problème ce qui cause des retards dans le développement du Liban sur la scène mondiale en matière du digital étant donné que le droit libanais a échoué de faire face aux divers et soudain métamorphoses induites par le numérique.

Une analyse pragmatique exige de stresser sur l'ensemble des manœuvres existantes en posant les questions sur leur influence dans la mise en œuvre de nouvelles pratiques. Ces pratiques constituent des outils qui permettent de bien définir la base de ce nouveau cadre juridique. Il s'agit donc de décrypter les spécifiés de la banque digitale afin de définir un nouveau cadre juridique fondé sur des règles classiques et modernes incluant des modalités purement interactives de l'internet adaptés à la numérisation.

La digitalization des services bancaires a permis de développer une startégie financière mieux ciblée et de simplifier les produits bancaires offerts à la clientèle.

Avec l'émergence du COVID19 à travers le monde, il y a une tendance internationale de basculer fortement dans le numérique.

La technologie de l'information et de la communication a été consacrée pour la première fois dans la législation libanaise, selon l'article 81/2018.

L'utilisateur jouit de ces droits et libertés consacrés en sa faveur dans les conventions internationales et les textes constitutionnels et les lois ordinaires, dans le monde virtuel, et cela a été stipulé pour la première fois sous l'article 2 de loi.

Il est clair que la loi 81/2018, récemment adoptée, est une initiative promotrice dans le monde de la technologie. Cependant, cette loi nécessite une réforme majeure permettant de maximiser ses pouvoirs divers sur la technologie et de récolter ses avantages envisages tout en minimisant les dangers et les risques informatiques.

Le rôle de la BDL a été clairement reflété dans la loi 81/2018 puisque plusieurs articles notamment les articles 61, 64 et 133 lui ont accordés de larges pouvoirs pour maintenir en vigueur les circulaires qu'on a déjà présenté et ont traite multiples sujets très récents comme la protection des données à caractère personnel et la monnaie électronique.

Cependant, la bureaucratie, les conflits politiques infinis et les instabilités legislatifs, ont participé à la chute de la loi 81/2018. A titre d'exemple, l'article 96 section 13 de la loi 81

impose une définition des mesures garantissant la sécurité des données personnelles cependant les actions nécessaires pour les mettre en œuvre sont absentes, on s'interroge ainsi sur le but recherché de ces mesures et les obligations et qui y découlent.

De même que certaines dispositions légales du texte qui a été adopte en Septembre sont inopérantes sans décret d'application. Avec l'absence d'un président libanais et d'un propre gouvernement, cette mission est suremement impossible.

Cette recherche s'inscrit dans un contexte d'instabilité législative. Le droit libanais est connu malheureusement par la stabilité de ses règles ce qui n'est du tout prometteur vu le développement incessant des nouvelles technologies.

On remarque une déficience des lois libanaises et une quasi absence de la jurisprudence et doctrine qui se contentent de la globalisation du digital et se suffisent par la simple interprétation des lois française en la matière.

Tout particulièrement, l'étude menée a révélée l'inadéquation du régime actuel des sanctions libanaises et françaises. Ce qui implique un renforcement des sanctions classiques et primordiales.

La vulnérabilité du Liban aux attaques dans le monde cyber a été traite par La loi 81/2018 ainsi que les circulaires de la BDL en renforçant la protection de la clientèle en cas de cyberattaques. A noter que les transactions électroniques étaient régies par des notes internes et des annonces issues par la BDL, ce qui implique qu'en cas de procès juridique, le juge n'avait aucune loi sur laquelle il peut s'appuyer.

La loi a aussi renforcé la protection des données personnelles. Ainsi elles ne peuvent plus être traitées pour des raisons non déclarées dès le début du traitement. La loi énumère des exceptions dans de tels cas. Une autorisation préalable du ministère de l'Economie est obligatoire ici pour la collecte des données.

