Université Libanaise
Faculté de Droit et des Sciences Politiques et Administratives
Filière Francophone de Droit

Sécurisation des transactions bancaires via internet

Mémoire pour l'obtention d'un diplôme d'études approfondies en Droit des Affaires Internes et Internationales

Présenté par

Joséphine M. Habib El Khoury

Membres du Jury

Dr. Amal Abdallah	**Directeur**
Dr. Ghassan Salameh	**Membre**
Dr. Rania Saliba	**Membre**

2018

Remerciements

Mes remerciements les plus chaleureux vont tout d'abord à ma directrice de mémoire, Docteur Amal Abdallah, qui m'a fait l'honneur de diriger mon mémoire. Je la remercie vivement pour sa grande disponibilité, son support, sa gentillesse, ses précieux conseils ainsi que pour ses méticuleuses relectures.

Mes remerciements vont également à mes parents à qui je dois ce que je suis, à mes enfants qui rayonnent ma vie, et à mes amis qui m'ont apportés support et encouragement.

L’Université Libanaise n’entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à son auteur.

Résumé

De la dématérialisation de la monnaie à la dématérialisation des services bancaires et des banques !

Certes la banque en ligne est investie de nombreux avantages toutefois pour en bénéficier de ces avantages, les transactions bancaires en ligne doivent être sécurisées à un double niveau contractuel et institutionnel. Au niveau contractuel, la transaction bancaire en ligne serait sécurisée lorsque le client y consentant jouit de la capacité légale le rendant éligible pour faire une telle transaction mais aussi qu'il soit identifiable pour la banque cocontractante. Cette identification est réalisée par des moyens traditionnels et nouveaux spécifiques à ce mode électronique. De nos jours, les législations anti blanchiment et d'échanges d'informations fiscales, imposent l'identification du bénéficiaire effectif et la traçabilité des transactions à l'échelle internationale. En outre, la sécurisation connote également un consentement éclairé du client internaute et implique fondamentalement la protection de ses données personnelles qui sont devenues des ressources de revenus considérables pour les géants du monde numérique. Quant à la sécurisation au niveau cadre institutionnel, la banque en ligne, comme toute banque à quelques différences près, doit être dotée d'un agrément lui permettant d'exercer l'activité bancaire et doit également être identifiable pour le public en général et pour sa clientèle en particulier. Néanmoins, plusieurs obligations incombent aux deux parties à la transaction bancaire en ligne. La banque est tenue en autre de l'obligation de sécurité, de confidentialité et de remboursement. Pour sa part, le client internaute doit aussi contribuer à cette sécurisation par sa vigilance et coopération. Enfin, les recours judiciaires et extrajudiciaires sont indispensables pour instaurer la sécurisation des transactions bancaires en ligne.

Liste des principales abréviations

ACPR	Autorité de contrôle prudentiel et de résolution
BDL	Banque du Liban
Bull.	Bulletin des arrêts de la Cour de Cassation
CConsom.	Code de la consommation
C.App	Cour d'appel
Cass.	Cour de cassation
Cass.civ.	Chambre civile de la Cour de cassation
Cass.com.	Chambre commerciale de la Cour de cassation
CCiv	Code civil français
CCom	Code de commerce
CJCE	Cour de Justice des Communautés Européennes
CMCL	Code de la Monnaie et du Crédit Libanais
CMF	Conseil des Marchés financiers
CNIL	Commission nationale de l'informatique et des libertés
COC	Code des obligations et des contrats libanais
CPC	Code de Procédure Civile
D.	Dalloz
DSF	Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs.
DCE	Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).
ENISA	European Union Agency for Network and Information Security (en français Agence Européenne chargée de la sécurité des réseaux et de l'information).
FAI	Fournisseur d'accès à Internet
Fasc	Fascicule

FATCA	Foreign Account Tax Compliance Act
FEVAD	Federation du E-commerce et de la Vente à Distance
FICP	Fichier national des incidents de remboursement des crédits aux particuliers
Gaz. Pal.	Recueil de la Gazette du Palais
JO	Journal Officiel
JCP	La semaine juridique
JCP éd. G	La semaine juridique. Edition Générale
INPI	Institut National de la Propriété Industrielle
ISOC	Internet Society Club
KYC	Know Your Customer
LCEN	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004 p. 11168.
NIP	Numéro d'identification personnel – PIN en anglais
Op. cit.	*Opere citato*
PSCE	Prestataire de service de certification électronique
Rec.	Recueil
Rev.	Revue
RGDP	Règlement Général relatif à la Protection des Données Personnelles
TGI	Tribunal de Grande Instance
www	World Wide Web

Sommaire

Introduction

« *Banking is essential, banks are not* »[1].

« L'Internet n'est ni un nouveau monde ni un septième continent. C'est le monde réel mis en situation virtuelle. Si l'on accepte de considérer qu'il est tout aussi réel en virtuel, la majeure partie des questions trouve une réponse ».[2]

1. La dématérialisation et l'activité digitale sont devenues le style de vie de toutes les sociétés[3] et dans tous les domaines. L'internet, « réseau des réseaux »[4] a rendu les contacts faciles et rapides et il est de nos jours sollicité pour toute sorte d'activités et services. Il constitue le centre de la vie quotidienne des milliards[5] d'individus, des professionnels et des personnes morales à un tel point que nous expérimentons une mutation économique et sociale.

2. La genèse de l'internet a eu lieu aux États-Unis en 1969 lorsque l'Agence pour les Projets de Recherche Avancée du Pentagone[6] a adopté et financé un projet universitaire innovateur[7] dont le but consistait à rassembler les articles et les réflexions des différents chercheurs dans les universités américaines et de mettre en commun leurs travaux en supprimant les barrières imposées par la géographie. Ce projet a intéressé cette agence gouvernementale qui voulait créer une infrastructure de communication informatique

[1] BILL GATES, The Gates Letter 2015.

[2]BENSOUSSAN A, Commerce électronique et avenirs des circuits de distribution : de l'expérience des Etats-Unis aux perspectives françaises, aspects juridiques et fiscaux (colloque du 13 mai 1998), Gaz. Pal. 20 octobre 1998, p.1338 - cité par Fatima Zahra Boulaich Bayssa dans sa thèse intitulée « Les prestations financières en ligne », 2013.

[3] V. UNCTAD, information economy report 2017 "digitalization, trade and development", United Nations Conference on Trade and Development: http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

[4] LE TOURNEAU (P), « Contrats Informatiques et électroniques », Dalloz, 4e éd. 2006.

[5] 4.156.932.140 internautes connectés jusqu'au 31 décembre 2017. Statistique disponible au site suivant : http://www.internetworldstats.com/stats.htm.

[6] (Advanced Projects Research Agency - ARPA).

[7] Volle M, L'internet, 2005 ; http://www.volle.com/travaux/internet.htm.

destinée aux militaires américains répartis sur le globe, qui soit capable de résister à une déflagration nucléaire[8].

3. D'un réseau conçu à la communication, l'internet est devenu un réseau d'échange commercial. Il a transformé les usages et habitudes des consommateurs et professionnels et a créé des biens de nouvel ordre, ce sont les « *biens informationnels*[9]», ou biens virtuels.

4. De son côté, le secteur bancaire a jugé indispensable de s'immerger dans ce mode numérique. Par conséquent, il a subi des changements radicaux et a témoigné de méthodes d'opérations innovatrices[10]ainsi qu'une nouvelle dématérialisation différente par sa nature. C'est la dématérialisation des services[11] et des banques. Effectivement, la dématérialisation des banques fut le fruit de la dématérialisation de la monnaie.

5. La banque électronique ou banque en ligne fut introduite progressivement dans l'esprit du public depuis plusieurs années sous forme de guichets automatiques[12] qui ont fait disparaître la notion de lieu, de temps et d'action, et ont ultérieurement rendu familières les transactions bancaires en ligne. De récentes technologies de banque sans fil ont vu le jour (téléphone portable, smartphone) qui permettent d'effectuer des opérations bancaires en appuyant sur un bouton téléphonique.

---

[8] La première connexion fut établie le 21 novembre 1969, à l'université University of California of Los Angeles (UCLA), entre Standford, Santa Barbara et l'université d'Utah. Située à UCLA, elle permettait de diriger vers son destinataire, où qu'il se trouve sur le réseau, le message envoyé par un ordinateur distant. Ce n'est qu'en 1973 que le concept d'internet a vraiment vu le jour et ce lorsqu' il y a eu un problème de la connexion du système Arpanet avec les réseaux qui avaient pu apparaitre dans le monde, et qui obéissaient à des normes différentes. D'où la nécessité d'harmoniser la communication entre les différents réseaux en créant un langage homogène. Robert KAHN de l'ARPA et Vinton CERF, professeurs à Standford, inventèrent un ensemble de protocoles de transmissions et de routage portant le nom de Transmission Control Protocol / Internet Protocol (TCP/IP).

[9] VIVANT M, Biens informationnels, JCP éd G 1984, I, no 3132.

[10] MATHIEU M-E, Transactions bancaires et financiers à distance, Juris- Classeur, Banque - Crédit – Bourse, 2004, Fasc.125.

[11] Les premières banques opérant via Internet datent de plus de 15 ans et les applications mobiles presque 10 ans. Fédération Bancaire Française, L'année de la banque en 2016, p. 20.

[12] Quand un client vient à la banque pour émettre une carte de paiement, il dispose de deux instruments de paiement : une carte de paiement en plastique et un compte de carte de banque. Par le biais de la carte, le client peut payer dans les magasins (avec POS-terminaux), retirer des espèces aux distributeurs automatiques et payer des biens / services sur Internet (en utilisant le numéro de carte et code).

6. Pour définir la banque électronique, il serait utile de rappeler la définition d'une banque. C'est « *une entreprise dont l'objet essentiel est d'employer, pour son propre compte, en opérations de crédit, les fonds qu'elle reçoit du public* » (art. 121 du Code de la Monnaie et du Crédit Libanais). Et l'article L511-1 du code monétaire et financier français dispose que « *les établissements de crédit sont des personnes morales qui effectuent à titre de profession habituelle des opérations de banque au sens de l'article L. 311-1* ».

7. La Directive Européenne 2002/65/CE du 23 septembre 2002 relative à la commercialisation à distance de services financiers auprès des consommateurs[13] (DSF) définit le prestataire ou fournisseur des services bancaires comme étant « *toute personne physique ou morale, publique ou privée, qui dans le cadre de ses activités commerciales ou professionnelles est le fournisseur contractuel des services faisant l'objet de contrats à distance* ».

8. La banque électronique peut être définie comme toute activité bancaire destinée à un client ou à un prospect, se déroulant à partir d'un point de service électronique[14] et utilisant un système de télécommunication tel que le réseau téléphonique, la Télévision Par Satellite (TPS), ou internet.

9. La banque en ligne est donc un système basé sur le réseau internet qui permet aux clients d'une banque d'accéder à leurs comptes et à des informations générales sur les produits et services bancaires et de faire des transactions en ligne, via un ordinateur ou tout autre dispositif intelligent. De plus en plus, nous témoignons des consultations de compte en ligne, des virements électroniques, des commandes de chéquiers, des souscriptions de crédit en ligne, d'achats d'actions en ligne et autres opérations.[15]

[13] Cette directive a modifié les directives 90/619/CEE, 97/7/CE et 98/27/CE SF.

[14] Par exemple, téléphone, micro-ordinateur, téléviseur, distributeur automatique de billets DAB (Distributeur automatique de billets Guichet automatique bancaire), guichet automatique de banque GAB (Guichet automatique bancaire).

[15]« Opération Audit de la banque en ligne », étude réalisée par la CNIL au 1er semestre 2005, p.2.

10. La définition des transactions bancaires en ligne peut être déduite de l'article premier de la directive 98/48[16]. Il s'agit «*de tout service presté, normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de service*»[17].

11. Le droit libanais a consacré la notion d'opérations financières et bancaires par moyens électroniques[18]. Il s'agit de transactions ou activités, conclues, exécutées ou développées par des moyens électroniques ou télématiques (téléphone, ordinateur, internet, distributeur automatique, etc.) par les banques, intermédiaires financiers, organismes de placement collectif ou par tout autre groupement ou établissement. Cette notion englobe toutes les opérations accomplies par les émetteurs ou distributeurs des cartes de crédit ou de paiement électroniques de toute nature, les opérations de virement de somme d'argent électronique, tous les sites d'offre, d'achat et de vente, tous les sites proposant des services électroniques relatifs aux différents instruments financiers ainsi que tous les centres de compensation qui leur sont liés[19].

12. La prolifération de ce nouveau type de banque a eu des conséquences avantageuses notamment quant à la suppression des contraintes traditionnelles au niveau temps, de la distance et du coût des transactions qui ralentissaient le développement des services et des activités et saturaient les bureaux des employés par des formalités papier.

---

[16] Directive 98/48/CE du Parlement européen et du Conseil du 20 juillet 1998 portant modification de la directive 98/34/CE du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques.

[17] Selon la directive 98/48 article 2-1 « *Aux fins de la présente définition, on entend par :*
le terme « à distance » : un service fourni sans que les parties soient simultanément présentes, – « par voie électronique» : un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques,

[18] Décision de la BDL n° 7548 du 30 mars 2000, JO n°15 du 6 avr. 2000, 1362. La Décision de la BDL n° 7548 réglemente l'exercice desdites opérations. De même, l'arrêté n° 7547 du 30 mars 2000 relatif aux réseaux informatiques a instauré auprès des banques, des réseaux informatiques auxquels elles sont obligées de se «connecter » sous peine de sanctions administratives. Egalement, l'arrêté n° 8341 du 24 janvier 2003 règlemente la *«compensation électronique des cartes de paiement et de crédit ».*

[19]Nammour F. Cours de Droit Bancaire. p.2

13. Ainsi, l'activité en ligne s'adapte aux besoins des clients (surtout professionnels) souhaitant réaliser leurs opérations routinières à tout moment de la journée[20] et en tout lieu où ils se trouvent (même lors de leur déplacement) sans devoir se rendre aux sièges des banques strictement durant les jours ouvrables et horaires indiqués par la banque. Conséquemment, l'internet a facilité la mondialisation de l'économie et les paiements transfrontaliers.

14. De même, l'internet se caractérise par la souplesse des transactions, de l'échange d'informations, et de la passation de commandes. D'ailleurs la conclusion des contrats en ligne s'effectue pratiquement par un simple clic entre des personnes situées dans différents pays et continents.

15. En parallèle, la transaction bancaire en ligne rend plus rentable l'activité de la banque grâce à l'économie de temps et de personnel. La banque a l'opportunité d'expansion et de multiplication des produits simples et les marchés financiers évoluent plus rapidement sans recours à des agents ou intermédiaires.

16. La banque en ligne participe à l'inclusion financière en assurant, à tous les individus et entreprises, même localisés dans des zones démunies ou agricoles d'un tiers monde, la possibilité d'accès à moindre coût à toute une gamme de produits et de services financiers utiles et adaptés à leurs besoins (transactions, paiements, épargne, crédit et assurance) proposés par des prestataires fiables et responsables. Les banques en profitent sans avoir à ouvrir des branches ou succursales dans lesdites zones.

17. Pour bénéficier des avantages des transactions bancaires en ligne, une condition primordiale s'impose, c'est la sécurisation de ces transactions qui implique la protection à la fois du cyberconsommateur ou client internaute et de la banque en vue de contourner

[20] Les défenseurs de l'e-banking affirment qu'il est plus rapide, mieux, et moins onéreux que les agences traditionnelles. « Faster/better/cheaper » est devenu l'adage du commerce électronique, alors que « anything/anytime/anywhere » est devenu celui des consommateurs : Gup, Benton E., The Future of Banking. ed., Greenwood Press, 2003.Available at SSRN: https://ssrn.com/abstract=333420.

tout genre de risques financiers (opérationnels, juridiques, de réputation[21], etc.), pouvant être engendrés par internet. Cette condition est la sécurisation qui instaure la confiance. Cette hypothèse est confirmée par la Fédération du E-commerce et de la Vente à Distance (FEVAD[22]) selon laquelle « *la confiance est un élément essentiel au développement de la vente à distance. Et ce n'est certainement pas un hasard si, au cours des dernières années, la courbe des ventes sur internet a suivi celle de la confiance des internautes* » et que la moitié des consommateurs français fait aujourd'hui confiance à internet. [23]

18. Accéder aux transactions bancaires en ligne soulève une question primordiale comment assurer la sécurisation dans les banques opérant dans le cyberspace ?

19. Par définition, la sécurisation désigne l'action de procurer la sécurité à quelque chose ou à quelqu'un et d'éviter le risque. Par définition, un risque financier est un risque de perdre de l'argent à la suite d'une opération financière (sur un actif financier) ou à une opération économique ayant une incidence financière (par exemple une vente à crédit ou en devises étrangères).

20. D'autres questions se posent au niveau de la sécurisation procurée par la loi: Quelles sont les règles applicables à l'internet ? Faut-il édicter des règles spécifiques aux activités et transactions ayant lieu via internet ou les règles existantes sont suffisantes ou peuvent être interprétées extensivement pour les inclure ?

21. Le Conseil d'Etat français a tranché cette polémique en décidant que « *les questions juridiques suscitées par le développement d'Internet et des réseaux numériques ne sont pas de nature à remettre en cause les fondements mêmes de notre droit* », au contraire, «*l'ensemble de la législation existante s'applique aux acteurs d'internet*».

[21] L'utilisation d'internet augmente le danger d'une perte de crédibilité de la part du public - et non seulement des clients - face à des dysfonctionnements : problèmes techniques, fraudes, malversations, déni de service, détournements d'utilisation, propagandes répréhensibles.

[22] La FEVAD est un syndicat professionnel français créé en 1957, regroupant plus de 500 entreprises ayant une activité de vente à distance quel que soit le moyen de communication utilisé (Internet, correspondance, téléphone, etc.).

[23]FEVAD, rapport 2010, p 3, disponible sur : http://www.fevad.com/images/Publications/ra2010.pdf.

22. A la problématique soulevée par notre sujet, à savoir la sécurisation des transactions bancaires en ligne, nous pouvons riposter que plusieurs dispositions législatives au niveau national et international ont été édictées pour faire régner la confiance en ces transactions.

23. Effectivement, le législateur devant le développement et l'expansion des nouvelles technologies n'a pu rester muet surtout que des problèmes juridiques en ont jaillis. Ainsi, nous confirmons avec M. De LAPRADELLE que « *ce ne sont pas les philosophes avec leurs théories, ni les juristes avec leurs formules, mais les ingénieurs avec leurs inventions qui font le droit et le progrès du droit* »[24]. Ceci décrit la relation entre le droit et le progrès technologique qui se traduit par le constat que toute technologie nécessite l'édiction d'une loi pour l'encadrer et délimiter ses inconvénients et abus.