En tant que système informatique, la preuve dans les cybercrimes bancaires est principalement la preuve numérique dont les conditions ont été révélés dans la loi 81/2018. Celle-ci a relevé plusieurs problématiques dont la confidentialité de l'utilisateur et a fait reculer certaines garanties d'inspections traditionnelles**.**

Le développement technologique a imposé la création d'un dispositif spécialisé de lutte contre les crimes commis par des moyens informatiques dont le plus important au Liban est le « Bureau de lutte contre les délits informatiques et de protection de la propriété intellectuelle ». Il est chargé des fonctions de la police judiciaire dans son cadre. Son institution est accusée d'être contraire à la loi.

A noter que les plus fondamentaux sujets examinés dans les stratégies de lutte contre la cybercriminalité sont l'adoption d'une culture des cyber risques, l'intervention rapide dans la gestion des incidents et la collaboration entre la banque, ses régulateurs et les organes publiques et privés qu'ils soient juridiques ou réglementaires[261] en sus de faciliter l'échange et le partage fiable d'information sur les crimes informatique.

Pour une utilisation sécurisée de la banque digitale et afin de minimaliser les pénalités en cas de non-conformité avec les règlements et loi en vigueur, une bonne réflexion approfondie s'avere indispensable pour proposer des recommandations et améliorations qui répondent aux besoins essentiels du numérique.

Tout d'abord, au vu de l'ensemble de mutations induites par le numérique et l'évolution rapide des divers pratiques illicites sur internet, il s'avère essentiel de repenser le régime classique pour mettre en place de nouvelles exigences plus strictes. On songe notamment à la modernisation des lois de protection contre les cyberattaques.

Travailler tous ensemble de manière solidaire, rapide et armée de qualifications nécessaires, donnera surement un avantage au pays, à son économie et par conséquence à ses citoyens et le placera sur la carte de la technologie numérique.

Le développement rapide du numérique sur la scène internationale soulève la nécessité de bâtir un nouveau modèle de services électroniques adapté à l'environnement dynamisme

[261] Serge Escale, La pénurie des talents pénalise le secteur de la cybersécurité, 18 Décembre 2022 https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/la-penurie-des-talents-penalise-le-secteur-de-la-cybersecurite/

du digital. Cela signifie que les réformes au Liban ne sont pas seulement recommandées; mais aussi vitales et inévitables car nous sommes encore très loin des pays voisins dans ce domaine.

Il est difficile de comprendre comment la BDL ignore ses obligations envers les banques libanaises, ayant vu les pays voisins promulguer des règlementations qui protègent la clientèle et la banque avec l'accroissement exponentiel de la technologie moderne.

Avec l'élection d'un président et la formation d'un nouveau gouvernement, la priorité devrait être la mise en œuvre de ces réformes afin de gagner la confiance de la IMF et de la communauté internationale surtout que la crise des banques au Liban ne cesse de s'accentuer.

En France, la protection des données personnelles est dans les mains d'un seul organisme; la CNIL qui jouit des pouvoirs nécessaires. Au Liban, il fallait suivre la même direction et créer une autorité similaire libanaise à cet égard au lieu de diviser les tâches par ministère, ce qui notamment affaibli la loi.

En effet, le caractère international du numérique exige évidemment une coopération au niveau international des multiples autorités normalement compétentes en la matière pour inciter les banques au respect de la loi.

Il est important dans ce cadre de développer une compréhension étroite des techniques et nouveaux modèles entrepris par les criminels en se basant sur une analyse juridique, voire technique des différents services électroniques offerts par le digital vu la plasticité des règles juridiques existantes qu'elles soient laxistes ou strictes.

Il faut certainement privilégier l'éducation puisque le fait de transmettre l'information par l'éducation renforce la capacité cognitive voire la vigilance de l'autre partie.

En France, par exemple, La CNIL publie de manière simplifié des instructions sous forme de schémas ou même de vidéos dans le but de sensibiliser le public. Un simple comportement de prudence permettra de limiter le nombre de ces préjudices.

Même si ces modalités facilitent la prise de conscience du client, on ne peut nier que ces formes d'éducation exigent aussi une motivation de la part de ce dernier.