24. En droit libanais, en l'absence des textes législatifs, la Banque Centrale ou Banque du Liban (BDL), qui veille au bon fonctionnement et à la sécurité du secteur bancaire, a décrété des circulaires et décisions visant à régir les services bancaires en ligne et a édicté les conditions et mesures requises en vue d'organiser et d'assurer l'efficacité et la confiance dans les transactions bancaires en ligne. Parmi ces circulaires et décisions figurent principalement la décision de base sur les opérations financières et bancaires par voie électronique du 3 mars 2000, la décision de base n° 7548 du 3 mars 2000 sur les opérations financières et bancaires par voie électronique, la décision de base no. 8710 sur les opérations électroniques et bancaires par voie électronique, la décision intermédiaire no. 11445 en date 6 juin 2013, la décision de base n° 8341 du 24 janvier 2003 relative à la compensation électronique des cartes de paiement et de crédit la décision intermédiaire, la décision de base no. 12725 du 28 novembre 2017 relative à la prévention des actes criminels électroniques, la décision de base n. 12872 du 13 septembre 2018 relative à la protection des données personnelles, etc.

25. En Europe, le législateur communautaire s'est préoccupé par la matière des services financiers en ligne et a jugé nécessaire d'harmoniser les règles applicables pour instaurer la

[24]COLLIARD (C.A), « La machine et le droit privé français contemporain », Mélange offert à Georges RIPERT, Paris, L.G.D.J., 1950, p. 115.

confiance et assurer un développement législatif continu des activités sur internet. De ce fait, le parlement européen a édicté à ce sujet plusieurs directives[25] protectrices, qui ont réussi à dissiper les craintes et vaincre la réticence initiale à utiliser internet.

26. Le législateur européen fut suivi par le législateur français qui, dans le but de transposer le contenu des directives européennes, a modifié ou édicté des lois nationales dont la principale en la matière est la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[26].

27. Ces règles spéciales sur le commerce ou banque électronique se conjuguent avec les règles générales. Ainsi, en l'absence de règlementation spécifique à la cyberbanque ou de droit des nouvelles technologies et activités sur internet, l'encadrement des transactions bancaires en ligne par de nouvelles règles n'est donc pas exclusif de l'application des dispositions existantes relative aux diverses branches de droit notamment le code monétaire

[25]Les directives et règlements européens relatifs à notre sujet sont les suivants :
- Directive n°93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.
- Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («Directive sur le commerce électronique»).
- Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs.
- Directive 2005/60/CE du Parlement Européen du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.
- Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.
- Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE sur les signatures électroniques.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) mis en vigueur mai 2018.

[26] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004 p. 11168. Elle a transposé la Directive du commerce électronique.

et financier[27], le droit des obligations ou code civil, le droit de la consommation[28] mais aussi le droit commercial.

28. Nous affirmons, dès à présent, que les banques en ligne proposent les mêmes services que les banques traditionnelles tels que le compte bancaire avec ses moyens de paiement (carte, chéquier) et de transfert de fonds (virement, prélèvement, etc.), des crédits à la consommation et immobiliers, des livrets d'épargne, de l'assurance vie, l'accès à la bourse, etc. Par conséquent, les risques financiers qui existent dans le secteur bancaire traditionnel se retrouvent dans le secteur bancaire généré par les nouvelles technologies. Cependant les risques de ces dernières sont plus accentués et proviennent aussi d'infractions nouvelles engendrées par l'internet.

29. En effet, il s'agit de distinguer entre la criminalité non-informatique sur internet et la criminalité informatique sur internet[29]. La première englobe les crimes traditionnels commis par le biais de l'internet. Dans ce cas, l'internet n'est que le moyen utilisé pour réaliser les actes criminels normalement commis hors ligne tels que le vol, l'escroquerie, l'abus de confiance, la diffamation, etc. Quant à la deuxième criminalité, elle englobe les infractions qui ont pour but et pour cause l'internet. Dans ce cas, nous sommes en présence de nouvelles infractions liées au monde virtuel tels que l'attaque d'un système informatique ou site web ou encore l'atteinte aux informations confidentielles à titre d'exemples.

30. Les réflexions menées dans le cadre de ce mémoire font apparaître que malgré les avantages procurés par Internet, cet outil permet également l'existence d'un certain nombre de menaces pesant sur les transactions bancaires en ligne, d'où la nécessité d'en sécuriser le cadre. C'est ce que nous proposons de faire en analysant le cadre contractuel des transactions bancaires en ligne (Partie I) avant d'aborder le cadre institutionnel de cette catégorie particulière de transactions (Partie II).

---

[27] Au Liban : Code de la monnaie et du crédit et la Loi sur le secret bancaire du 3 septembre 1956 : JO no 36, 5 sept. 1956. En France : Code monétaire et financier.

[28] Au Liban : Loi no 659-du 4 février 2005 sur la protection du consommateur. En France : code de la consommation.

[29] ISSA (T), L'organisation légale de l'internet, Sader 2001, p. 24

Partie 1 : Sécurisation du cadre contractuel

31. La transaction bancaire conclue en ligne ne déroge pas à la règle du droit commun qui exige la rencontre de la volonté des deux cocontractants. S'agissant d'un contrat électronique entre personnes non présentes physiquement, le contrat est conclu par un « double clic ». L'internaute doit dans un premier temps avoir la possibilité de vérifier le détail de sa commande et son prix total (taxe inclue) et de corriger les erreurs éventuelles : il s'agit du « premier clic ». Puis, s'il décide de poursuivre sa commande, il doit avoir la possibilité de confirmer sa commande par un « second clic » et de conclure ainsi définitivement le contrat électronique qui le lie au cybervendeur.

32. Cette condition est imposée par la LCEN sous peine de nullité du contrat. Techniquement la conclusion de la transaction en ligne se réalise à l'issue de trois messages successifs échangés sur l'écran message relatif à la passation de la commande par le client, message par la banque accusant réception, et message par lequel le client confirme son acceptation.

33. D'où allons-nous exposer dans un premier temps la sécurisation de l'identité du client internaute (Titre 1) et dans un deuxième temps la sécurisation du consentement de ce client et de ses données personnelles (Titre 2).

Titre 1 : Sécurisation de l'identité du client internaute

34. Le consommateur[30] ou client internaute est la personne qui accède à internet aux fins de consultation, de correspondances privées ou courrier électronique, mais aussi de transactions commerciales et bancaires. Le cocontractant de la banque en ligne c'est le client qui peut être toute personne physique ou morale agissant à titre privé ou professionnel.

35. En droit libanais, le consommateur est défini par la loi de la protection du consommateur comme étant toute personne physique ou morale qui achète, loue, utilise ou bénéficie d'un service ou produit à des fins non liées directement à son activité professionnelles (art. 2).

36. En droit français, le consommateur est défini comme « *toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale*»[31]. Cette définition est inspirée de l'article 2 (d) de la DSF 2002[32], qui définit le consommateur comme étant « *toute personne physique qui, dans les contrats à distance, agit à des fins qui n'entrent pas dans le cadre de son activité commerciale ou professionnelle* ».

[30]Le terme "consommateur" fait l'objet de diverses définitions, ainsi dans :

- la convention de Bruxelles de 1968 (modifié par le règlement communautaire du 22 décembre 2000) ;
- la Convention de Rome de 1980 ;
- la directive 93/13/CEE du Conseil, du 5 avril 1993, concernant les clauses abusives dans les contrats conclus avec les consommateurs ;
- la directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.

[31] La loi n°2014-344 du 17 mars 2014, dite « Loi Hamon », a inséré un nouvel article préliminaire dans le Code de la consommation portant définition du « consommateur ». Cette définition est issue de la directive n°2011/83 du 25 octobre 2011 relative aux droits des consommateurs.

[32] Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs, et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE.

37. Il en résulte que ne peuvent être considérés comme consommateur les sociétés, les associations, les syndicats de copropriétaires ainsi que toute autre entité qui ne remplit pas la définition de consommateur donnée par le Code de la consommation. Cependant en matière de transaction bancaire en ligne, nous considérons que ces entités doivent bénéficier du régime protecteur du consommateur nonobstant leurs identités professionnelles puisqu'elles sont profanes en matière bancaire et leur professionnalisme se borne à leurs spécialisations et objets.

38. Nous allons cerner les conditions d'éligibilité du client (Chapitre 1) pour vérifier ensuite les procédés d'authentification de la transaction bancaire en ligne (Chapitre 2).

Chapitre 1 : Les conditions d'éligibilité du client internaute à la transaction bancaire en ligne

39. Agir sur internet est certes une liberté totale[33]. Créer un email, visiter des sites et des plateformes, commenter, télécharger, communiquer des informations se font en principe librement sans aucune condition préalable. D'ailleurs, cette liberté est due aux caractéristiques inhérentes à l'internet à savoir la dématérialisation, la délocalisation et surtout la dépersonnalisation.

40. Néanmoins, lorsqu'il s'agit d'entreprendre des transactions bancaires, cette liberté doit être encadrée[34] pour être sécurisée contre certains risques majeurs tels que vol, usurpation d'identité, blanchiment d'argent[35], etc.

41. Nous allons démontrer dans une première section que la capacité légale du client internaute est garantie de son consentement (Section 1) et exposer dans une seconde section l'identification du client internaute (Section 2).

[33] Au Liban, cette liberté trouve son justificatif dans le principe de la liberté d'expression consacrée à l'article 13 de la Constitution libanaise qui dispose : « *La liberté d'exprimer sa pensée par la parole ou par la plume, la liberté de la presse, la liberté de réunion et la liberté d'association, sont garanties dans les limites fixées par la loi* ». En France, le chapitre premier intitulé « la liberté de la communication en ligne » de la LCEN dispose dans son article premier que « *la communication au public par voie électronique est libre* ». Cependant cette liberté se trouve limitée par certaines conditions invoquée dans ce même article à savoir : «*d'une part le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, la sauvegarde de l'ordre public, les besoins de la défense nationale, les exigences de service public, les contraintes techniques inhérentes aux moyens de communication, ainsi que la nécessité, pour les services audiovisuels, de développer la production audiovisuelle*».

[34] Les premières limites à la liberté totale ont été imposées aux Etats-Unis par l'Organisation ISOC (Internet Society Club), un club international des enthousiastes de l'internet daté 1992 non-profitable.

[35] Trois facteurs aggravent les risques de blanchiment dans le cas de services en ligne : la facilité d'accès à un service sans contrainte géographique (matérielle ou temporelle), la dématérialisation, la rapidité de prise en compte des ordres.

Section 1 : La capacité légale de l'internaute, une garantie de son consentement

42. La transaction en ligne étant une transaction délicate qui touche aux fonds des personnes et peuvent leur causer des dommages importants, le législateur et les autorités de tutelle du secteur bancaire veillent à encadrer l'activité bancaire sur internet et lui assurer une base de sécurisation solide. D'où l'exigence de certaines conditions d'accès à l'activité bancaire en ligne qui sont prévues dans le droit commun quant à la capacité du client internaute et dans les recommandations de la Banque des Règlements Internationaux quant à son identification.

43. Quel internaute peut être partie à la transaction bancaire en ligne ? Doit-il être investi d'une certaine capacité ? Nous allons développer dans ce qui suit la capacité du client internaute, personne physique (Paragraphe 1) pour ensuite vérifier la capacité du client internaute, personne morale (paragraphe 2).

Paragraphe 1 : La capacité du client internaute, personne physique

44. Le principe est que « *toute personne peut contracter si elle n'est pas déclarée incapable par la loi*» (art. 1145 du Code Civil français).

45. La capacité est l'aptitude d'une personne à être titulaire d'un droit (capacité de jouissance) et à l'exercer (capacité d'exercice). Cette exigence de capacité légale contribue à assurer un minimum de sécurisation. Une personne jouissant de capacité légale est présumée pouvoir repérer plus facilement les risques et tentatives de fraude et prendre les précautions appropriées.

46. L'article 125 du COC requiert en plus de la capacité, la majorité. Dans le même sens, la BDL dans sa décision de base no. 7548 (art. 21) précise que « *l'âge du client ne doit pas être inférieur à dix-huit ans et qu'il doit jouir de la capacité totale de contracter* ».

Cette exigence de majorité implique le discernement et la compréhension par le client de la portée matérielle, morale et juridique de ses actes et actions.

47. Ainsi, la banque doit demander des preuves que le client est majeur. En présence d'un doute au sujet du statut juridique, la banque doit vérifier la capacité du client à conclure l'acte envisagé. D'ailleurs, la banque peut s'assurer de la capacité par le recours à des documents identifiant l'âge et la capacité.

48. En matière civile, lorsque la personne n'a pas accédé à l'âge de majorité, c'est son représentant légal, généralement un de ses parents, qui doit contracter au nom et pour le compte du représenté mineur.

49. Qu'en est-il en matière d'internet ? Est-ce le même principe prévaut ? Faut-il modifier la loi civile en la matière pour régir les transactions bancaires en ligne ?

50. Nous considérons qu'en l'absence de dispositions légales spécifiques à l'espace virtuel, les dispositions du droit commun doivent s'appliquer aux opérations en ligne. D'ailleurs, nous jugeons qu'il n'y aurait pas de valeur ajoutée si le législateur transpose les mêmes dispositions législatives du droit hors ligne pour les reformuler dans une cyberloi sachant que les mêmes principes de droit seront applicables.

51. Par rappel des principales règles relatives à la capacité à conclure des actes bancaires, en droit libanais, le mineur dépourvu de discernement n'a pas la capacité civile et ne peut faire des actes bancaires même les plus simples (ouvrir un compte bancaire) (art. 216 al. 1 COC). En revanche, le mineur doué de discernement peut conclure des transactions bancaires. Cependant celles-ci ne sont annulables que par la mineur lui-même que le législateur a voulu protéger (art. 216 al. 2 COC) et à condition de prouver qu'il a été victime de lésion (art. 216 al. 3 COC). Toutefois, le mineur habilité jouit d'une capacité spéciale concernant l'exercice d'activités commerciales (art. 217 COC)[36].

[36] La banque est-elle tenue de vérifier si les transactions effectuées en ligne par le mineur habilité s'inscrivent dans le cadre de son activité commerciale ? La banque est tenue d'être vigilante en présence d'actes graves.

52. En droit français, le mineur peut entreprendre des activités quotidiennes et habituelles (art. 481 CCiv.) sauf pour les actes nécessitant l'intervention du représentant (art.389 et 450 CCiv.).

53. Pratiquement, les banques n'acceptent pas d'ouvrir des comptes bancaires[37] à des mineurs ou personnes majeures protégées sans l'accord exprès d'un parent ou d'un tuteur légal. La banque est tenue légalement de vérifier la qualité du représentant du mineur et obtenir un mandat notarié stipulant expressément les pouvoirs du mandataire entre autres ouvrir et fermer un compte bancaire, mettre et retirer des fonds, etc. et la banque est tenue d'appliquer ce mandat littéralement sans aucune interprétation extensive (art.3 de la décision 7818 de la BDL).

54. Qu'en est-il du mineur de mauvaise foi ? Si le mineur utilise la carte bancaire internet de ses parents et donne ordre à la banque qui effectue la transaction, la banque ne pouvant pas vérifier si le donneur d'ordre était le mineur ou ses parents, peut se baser sur la théorie de l'apparence[38] ou encore sur les règles de responsabilité délictuelle, et la responsabilité des parents des actes commis par leurs enfants. Par conséquent, nous estimons que, dans de tels cas, les parents assument les actes en ligne de leurs enfants.

55. Notons qu'en pratique, plusieurs sites requièrent de la part de l'internaute de certifier qu'il est majeur en affichant une alerte. Ce n'est qu'à la suite de la confirmation par l'internaute qu'il a atteint l'âge de la majorité que la procédure en ligne s'ouvre. Cette confirmation est requise à la suite d'un questionnaire à remplir par l'internaute qui sert à détecter des indices à cet égard.

Cependant sa responsabilité ne peut être engagée du fait du devoir de non-ingérence. Ainsi, la banque n'est pas responsable lorsqu'il y a eu un détournement des sommes empruntées par le mineur sauf connaissance préalable, chose difficile à prouver.

[37] Chaque ouverture de compte nécessite de la part de la banque une interrogation à la Banque Centrale (en France comme au Liban) afin de vérifier que le client n'est pas frappé d'une interdiction d'émettre des chèques, n'est pas sur la liste du centre des risques ou n'a pas fait un usage abusif de sa carte bancaire.

[38] Nassif E., Le contrat électronique en droit comparé, Al Halabi Law Publishers, éd. 2009, p. 125.

Paragraphe 2 : La capacité du client internaute, personne morale

56. Le client internaute ou destinataire du service bancaire via internet peut être un professionnel aussi bien qu'un consommateur profane. Qu'il s'agisse d'un contrat B2B ou B2C[39], l'internaute est soumis aux mêmes obligations et surtout aux mêmes conditions de capacité et d'exigences légales.

57. La loi française vise sur le même plan de protection le consommateur professionnel et le consommateur profane. Et la jurisprudence est allée plus loin en adoptant une définition extensive du consommateur considérant qu'une personne morale peut jouir de la protection si elle était au sujet du contenu du contrat « *dans le même état d'ignorance que n'importe quel autre consommateur »*[40].

58. La jurisprudence a ensuite nuancé ce concept et a adopté une vision plus restrictive en délimitant le domaine de protection aux contrats n'ayant pas un rapport direct avec son activité professionnelle[41]. Cette jurisprudence nous semble bien équitable.

59. La personne morale doit prouver sa capacité de conclure des transactions en ligne en fournissant ses documents légaux (en France, extraits Kbis ; au Liban, les documents d'immatriculation à savoir statuts, circulaire, certificat d'immatriculation, etc.). Elle doit également présenter des justificatifs sur le statut et les pouvoirs des personnes physiques agissant en son nom et pour son compte. Lesdits pouvoirs sont généralement mentionnés dans une circulaire ou un procès-verbal de la réunion de l'organisme qualifié qui mentionne le nom du signataire autorisé, les pouvoirs de ce dernier ainsi que le modèle de sa signature.

[39] B2B pour « business-to-business » : relations interentreprises B2C pour « business-to-consumer»: relation entreprises- consommateurs/particuliers

[40]Cass. 1e civ. 28 avril 1987, D. 1988.1 note Delebecque.

[41]Cass. 1re civ. 24 nov. 1993, D. 1994 som. com. p. 236, obs. Paisant, Defrénois, 1994 p. 818 obs. D. Mazeaud , Cass. 1re civ. 21 fév. 1995, JCP 1995.II.22502, n. Paisant).

60. Si la société est encore en phase de formation, le représentant fondateur doit être investi des pouvoirs nécessaires pour agir pour le compte de la société en formation. D'ailleurs la banque, en ouvrant un compte bancaire pour la société en formation, précise qu'il s'agit d'une société en formation et elle bloque ledit compte jusqu'à la soumission des documents officiels prouvant l'immatriculation définitive de la société.