Cela reflète l'idée que la cybercriminalité en tant que crime doit être inclus parmi les infractions cités dans l'article 1 de la loi 44 relative à la lutte contre le blanchiment d'argent et le terrorisme dans le but de mettre en relief ses conséquences atroces surtout que ses techniques et typologies sont aujourd'hui commises dans le but d'encaisser des fonds illicites.

On propose dès lors la modification de plusieurs articles de la loi 81 notamment les articles 8, 79, 88, 89 et 134 afin d'introduire des information plus cohérentes et adaptés. Dans ce cadre, il est nécessaire de rapprocher les dispositions libanaises de celles française comme les ces dernières sont mises à jour aux changements induites par le numérique ce qui justifie la nécessité de transposer certaines dispositions françaises au droit Libanais.

Aussi, il est préférable que le législateur libanais cumule l'amende et la peine d'emprisonnement crainte de limiter l'efficacité de la sanction. De tels mesures bien établies peuvent prévoir toute formes de risques éventuels.

Il est nécessaire de stipuler explicitement que la police judiciaire ne doit pas restreindre la recherche de la preuve numérique a un délai déterminé du a l'élément de vitesse requis dans ce domaine et la possibilité d'accéder aux données à distance en mettant en exergue le strict respect du principe de confidentialité dans les modalités d'obtention de ces preuves.

Sous une atmosphère de coopération très vigilante avec d'autres comités, créer une comité IT dans les banques responsables de veiller sur les bonnes pratiques qui s'articulent en matière de protection contre les crimes dans le monde cyber et bien gérer une stratégie de sécurité bancaire.
Il est essentiel de pouvoir combiner les pratiques existantes avec celle contemporaines afin de saisir l'étendu réelle de ces nouvelles pratiques.

Aussi, mettre en exergue des procédures spécifiques dans le but d'atteindre l'objectif du « compliance » ou de la mise en conformité. Ce fait n'est possible que si la transparence est renforcée et la mission des autorités de contrôle est facilitée.

Adhérer à la convention arabe pour lutter contre les délits liés aux technologies de l'information (2010) et la Convention de Budapest sur la cybercriminalité (2001) qui ont organisé la coopération internationale dans le domaine de la collecte et la conservation des preuves numériques.

En guise de synthèse, on conclut que les banques ont parfaitement changer la nature des opérations et services bancaires offertes avec l'apparition des TIC pour se transformer de banques traditionnelles en banques digitales. Mais cette transformation est-elle sans risque dans un monde virtuel où la criminalité est en croissance continue et la technologie est utilisée à des fins dommageable?

On espère que le futur apportera des réponses adéquates sur ce qui nous attend dans ce monde virtuel qui ne cesse de nous étonner, et place les législateurs et régulateurs face à des défis sans fin pour lutter contre les risques perçus d'une utilisation abusive de ces méthodes et outils...

Bibliographie

A- Ouvrages Généraux

[B-1]. Adala, A., & Djellam, A. (2015). Le rôle du marketing digital dans l'amélioration des performances des banques commerciales Algérienne, étude analytique statéstique. Finances et marchés

[B-2]. Ben Boubaker Safa, L'évolution du modèle bancaire a l'ère du digital, Décembre 2020

[B-3]. Berdi Abdelaziz, La relation entre la banque traditionnelle et l'e-Banking: une tentative d'analyse à partir du cas marocain, Revue de contrôle de la comptabilité et de l'audit, Numéro 7, décembre 2018

[B-4]. Chamoux J.P., L'ère du numérique 2 : l'économie revisitée, Ed ESTG, London, 2018

[B-5]. Cornu G. Vocabulaire Juridique. Association Henri Capitant, Paris, PUF, 11eme édition, 2016

[B-6]. Cronin, J.Mary. Banking and Finance on internet, Wiley, New York, 2007

[B-7]. Colein F., Manuel de l'interne. Paris, Lavoissier 2001

[B-8]. Cronin, M.J., Banking and Finance on Internet., New York, 1998

[B-9]. Diniz Eduardo, web banking in USA, 1997

[B-10]. Dixon, Mary et Nixon, Brian. 2000. e-banking: Managing your money and transactions online. SAMS publishing

[B-11]. Gusdorf F.et Lassure Ch.