61. En outre, le banquier est obligé de s'informer sur la capacité légale de son client mais aussi sur sa situation financière ainsi que ses objectifs afin de lui recommander les services les plus adaptés à sa situation (art. L.533-13 du Code monétaire et financier français). Par exemple, en cas de demande de crédit, la banque doit être vigilante quant aux documents présentés par le client. D'ailleurs même si la banque a une liberté d'appréciation de ces documents, elle doit vérifier la véracité des postulats qui seraient à leurs origines notamment si ce sont des documents prévisionnels.

62. Pour conclure, la sécurisation des transactions bancaires en ligne exige que le banquier puisse identifier correctement son interlocuteur.

Section 2 : L'identification du client internaute

63. Dans le secteur bancaire, l'identification du client est un processus primordial qui préoccupe non seulement le législateur, mais aussi les banques elles-mêmes puisque quiconque peut profiter de la dématérialisation, de l'automatisation des opérations et de la dépersonnalisation des relations avec le banquier pour effectuer des opérations de blanchiment[42], fraude ou autres.

64. L'identification de la clientèle des transactions bancaires en ligne n'est pas très différente de l'identification des clients hors ligne. Nous allons exposer dans ce qui suit l'identification classique du client ou KYC (Paragraphe 1) puis développer l'identification électronique ou E-KYC (Paragraphe 2).

Paragraphe 1 : Identification classique du client ou KYC

65. L'identification du client figure parmi les 14 principes relatifs à la gestion du risque de la banque électronique édictés par la Banque des Règlements Internationaux [43]. Par conséquent, toute banque, opérant en ligne ou hors ligne, est tenue, de par la loi, d'avoir une connaissance actualisée de tous ses clients[44] y compris leurs revenus et patrimoines et à suivre leurs opérations. C'est l'obligation de « *Know Your Customer* » (KYC) c'est-à-dire s'informer sur ses clients, imposée par les législations anti-blanchiment[45].

---

[42] L'internet constituant un nid idéal pour les auteurs de
, a non seulement crée de nouveaux moyens, mais a aussi facilité la mise en œuvre des techniques traditionnelles de blanchiment telles que l'utilisation de services bancaires dans des centres illusoires ou création de sociétés écrans.

[43] Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, July 2003, www.bis.org

[44] Article L. 561-5 et 562-1du code monétaire et financier– CMF. L'obligation consiste en une double exigence de «connaissance actualisé » du client et d' « examen attentif des opérations effectués » afin que la banque soit toujours en mesure d'évaluer la cohérence des opérations en question en fonction de la connaissance qu'il a du client.

[45] Directive 2005/60/CE du Parlement Européen du 26 octobre 2005.
En France, l'article 561- 5 « mesures de protection » introduites par la loi no. 90-614 du 12 juillet 1990 relative à la participation des organismes financiers à la lutte contre le blanchiment des capitaux. Au Liban,

66. Ces dernières imposent aux banques d'aller plus loin et de vérifier non seulement les identités réelles des clients, mais surtout d'identifier le bénéficiaire effectif ou l'ayant droit économique de la transaction envisagée[46]. Dans cette même lignée, le législateur américain a édicté la loi fiscale « FATCA[47] » dont la nouveauté vise à détecter tout acte de blanchiment grâce à la traçabilité des activités de son auteur au niveau international par le biais d'échanges des informations financières[48]. Le législateur libanais a mis en vigueur les obligations de cette loi américaine par le biais de la loi no. 55 relative à l'échange d'informations à des fins fiscales, édictée par le gouvernement en date du 27 octobre 2016.

67. Nous allons énumérer les moyens d'identification (A) avant d'exposer les conséquences du manquement à cette obligation d'identification (B).

---

loi no. 318 du 20 avril 2001 sur la lutte contre le blanchiment de capitaux et loi no. 42 du 24 novembre 2015 relative au transport transfrontalier de l'argent liquide.
Au Liban : Loi libanaise no. 44 du 24 octobre 2015- La loi no. 318 du 20 avril 2001 relative à la lutte contre le blanchiment de capitaux.- La Décision no.7818 BDL qui consacre un titre à la vérification de l'identité du client et la précision du bénéficiaire de l'opération - Décision de Base de la BDL no. 10965 relatives à la relation entre les banques et institutions financières et leurs correspondants. Circulaire Intermédiaire no. 498 du 13/6/2018.

[46] Art. 1 de la Décision de base de la BDL 10965 du 5 avril 2012.

[47] https://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx: Foreign Account Tax Compliance Act (FATCA) est un règlement du code fiscal des États-Unis qui oblige les banques des pays ayant accepté un accord avec le gouvernement des États-Unis à signer avec le Département du Trésor des États-Unis un accord dans lequel elles s'engagent à lui communiquer tous les comptes détenus par des citoyens américains. La particularité du système fiscal américain est que cette notion couvre, outre les résidents aux États-Unis, les citoyens de cet État résidents à l'étranger, les titulaires d'une carte de résident permanent aux États-Unis, leurs conjoints et enfants, ainsi que toutes personnes, indépendamment de leur résidence ou nationalité, qui ont des biens substantiels aux États-Unis. Il a été adopté dans le cadre de la loi du Congrès Hiring Incentives to Restore Employment Act signé par le président Obama le 18 mars 2010. Le système prévoit des pénalités pour les récalcitrants, pouvant aller jusqu'à la clôture forcée du compte d'un particulier ou un prélèvement d'un impôt sur 30 % de la valeur d'un investissement aux États-Unis.

[48] Ainsi lorsqu'un client dépose une somme d'argent sans rapport avec ses revenus ou sa situation patrimoniale, le banquier doit lui demander l'origine de ces fonds et réclamer des justificatifs probants (déclaration de succession, acte de vente, etc.).

A- Les moyens d'identification

68. L'identification se fait par le biais de vérification de tout document écrit à caractère probant. Pour ce, le client doit fournir tout document requis et doit communiquer à la banque toute information nécessaire qui permet de l'identifier et le distinguer de tout autre intervenant faussement semblable.

69. La banque peut aussi demander à son client de justifier son domicile (pour s'assurer de la véracité de l'adresse[49], elle peut lui envoyer un courrier avec accusé de réception[50] ou même par la présentation d'une facture d'électricité ou télécommunications, acte de propriété ou contrat de location[51]). Elle doit l'interroger sur les opérations qu'il envisage (montant, nature, la provenance et la destination des fonds, la justification économique ou le fonctionnement prévu de son compte) ou sur son statut juridique ainsi que sa situation professionnelle, économique et financière (activité, revenus ou tout élément permettant d'estimer ses ressources et d'apprécier son patrimoine), de comprendre ses motivations et de lever l'éventuel doute sur les conditions dans lesquelles l'opération est entreprise. En cas d'un client ancien, il est possible que la banque renouvelle cette démarche afin d'actualiser son dossier.

70. La Banque du Liban impose l'identification du client et de son domicile par le biais de documents officiels. Elle impose la conservation des documents retenus au sujet de l'identification et domiciliation pour au moins cinq ans après l'exécution de l'opération ou clôture du compte (art. 9 bis décision de base 7548 du 30 mars 2000 tel que ajouté par la décision intermédiaire 12018 daté 30 juin 2015).

71. L'identification peut se faire au niveau de la signature. Les banques requièrent lors de l'ouverture d'un compte, un spécimen de signature permettant à la banque d'identifier le donneur d'ordres en opérant un contrôle sur sa signature[52].

---

[49] Article 33 du décret 92-456 daté du 22 mai 1992.

[50] Dans ce cas, la vérification se fait à distance mais pas en ligne : MATHIEU Marie- Elisabeth, « Transactions bancaires et financières à distance, Juris-Classeur, Banque –Crédit – Bourse 2004, FASC. 125.

[51] Bonneau Th., Droit Bancaire, Montchrestien, 4e éd. 2002 p. 222.

[52] NAMMOUR (F.), Droit Bancaire 2003, p. 225.

72. De même, la banque requiert parfois deux copies de justificatifs d'identité différents en vue de les comparer et de détecter une potentielle falsification. Dans cette même perspective, les banques en ligne ont recours à l'authentification qui associe deux facteurs à divulguer cumulativement par le client ce qui confirme son identité et entrave les actes d'usurpation d'identité.

73. Sur la même lignée, la banque peut vérifier l'identité du client en sollicitant ses coordonnées auprès d'autres établissements. Par exemple, la banque peut requérir un numéro de compte déjà existant auprès d'une autre banque ce qui implique que cette dernière a déjà entreprit la procédure de vérification.

B- Le manquement à l'obligation d'identification

74. Le manquement à cette obligation d'identification du client engendre la responsabilité disciplinaire, voire pénale de la banque si la transaction faite par cette personne dont la banque n'a pas bien vérifié l'identité, a causé un dommage aux tiers[53].

75. Lorsque la banque n'est pas en mesure d'identifier son client ou d'obtenir des informations sur l'objet et la nature de la relation d'affaires, elle ne doit exécuter aucune opération « *quelles qu'en soient les modalités* », et ne doit établir ni poursuivre aucune relation d'affaires (art. L. 561-2 code monétaire fr.) sous peine de voir sa responsabilité totale retenue[54].

[53] Responsabilité civile du banquier en matière de compte, Juris. Class. Banque, Fasc. 150, no. 9 et suivants.