[B-12]. Jürg Schneider, Digitalisation, les nouveaux défis juridiques, smart media, Walderwyss avocats, 2019

[B-13]. Jon P. Wade (2015), a definition of system thinking : a systems approach, Elsevier, 2015

[B-14]. Lamirault, F. (2017). L'évolution du modèle bancaire à l'ère du digital. Paris: Livres blancs

[B-15]. Mansfiled Edwin, Technical change the rate of imitation, Econometrical, October 1961

[B-16]. Nasser Saidi, Le systeme de paiement au Liban

[B-17]. Nassif E., les contrats internationaux, le contrat électronique en droit libanais, Beirut, El Halabi, 1ere édition, 2009

[B-18]. Nammour Fadi, Le droit bancaire, Université Libanaise, Faculté de Droit et des Sciences politique et administrative 2015

[B-19]. Seybold, P.B. et Marshak, R.T. Customers.com: How to create a profitable business strategy for the internet and beyond, 1998

[B-20]. هانيا محمد علي فقيه، حماية الحق في الخصوصية المعلوماتية، دراسة تحليلية لواقع الحماية وتحديات العصر، دراسة منشورة في مجلة الحياة النيابية، المجلد المائة وخمسة، كانون الأول/ديسمبر ٢٠١٧، لبنان

[B-21]. الصغير، جميل عبد الباقي، ٢٠٠٢، أدلة الإثبات الجنائية والتكنولوجيا الحديثة، دار النهضة العربية، ط ١، القاهرة.

[B-22]. حجازي، عبد الفتاح بيومي، ٢٠٠٩، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دراسة مقارنة، منشأة المعارف، ط ١، الإسكندرية،

[B-23]. علي مصباح إبراهيم، الوافي في أصول المحاكمات المدنية – الجزء الأول، الطبعة الأولى، الناشر غير مذكور، ٢٠١

[B-24]. سمير عالية وهيثم سمير عالية، الوسيط في شرح قانون العقوبات -القسم العام، الطبعة لأولى، مجد المؤسسة الجامعية للد ا رسات والنشر والتوزيع، ٢٠١٠

[B-25]. خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩

B- **Articles**

[B-1]. Abdelaziz Berdi, the relationship between traditional bank and e-banking , Revue du contrôle de la compatibility et de l'audit, Numéro 7, Decembre 2018

[B-2]. Bollo Édouard Fernandez-, institution financière et cybercriminalité, revue d'économie financière, 2015/4, (n.120)

[B-3]. Boumedienne Nada et Renaud Garcia Bardidia, l'impact du digital sur la clientele du service bancaire, revue innovation, Volume: 11/ N°: 01A (2021)

[B-4]. Boudchicha Rima, Kahoul Mohamed Yazid, Impact de la Pandémie du Coronavirus sur le Paiement Électronique en France – Etude Descriptive Analytique, 31 Décembre 2021, Revue EL - Maqrizi pour les études économiques et financières Volume:5 / N°:2 (2021),

[B-5]. Bruno Teboul, Le tournant cognitif de la cybersécurité : changement de paradigme et prolégomènes à la cybersécurité cognitive, 14 Avril 2022

[B-6]. Benoit grange, Cybersecurity : les banques face au défi de la protection de leur clientèle, ZD NET

[B-7]. Deutsche Bank, boss says 'big number' of staff will lose jobs to automation, the Guardian, 2017

[B-8]. Edouard Fernandez Bollo, Institution financière et cybercriminalité, Revue d'économie financière, 2015/4 N. 120

[B-9]. Esther Jeffers, Asma Abidi, La gouvernance des banques à l'épreuve de la crise : comment concilier intérêt général et intérêts des parties prenantes ? Revue d'économie financière 2018/2 (N 130)

[B-10]. ETER Sanaa, The Lebanese e-transaction law in relation with personal data protection law, Data and Society,

[B-11]. Frank Plaschke, Ishaan Seth, and Rob Whiteman, Bots. Algorithms and the future of the finance function, Article, 9 January 2018

[B-12]. Harb Bissane, Saleh Mariam, les enjeux de l'e-banking au Liban, revue N. 29, 2017

[B-13]. La transformation numérique dans le secteur bancaire français, ACPR banque de France, N. 131

[B-14]. Laurent Bour, l'évolution des banques face à la transformation digitale, Le journal du CM, Octobre 2019

[B-15]. Le Commerce du Levant, Les cartes bancaires en hausse fin 2011, 24févr. 2012

[B-16]. Laura Noonan and Patrick Jenkins, Citigroup CEO says machines could cut thousands of call centre jobs, Financial Times 2019

[B-17]. Moughabgheb N., la protection des programmes informatiques. Les moyens et les lacunes, Beyrouth, El Halabi, 2006

[B-18]. Saleh M. Nsouli et Andrea Scheaechter, les enjeux de la banque électronique, Finance & développement, Septembre 2022

[B-19]. Reich C. Pauline, Cybercrime and security, Vol. 1, Thomson Reuters, 2012

[B-20]. Stamoulis, D.S. How banks fit in an Internet Commerce Business Activities Model, 1994

[B-21]. Vieira et Nathalie Pinède. (2005), enjeux et usages des TIC : aspects sociaux et culturels T1, Presses universitaires de Bordeaux, Bordeaux

[B-22]. Toufaily, E., Daghfous, N., & Toffli, R. (2009). The Adoption of "E-Banking" by Lebanese Banks: Success and Critical Factors. International Journal of E-services and Mobile Applications, 1(1),

[B-23]. ZAOUI Asmae, BOUDAOUD Fatima, HASSEB Mohamed Lamine, L'impact du covid-19 sur la transformation digitale du secteur bancaire, Revue d'excellence pour la recherche en économie et en gestion, Vol 05, N°01 (2021),

[B-24]. علوش محمد. ، رسالة لمكتب جرئم معلوماتية: أوقفوا مخالفة القانون أوعدّلوه٣/١٢/٢٠١٣ ، مقال منشور على موقع "النشرة السبت ١١ آب ٢٠١٨

[B-25]. مجلة مستقبل العلوم الاجتماعية، العدد الرابع، نيسان ٢٠٢١

[B-26]. نصر فيلومين يواكيم، أصول المحاكمات الجزائية، الطبعة الأولى، المؤسسة الحديثة للكتاب، ٢٠١٣

[B-27]. فرنجية غيدة ، مكتب مكافحة الجرا ئم المعلوماتية :رقابة غير منظمة على المساحات الإلكترونية، مقال منشور على الموقع الإلكتروني لمجلّة" المفكرة القانونيةwww.legal-agenda.com:

C- **Thèses et mémoire de recherche**

[C-1]. Chencheh Ossama, Les déterminants de l'adoption de e-Banking par les institutions financières et la clientèle organisationnelle, et son impact sur

l'approche relationnelle: cas de l'internet Banking en Tunisie, mémoire de maitrise, université de Quebec, Montreal, Juillet 2011.

[C-2]. Christoph Chloé, la cybercriminalité bancaire, mémoire de master 2 chargé de clientele professionnelle, Université de Strasbourg, faculté des sciences économiques et gestion 2020- 2021

[C-3]. Roger Et Shoemaker, F.F. communication et innovations, New York, Free press,1971

[C-4]. Sofia Karim, Electronic transactions in Lebanon:legal challenges and opprortunities, Master en business law, Lebanese American University, February 2019

[C-5]. Saadi Makrem, Implantation de l'approche relationnelle dans le domaine des services: cas du secteur bancaire, Mémoire de maitrise, université de Québec, Montréal,

[C-6]. سامر أبو شقرا، الدليل الرقمي بين الضابطة العدلية والقضاء .لبنان نموذج، رسالة لنيل دبلوم الدارسات العليا في القانون الجزائي، الجامعة اللبنانية - كليّة الحقوق والعلوم السياسية والإدارية، الفرع الثاني