[54]Cass. Com. 29 janvier 2002 n°260 FS-P+B Compagnie Préservatrice Foncière Assurance-Crédit Agricole du Finistère. La Cour de cassation française a retenu la responsabilité totale de la banque en décidant que :«*la banque réceptionnaire d'un virement, même électronique, ne peut se borner, avant d'en affecter le montant au profit d'un de ses clients, à un traitement automatique sur son seul numéro de compte, sans aucune vérification sur le nom du bénéficiaire, dès lors qu'il est inclus dans les enregistrements reçus du donneur d'ordres et qu'il n'a pas été exclu de tout contrôle avec l'assentiment de ce dernier* ».
Cass. Lib. Pourvoi no. 92, 11 oct. 1956, Baz 955 p.111. Cour Banc. Spec. No. 103/167 du 1 déc. 1998 Mebco (en liquidation) c/ BLOM Bank , citée par Sader « Les banques, droit et jurisprudence», p. 214.

Paragraphe 2 : Identification électronique du client internaute ou E-KYC

76. L'identification peut s'opérer par la vérification à distance des informations, par exemple au moyen de webcams et de documents scannés, ou la vérification par des tiers des documents originaux. Au Liban, la vérification électronique n'est pas admissible. Les documents doivent être soumis à la banque par le client en personne.

77. Dans le but de systématiser les modalités d'identification en ligne, l'Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, suivie d'un arrêté du 8 mars 2012 [55] fixent les garanties à respecter lors des procédures sécurisées relatives à la vérification des données à caractère personnel contenues dans les actes d'état civil effectuées par voie électronique. Les demandes de vérification et les réponses relatives sont transmises via une plateforme de routage qui permet de mettre en œuvre la procédure de communication électronique des données de l'état civil mise en place par l'agence nationale des titres sécurisés (ANTS) et pilotée par le ministère de la justice et des libertés.

78. Une nouvelle carte d'identité[56] a vu le jour récemment ainsi qu'un nouveau passeport[57] dotés d'une puce électronique comprenant les données suivantes : *« 1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ; 2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ; 3° Son domicile ; 4° Sa taille et la couleur de ses yeux ; 5° Ses empreintes digitales ; 6° Sa photographie» (art. 2 de la loi 27 mars 2012)* [58].

[55] JORF n°0065 du 16 mars 2012 page 4862 - texte n° 37.

[56] Loi n°2012-410 du 27 mars 2012 sur la protection de l'identité - JORF n°0075 du 28 mars 2012 p 5604.

[57] En Au Liban, la Sûreté Générale délivre depuis août 2016 des passeports biométriques dotés d'une puce électronique qui contient des informations biométriques pouvant être utilisées pour authentifier l'identité du détenteur du passeport. Il s'agit d'une technologie de carte à puce sans contact, une puce de microprocesseur et une antenne intégrée dans la couverture avant ou arrière, ou page centrale du passeport. Les informations critiques du passeport sont à la fois imprimées sur la page de données du passeport et stockées dans la puce. Ce document hautement sécurisé intègre un microprocesseur qui embarque des données photographiques et biométriques telles que les empreintes digitales, afin de permettre la vérification de l'identité du titulaire.

[58] Saisi sur la constitutionnalité des dispositions de cette loi, le Conseil constitutionnel français par une décision n°2012-652 du 22 mars 2012, a justifié la création d'un fichier de traitement des données à caractère

79. La délivrance de pièce d'identité électronique comprenant un composant électronique qui inclut les informations entre autres biométriques (empreintes digitales numérisées) de la personne, assure une grande fiabilité aux passeports et aux cartes nationales d'identité et consolide la lutte contre les délits d'usurpation d'identité. En cas de doute, il sera facile de vérifier l'identité de la personne en comparant les empreintes digitales numérisées contenues dans la puce électronique et les empreintes physiques de la personne en question.

80. Au Liban, les administrations publiques ont pris des initiatives très importantes érigeant en quelque sorte certains actes administratifs au plan électronique en reconnaissant l'identité électronique. Ainsi, le fisc[59] exige depuis quelques années la déclaration et le règlement des impôts en ligne.

81. Pour conclure, il serait intéressant d'évoquer que non seulement le client est identifiable mais aussi son ordinateur ou devis est identifiable. En effet, chaque devis qui se connecte à un réseau est doté d'un « *Internet Protocol* » (IP) qui est unique sans possibilité de duplication. Cet IP est primordial pour la connexion de la machine ou devis avec d'autres devis sur le réseau. Techniquement, l'IP permet de détecter l'origine d'un acte et son potentiel acteur. Néanmoins, il faut noter que parfois le devis peut ne pas être personnel à son utilisateur.

82. Nous soulignons l'importance de cet IP et suggérons d'en bénéficier davantage en créant un organisme chargée d'enregistrer les IP, les propriétaires des devis devant s'inscrire obligatoirement auprès de cet organisme par un seul IP et déclarer tout changement de propriétaire. Ce mécanisme peut s'inspirer du régime de transfert de la propriété des véhicules et automobiles.

83. Une fois la banque identifie son client, elle a besoin de mettre en œuvre certains procédés pour certifier et authentifier cette identification et la transaction en question.

---

personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage par l'amélioration des moyens de lutte contre la fraude.
http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-pardate /decisions-depuis-1959/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html

[59] Ministère des finances libanais Décisions no. 449/1 du 17 mai 2016 et no. 883/1 du 12 aout 2013 et no. 15/1 du 14 janvier 2016.

Chapitre 2 : Les procédés d'authentification de la transaction bancaire en ligne

84. Les rapports contractuels relatifs aux services bancaires sur internet se font pratiquement entre deux ordinateurs ou dispositifs. Cependant derrière ces écrans, des personnes physiques ou morales agissent. Comment la banque peut-elle garantir l'identité de ses cocontractants ?

85. Pour atteindre cet objectif, le règlement relatif à l'identification électronique et aux services de confiance pour les transactions électroniques[60] a apporté des solutions pour l'utilisation transfrontière de l'identification électronique et des services de confiance électroniques telle que les signatures électroniques, cachets électroniques[61], horodatages[62] électroniques, service d'envoi recommandé électronique et authentification de site web auxquels s'ajoutent d'autres procédures pratiques telles que l'envoi par des colis postaux séparés des identifiants personnels, clavier numérique [63] , ou même les codes d'authentification pour opérations sensibles[64]. Ceci permet d'identifier plus facilement leurs clients internautes ou d'obtenir une authentification[65] fiable des parties aux opérations de paiement.

[60] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014.

[61] Une attestation électronique associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne (Règlement (UE) nº 910/2014).

[62] L'horodatage est un ensemble de techniques consistant à associer de manière sûre une date et une heure de référence à des données, dans le but de prouver l'existence de ces données avant une certaine date3. Ce mécanisme est souvent utilisé conjointement avec la signature numérique. L'obtention d'une date et heure de référence nécessite généralement l'utilisation des services d'un tiers horodateur de confiance, ou autorité d'horodatage. La RFC 3161 définit un protocole d'horodatage applicable par une autorité d'horodatage.

[63] Ces claviers permettent l'insertion du numéro de client uniquement avec la souris, et ainsi lutter contre certains virus capables de stocker les touches tapées.

[64] Pour contourner tout acte par un potentiel mal intentionné qui parviendrait à se connecter dans un espace client, les banques en ligne font usage de codes d'authentification c'est-à-dire l'envoi automatique au titulaire du compte d'un SMS contenant un code à usage unique et sans lequel l'opération souhaitée est irréalisable.

[65] L'authentification c'est le mécanisme de sécurité qui permet de s'assurer de l'authenticité de l'émetteur ou du récepteur d'un message. L'authentification peut être simple (utilisation d'un mot de passe) ou complexe (recours au chiffrement). Authentification de l'origine des données c'est la confirmation que la source des données est telle que déclarée. Dictionnaire de l'informatique, sous la direction de Pierre Morvan, Larousse.

86. Nous allons démontrer dans ce qui suit que la signature électronique est un véritable procédé de sécurisation (Section 1) et développer ensuite l'authentification par une tierce personne (Section 2).

Section 1 : La signature électronique, un procédé de sécurisation

87. Par définition une signature a un double rôle significatif. Elle identifie, d'une part, son auteur et manifeste, d'autre part, son consentement. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte (l'article 1367 CCiv fr.).

88. Le législateur français consacre l'égalité de l'écrit électronique et de l'écrit papier lorsqu'un tel écrit est exigé *ad validitatem (*art. 1366 CCiv.*)*[66]. Cette reconnaissance du document électronique a engendré la reconnaissance de la signature électronique qui vient s'ajouter aux autres types de signature, à savoir la signature physique ou manuscrite, la signature biophysique (telle que l'ADN, ou les empreintes digitales, ou identification rétinienne), et la signature numérique[67]. Pour s'assurer de la vigueur d'une signature électronique, de même que pour les signatures manuscrites, six attributs sont à analyser : la permanence, la liaison, la stabilité, l'identification, la non-répudiation et l'intention.

89. Au Liban, très récemment[68] une loi libanaise sur les transactions électroniques a vu le jour. Désormais, l'écrit électronique et la preuve électronique sont admis légalement et par suite judiciairement. Avant cette loi, le droit libanais ne reconnaissait pas la validité des transactions électronique et en matière de preuve, le document électronique ne valait qu'un commencement de preuve par écrit.

90. Nous allons exposer les différentes étapes de la reconnaissance de la signature électronique (paragraphe 1) pour démontrer ensuite sa fiabilité (paragraphe 2).

---

[66] Un document électronique revêt la même force probante qu'un acte sous seing privée à la double condition que soit identifiée la personne dont il émane et qu'il soit établit et conservé dans des conditions de nature à en garantir l'intégrité (art. 1366 du Code civil). Ces critères avaient déjà été dégagés par la jurisprudence dans des termes pratiquement similaires par la Chambre commerciale de la Cour de cassation dans un arrêt rendu le 2 décembre 1997 qui déclare qu'un écrit peut être établi et conservé sur tout support, y compris par télécopies, «*dès lors que* son *intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées*».