[C-7]. شهرزاد حداد، الدليل الإلكتروني في مجال الإثبات الجنائي، مذكرة مكملة لنيل شهادة الماسترفي الحقوق، جامعة العربي بن مهيدي أم البواقي– كلية الحقوق والعلوم السياسية - قسم الحقوق،.٢٠١٧ / الجزائر

[C-8]. هانيا الحلوه، الجرائم السيبارنية بين مشروع القانون الصادر بالمرسوم رقم ٢٠١٢/٩٣٤١ لنيل شهادة الدرا سات العليا في القانون الجزائي، الجامعة اللبنانية – كلية الحقوق والعلوم السياسية والإدارية، الفرع الثاني، ٢٠١٧

D- <u>Rapports</u>

[D-1]. Accenture, rapport annuel, 2021-2022

[D-2]. Accenture Global Banking Consumer Study, Making digital banking more human, 2020

[D-3]. Accelerate Collective Intelligence Partner, Le règlement général sur la protection des données RGDP, règlementation et enjeux dans les banques et assurances

[D-4]. Banques des règlements internationaux, Comité de bale sur le controle bancaire, principe de gouvernance des entreprises a l'intention des banques

[D-5]. Cybersouth project, situation report on cyber crime and money laundering on the Internet, in Lebanon, Novembre 2020

[D-6]. Deloitte, cybersecurité et role de l'audit interne: un appel urgent à l'action, 2020

[D-7]. Institut de recherche en management et en pratique de l'entreprise, la digitalisation au sein du secteur bancaire entre causes et conséquences, Juillet 2020

[D-8]. Interpol, la cybercriminalité : impact du COVID 19, Aout 2020

[D-9]. ISF, livret de sensibilisation aux cybercmenaces
[D-10]. Le centre pour la gouvernance du secteur de la securité, guide pour la bonne gouvernance de la cybersecurité, Genève 2019
[D-11]. Les nouvelles technologies de la banque à distance: quelles conséquences pour les établissements financiers et leur autorité de contrôle, étude du rapport annuelle de la commission bancaire, 1999
[D-12]. Mk Mckinsey, accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France, Mckinsey&Company, 2014
[D-13]. MM. Sébastien MEURANT et Rémi CARDON, rapport d'information fait au nom de la delegation aux entreprises relatif à la cybersecurité des entreprises, 10 Juin 2021, N. 678
[D-14]. Président du conseil des ministers, stratégie nationale libanaise de cybersécurité, 2019
[D-15]. Rocoveo, Livre blanc, Cyberattaques par ransomware
[D-16]. Gouvernement Libanais, Stratégie Nationale Libanaise de Cyber sécurité, Juin 2019
[D-17]. United Nations Office of Drugs and Crime, Utilisation de l'internet a des fins terroristes, NY, 2014
[D-18]. Rapport de la banque de France, Évaluation des risques du système financier français, publié le 28 Juin 2021

E- Discours

[E-1]. Halilou Yerima, discours du Directeur de l'unité Banque commerciale d'Arique du nord du CBA/FT.

F- Textes législatifs

[F-1]. Décret. N. 8341, Circ. no92, 24 janvier 2003, relatif à l'émission des cartes électroniques
[F-2]. BDL circulaire 69 – Banque éléctronique et transactions financières, 30 Mars 2000
[F-3]. BDL circulaire 118 - Conseils d'administration et comités des conseils d'administration des banques libanaises, 21 Juillet 2008
[F-4]. BDL circulaire 144 – Prévention des cybercrimes, 28 Novembre 2017
[F-5]. eIDAS Regulation (Regulation (EU) N. 910/2014)
[F-6]. Loi N. 81 du 10 Octobre 2018 – Les transactions électroniques et la protection des données personnelles
[F-7]. Traité international pour la protection des droits de l'homme sur le continent européen, 4 Mas 2009
[F-8]. Charte des droits fondamentaux de l'Union européenne 2000
[F-9]. Constitution libanaise
[F-10]. Directive 2013/36/UE du 26 juin 2013
[F-11]. Loi sur le secret bancaire, 3 Septembre 1956