[67] La signature numérique est un type de signature électronique dans laquelle le lien entre le signataire et l'information signée a été renforcé grâce à la cryptographie, ce qui lui donne plus de fiabilité.

[68] En date du 27 septembre 2018, le parlement libanais a voté en commission mixte une loi sur les transactions électroniques. Cette loi a été publiée dans le journal officiel no. 45 du 18 octobre 2018.

Paragraphe 1 : Reconnaissance juridique de la signature électronique

91. En droit international, la loi type de la CNUDCI[69] sur les signatures électroniques définit d'une manière fonctionnelle la signature électronique comme étant « *des données sous forme électronique contenues dans un message de données ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et «indiquer qu'il approuve l'information qui y est contenue*» » (art. 2a). Le champ d'application de cette loi-type est vaste puisqu'elle s'applique, selon son article premier, aux signatures électroniques utilisées dans le contexte d'activités commerciales. D'où son application aux activités bancaires qui sont inclues, de par la loi, parmi les actes commerciaux (art. 6 C.Com Lib. et L110-1 C.Com fr.).

92. En droit européen, la directive 2014 qui a remplacé la directive 1999[70] sur la signature électronique reconnait la signature électronique comme l'équivalent, sous certaines conditions, de la signature manuscrite. Cette directive définit la signature électronique comme étant une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification[71].

93. En droit français, la première définition légale de la signature électronique a été donnée à l'article 1367 du code civil « *la signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ».

[69] Commission des Nations Unies pour le Droit Commercial International : www.uncitral.org.

[70] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques. Elle a été complétée par les décrets n° 2001-272 du 30 mars 2001 et n° 2002-535 du 18 avril 2002 ainsi que l'arrêté du 31 mai 2002. Ce dernier arrêté a d'ailleurs été abrogé par un arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

[71]Cette directive a en outre envisagé une signature électronique dite « avancée » qui doit satisfaire à certaines exigences telles que être liée uniquement au signataire ; permettre l'identification du signataire ; et elle doit être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et elle doit enfin être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. Elle est plus sécurisée et dispose de systèmes de vérification d'identité plus poussés que la signature simple.

94. D'ailleurs la jurisprudence française[72] accorde une force probante aux signatures électroniques en affirmant que conformément à l'article 1367 du code civil, il existe une présomption d'identité entre le signataire de l'acte et l'auteur désigné du même acte ; qu'il relève que la signature portée au pied de la déclaration de créance s'apparente, dans sa typographie, à une écriture des lettres constituant le nom de Mme Y.

95. Au Liban, la signature électronique n'a pas été adoptée par une législation[73]. La décision no 7548 de la BDL règlementant l'activité bancaire électronique est le seul texte libanais qui reconnait la signature électronique sous les conditions suivantes cumulativement réunies. Le client doit avoir donné son accord explicitement. Il faut un code personnel d'identification du signataire[74]. Et pour entraver tout abus, la BDL a limité l'emploi de la signature électronique en prévoyant un plafond quant aux montants[75].

96. Cette décision de la BDL a le mérite de permettre au secteur bancaire libanais de se lancer sur internet et d'accorder aux banques nationales l'opportunité de proposer des produits et services en ligne tout en protégeant leurs intérêts ainsi que ceux de leurs clients.

---

[72] Cass. Com., 20 septembre 2017, pourvoi n°16-14341 :
https://juricaf.org/arret/FRANCE-COURDECASSATION-20170920-1614341.

[73] Le gouvernement libanais a soumis le 3 aout 2000 au parlement un projet de loi relatif à la signature électronique visant à modifier certaines dispositions du code de procédure civile et élargir leur champ d'application afin de couvrir et reconnaitre les actes et signatures électroniques. Ce projet de loi fut suivi par deux autres propositions de lois relatives à l'écrit électronique et la signature électronique (projet soumis en 2001 par le Député Ghinwa Jalloul et l'autre par le Député Yassine Jaber). Mais jusqu'à nos jours, ces projets sont dans les tiroirs du parlement et n'ont point intéressé le législateur libanais.

[74] La BDL a imposé une confirmation envoyée par courrier électronique par l'institution effectuant l'opération, dans un délai de 24 heures à compter de la date de l'opération, suivie d'une autre confirmation envoyée par courrier ordinaire dans un délai d'une semaine, sauf si la partie concernée demande à l'institution de conserver le courrier chez elle. Enfin, la banque est tenue d'envoyer au client un relevé mensuel détaillé à une adresse préalablement indiquée par ce dernier. En pratique, les banques libanaises incluent, dans leur convention avec leur client au sujet des transactions bancaires, des modalités d'identification. Il s'agit de la composition d'un mot de passe et d'une double clé. Le mot de passe est accordé par la banque au client sous pli fermé. Confidentiel, il ne circule sur le réseau d'internet que sous forme cryptée. Le client est tenu responsable de sa conservation et de son utilisation.

[75] « *La limite des crédits accordés par voie électronique à une même personne physique ou morale par une seule institution ne doit pas dépasser 20% des fonds propres de cette institution. Toutefois, les banques demeurent régies à ce sujet par les textes réglementaires de la Banque du Liban relatifs aux limites de crédit*» (art 8-4).

Paragraphe 2 : Fiabilité du procédé de signature électronique

97. Aux termes de l'article 1367[76] du code civil français la fiabilité de la signature électronique « est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décrets pris en Conseil d'Etat».

98. La législation sur la signature électronique constitue une certaine garantie aux actes électroniques[77]. La Cour de cassation a décidé récemment qu'entre deux parties qui le conviennent, les termes de l'article 1103 du Code civil, qui ne sont pas d'ordre public, peuvent être écartés. Par conséquent, s'engager par une signature manuscrite n'est pas obligatoire, les parties peuvent convenir préalablement d'autres modes (cas du code confidentiel)[78].

99. Différentes méthodes d'authentification pour les signatures électroniques ont été progressivement mises en place visant à conférer des niveaux de sécurité différents correspondant à des exigences techniques distinctes. Ces méthodes peuvent être classées en trois catégories : celles qui sont fondées sur la connaissance de l'utilisateur (mot de passe, numéro d'identification personnel etc.), celles qui sont fondées sur les caractéristiques physiques de l'utilisateur (comme la reconnaissance biométrique[79]) et celles enfin qui sont fondées sur la possession d'un objet par l'utilisateur (carte, clé USB, *token*[80], etc.).

---

[76] Tel que modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 3.

[77] Herve Causse, droit bancaire et financier, éd. Mare & Martin, 2015, no. 1134

[78] Le paiement réalisé par carte et par code a donc toujours été efficace du fait de la convention d'émission de carte (tenant compte de celle du banquier avec les commerçants) l'opération est prouvée par la composition du code. Cet ordre dématérialisé vaut un écrit, le bénéficiaire en donne acte par un ticket.

[79] Seul un procédé biométrique permet d'être vraiment certain que c'est la personne qui signe électroniquement qui est derrière son écran d'ordinateur. Mais aucun moyen technique ne permettra d'établir qu'au moment de la signature, le contrat n'a pas été vicié : par exemple par la violence (contrainte physique ou morale).

[80] L'utilisation d'un navigateur Internet portable sécurisé lancé depuis un *token* USB émis par la banque après l'insertion du dispositif et la saisie du mot de passe par l'internaute. Après la réussite de la connexion, l'utilisateur est acheminé directement vers le site de la banque émettrice. L'utilisation d'un navigateur adéquat et non infecté permet de garantir l'absence de logiciel malveillant dans ce dernier.

100. Ces catégories, qui peuvent se cumuler, reposent sur le triptyque classique de la sécurité : ce que je connais, ce que je suis et ce que je possède[81].

101. Pour accorder un effet juridique à la signature électronique, le Parlement Européen a édicté un régime de responsabilité. Le prestataire est notamment responsable du préjudice causé à toute entité ou personne qui se fie raisonnablement à ce certificat en ce qui concerne l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré ; et que le signataire identifié dans le certificat est la personne à laquelle il a été délivré (art. 6 de la directive).

102. Le prestataire de service de certification peut imposer une valeur limite des transactions pour lesquelles le certificat peut être utilisé. Le prestataire ne peut être tenu responsable du préjudice résultant d'un abus dans l'utilisation d'un certificat qui dépasse les limites fixées à son utilisation.

103. L'utilisation de l'authentification avec l'utilisation d'un lecteur CAP[82] implique la création d'un certificat à usage unique. Cette technique est assimilée à une signature électronique qui « consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache » (art. 1367 du CCiv.).

104. Afin d'assurer une meilleure garantie en matière d'authentification des personnes signataires, le recours à des tierces personnes telles que les prestataires de service de certification électronique (PSCE) est préconisé. Ces tiers de confiance délivrent des certificats[83] électroniques permettant de vérifier la signature en se basant sur trois modes du plus fort au plus faible : enregistrement en face à face, enregistrement sur la base de

[81] CAPRIOLI (E), «De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ?», disponible sur :
https://www.uncitral.org/pdf/english/colloquia/EC/ Caprioli _Article.pdf.

[82] Appareil lecteur de carte à puce autonome fourni par la Caisse d'Epargne à l'Utilisateur du service SOL par lecteur CAP. Le lecteur CAP est destiné à être utilisé avec une carte bancaire ou une carte Secur@ccès afin de fournir un code de contrôle.

[83] Fichier électronique attestant du lien entre les données de vérification de Signature électronique et l'Utilisateur signataire. Ce Certificat est à usage unique et généré à la volée lors de l'utilisation d'une Signature électronique.

documents justificatifs envoyés par la poste ou par électronique et avec une simple adresse électronique[84]. Le procédé d'identification de la signature électronique doit être fiable, comme le rappelle la jurisprudence[85].