[F-12]. Règlement (UE) 2016/679, 27 Avril 2016
[F-13]. Convention de Budapest, 23 Novembre 2001
[F-14]. Convention arabe sur la lutte contre les crimes liés aux technologies de l'information, 29 Juin 2021
[F-15]. Loi n.78-17 relative à l'information, aux fichiers et aux libertés, 6 Janvier 1978
[F-16]. Loi n. 88-19 relative à la fraude informatique, 5 Janvier 1988
[F-17]. Code de la cybersécurité, Dalloz, 2022
[F-18]. Protocole relatif à l'incrimination d'actes de nature racistes et xénophobe commis par le biais de systèmes informatique, 28 Janvier 2003
[F-19]. Protocole relatif au renforcement de la coopération et de la divulgation de preuves électroniques, 12 Mai 2022

G- Sitographie

[G-1]. http://www.theatlantic.com
[G-2]. https://www.i-vest.ch/fr/trends/banque-digitale/banque-en-ligne-et-banque-digitale-quelle-est-la-difference
[G-3]. https://www.lenetexpert.fr/comment-est-nee-la-cybercriminalite-2/
[G-4]. https://blogrecrutement.bpce.fr/quelles-sont-nouvelles-habitudes-bancaires-millennials
[G-5]. https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1502381-carte-bancaire-virtuelle-definition-et-utilisation/
[G-6]. https://artimon.fr/perspectives/le-cloud-computing-quels-avantages-et-risques-dans-le-cadre-de-la-transformation digitale/#:~:text=Le%20cloud%20computing%20est%20un%20processus%20d'acc%C3%A8s%20%C3%A0%20des,outil%20digital%20de%2
[G-7]. https://www.processmaker.com/fr/blog/intelligent-automation-in-banking/
[G-8]. www.legiliban.ul.edu.lb
[G-9]. https://www.cnbc.com/2020/05/27/coronavirus-crisis-mobile-banking-surge-is-a-shift-likely-to-stick.html
[G-10]. https://www2.stardust-testing.com/blog-fr/comment-le-covid-19-accelere-la-transformation-numerique-de-la-banque-de-detail
[G-11]. https://fr.linkedin.com/pulse/covid-19-et-secteur-bancaire-la-digitalisation-des-banques-aider
[G-12]. https://www.twilio.com/covid-19-digital-engagement-report
[G-13]. https://www.cgi.fr/.
[G-14]. https://www.executive-magazine.com/business-all/the-need-to-reform-electronic-money-transfer-regulations
[G-15]. http://www.dentons.com/en/insights/alerts/2019/january/21/new-lebanese-law-on-etransactions-and-data-protection
[G-16]. http://www.tohmelaw.com/news/covid-19-and-electronic-signatures-lebanon
[G-17]. https://www.moneyvox.fr/tarif-bancaire/mobilite-bancaire.php

[G-18]. https://www.moneyvox.fr/tarif-bancaire/mobilite-bancaire.php
[G-19]. BAU.digitalcommons.bau.edu.lb/lsjournal/vol2020/iss2020/7/
[G-20]. https://www.pwc.fr/fr/decryptages/securite/banques-une-transition-digitale-longue-couteuse-et-douloureuse.html
[G-21]. https://documents-addsny.un.org/doc/UNDOC/GEN/N13/449/45/PDF/N1344945.pdf?
[G-22]. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session
[G-23]. https://www.cnil.fr
[G-24]. https://www.legifrance.gouv.fr
[G-25]. http://www.l'orientlejour.com
[G-26]. https://www.anyti.me/fr/actualites/crise-bancaire-au-liban-les-epargnants-reclament-leur-argent/1370
[G-27]. https://www.dastra.eu/fr/guide/risques-rgpd/495
[G-28]. www.interpol.int
[G-29]. https://terranovasecurity.com
[G-30]. https://sic.gov.lb
[G-31]. https://www.guidedetectives.fr/articles/ec3-le-centre-europeen-de-lutte-contre-la-cybercriminalite, 7 Novembre 2022
[G-32]. https://www.societegenerale.com
[G-33]. www.isf.gov.lb

Sommaire