105. Au Liban, le tiers de confiance est le Conseil Libanais d'Accréditation (COLIBAC), sous tutelle du ministère de l'industrie a été créé par la loi libanaise no. 572 du 13 février 2004. Sa mission consiste à accréditer les organismes qui octroient des certificats et des labels de conformité. La désignation de l'organisme d'accréditation affectée aux signatures et écrits électroniques rentre dans le cadre des responsabilités qui lui ont été confiées. Toutefois, cet organisme n'a pas été opérationnel (art. 14 et 15 Ecomleb[86] 2005).

[84] Eric A. CAPRIOLI, « De l'authentification à la signature électronique » : op.cit.

[85] En ce sens, à propos d'une signature scannée (non admise) dans le cadre d'une procédure d'appel : CA Besançon, 20 octobre 2000, JCP éd. G. 2001, II, 10606, p. 1890 et s. note Eric A. Caprioli et Pascal Agosti ; confirmé par la Cour de cassation le 30 avril 2003, Bull. civ. 2003, n°118, p. 101 et s. (disponible sur le site www.legifrance.gouv.fr).

[86] Ecomleb est un avant-projet sur la communication, l'écriture et les transactions électronique (ECOMLEB), mai 2005. Ce projet bénéficiant de l'abrogation des dispositions du Titre IV du Livre 1er du code de commerce libanais pour les remplacer par un nouveau Titre IV intitulé « Du commerce électronique » qui comportera 8 articles numérotés de 40 à 41-3. Le projet Ecomleb a été financé par l'UE (environ 1,7 millions d'Euros) avec deux objectifs principaux le développement d'un cadre juridique complet du commerce électronique et la sensibilisation du public.

Section 2 : L'authentification par tierce personne

106. Le règlement communautaire du 10 mars 2004[87] définit l'authentification comme étant « *la confirmation de l'identité prétendue d'entités ou d'utilisateurs* » (art 4-e). Cette définition est extensive puisqu'elle englobe à la fois les personnes physiques et les personnes morales.

107. En France, la jurisprudence a classé l'authentification comme une véritable mesure de sécurité pour la gestion des accès à l'instar du contenu de la norme ISO 27001[88]. Dans un arrêt rendu par la Cour d'appel de Versailles[89], la responsabilité de la banque a été engagée sur le fondement de son manquement à l'obligation de sécurité.

108. Aux Etats-Unis, les juges [90] ont accentué l'importance de l'authentification au moment de l'accès au compte bancaire via internet, en décidant que la banque en ligne est tenue de satisfaire aux normes techniques et sécuritaires proportionnées aux risques liés à ses services et produits. Les juges ont fourni une liste de méthodes permettant de procéder à l'authentification des clients notamment l'utilisation des mots de passe, numéros personnels d'identification (NIP), certificats électroniques, ustensiles physiques tels que les cartes ou clé USB, *tokens*, mot de passe unique[91] (OTP), procédés biométriques, etc[92].

---

[87] Règlement Communautaire no. 460/2004 du 10 mars 2004 JOCE L 077, 13 mars 2004. Ce règlement a institué l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).

[88] ISO/IEC 27001: 2005 (para 16) (Code of practice for Information Security Management- Requirement) : The ISO/IEC 27000 series is a comprehensive set of controls comprising best practices in information security. It is an internationally recognized information security standard, broad in scope and generic in applicability. It focuses on risk identification, assessment and management.
It is aligned with common business goals: https://www.bankinfosecurity.com/iso-17799-27001-setting-standards-for-information-security-a-165.

[89] C. App Versailles 18 nov. 2010 Marie –Maure C. épouse A. c/SA Natixis Interépargne. Décision no. 09/06634.

[90] Case no. 07 C 5387 – 21 Aout 2009 - Tribunal Illinois : affaire Shames Yeakel vs. Citizen Financial Bank – Commentaire M. Eric Caprioli « Première décision américaine concernant l'authentification par voie électronique d'un client bancaire (Lexis Nexis no. 4, Avril 2010, comm. 41.

[91] One time password *:* la technique du mot de passe à usage unique présente un avantage. Le vol de l'identifiant ne fournit au pirate qu'un seul et unique accès. Les dégâts sont limités mais ce n'est pas une garantie totale.

109. Nous allons présenter le certificat électronique, le moyen le plus utilisé en matière de transaction bancaire pour authentifier la transaction (Paragraphe 1) pour expliquer le rôle significatif de l'hébergeur en matière de preuve de l'identité du client (Paragraphe 2).

Paragraphe 1 : Le certificat électronique, garantie de l'authentification de la transaction bancaire en ligne

110. Afin d'assurer une sécurisation des transactions bancaires en ligne, un certificat électronique[93] a été mis en place. Il s'agit d'une sorte de carte d'identité électronique générée par une autorité de certification objective et autonome (tiers de confiance), qui permet à la fois d'attester le lien entre l'identité physique et l'identité virtuelle, en assurant l'authentification de la personne signataire qui se réalise grâce à la clé secrète détenue par cette dernière, et la vérification de l'authentification qui se fait à l'aide de la clé publique figurant dans le certificat. Ce dernier constitue un registre informatique comportant tous les identifiants de la partie demandant la certification et l'autre partie ratifiant et accordant la certification avec la date de cette certification.

A- Le mécanisme du certificat électronique

111. Ce mécanisme inclut un élément connu du seul utilisateur comme son mot de passe et d'un élément, difficile à copier, auquel seul l'utilisateur a accès comme le jeton ou carte à puce physique et donc ils sont moins vulnérables aux ingénieries cybercriminelles.

[92] L'authentification permet de prévenir des attaques frauduleuses. Elle peut être multifactorielle et consister en une combinaison de deux canaux différents l'un en ligne, l'autre hors ligne (via le téléphone ou OTP généré de façon aléatoire). Cette méthode est jugée non rejouable et plus sécurisée que l'authentification à un seul facteur (fournir une information connue du destinataire).

[93] Le certificat électronique est un petit fichier divisé en deux parties, une contenant les informations et l'autre contenant la signature de l'autorité de certification. C'est une clé publique qui contient notamment le nom et le prénom de la personne titulaire du certificat, la dénomination sociale de l'entreprise et la clé qui permet d'authentifier la signature du titulaire du certificat.

112. Le certificat électronique se présente soit sous forme de matériel (carte à puce[94] ou une clé USB[95]) soit sous forme de logiciel à télécharger directement sur le poste de travail de l'ordinateur.

113. Le certificat électronique peut être adossé à une signature électronique. Dans ce cas, il est stocké dans des serveurs de clé (autorité d'enregistrement), qui contrôlent les certificats et répertorient des certificats radiés[96]. Le certificat électronique joue un rôle particulier dans le chiffrement et la sécurisation des données financières qui circulent en ligne au point que plusieurs banques françaises délivrent elles-mêmes des certificats électroniques.

114. Le tiers certificateur assiste à la création de preuve de ces transactions, il s'agit de preuve par témoins. Notons d'ailleurs que cette tierce personne ne doit pas s'ingérer dans le contenu de la transaction.

115. Cette technique ressemble à l'émission des extraits des états civils ou des cartes des professions libérales émises par les ordres et syndicats compétents qui certifient que le porteur de cette carte est membre de leur organisme.

116. En droit libanais et droit français, le procédé d'authentification implique la présence d'une autorité publique (ou une autorité déléguée) qui serait en qualité de vérifier et certifier (notaire, huissier de justice) le document et en faire de lui un *instrumentum* original et fiable sans altération or modification depuis son authentification.

[94] Dans ce cas de figure, le certificat électronique s'appuie sur l'utilisation d'un lecteur et d'une carte à puce dans laquelle sont logés le certificat et les éléments confidentiels liés à son utilisation, non accessibles à des tiers.

[95] Le mécanisme du certificat électronique ainsi que les données confidentielles sont logés dans une clé cryptographique USB qui lui envoyée par courrier recommandé avec accusé de réception soit remise en main.

[96]Parmi les opérateurs de service de certification électronique les plus connus figurent CertEurope qui est un prestataire de service de certification qualifié conformément à l'arrêté du 26 juillet 2004 et à la spécification européenne ETSI/ITS 101456.

117. La question qui se pose est de savoir qui est l'entité éligible pour certifier ? Est-ce une entité publique ou privée ? Une banque ou une compagnie d'assurance ? En fait, cette mission de certifier les transactions en ligne est certes une nouvelle profession, elle implique comme l'avait bien décrit M. BENSOUSSAN [97] une profession de notaire virtuelle qui garantit la bonne conclusion des transactions par les parties concernées et en crée une preuve. Cette nouvelle profession de notariat requiert un encadrement légal définissant les critères du tiers certificateur, ses missions et sa responsabilité.

118. Nous pensons que l'activation du COLIBAC pourrait être d'un grand intérêt et un vrai support à la sécurisation des transactions bancaires en ligne au Liban. A défaut de son activation, et pour combler ce vide nous suggérons qu'un organisme ad hoc soit créé à l'instar de LIBNOR et d'autres organismes d'accréditations qui ont connu un grand succès dans les secteurs éducatifs et hospitaliers.

B- Usurpation de l'identité électronique

119. Il existe plusieurs techniques d'usurpation d'identité. A titre d'exemple, installer un enregistreur de frappe sur l'ordinateur de sa victime, la mettre sur écoute téléphonique ou encore utiliser la technique de l'hameçonnage ou le *phishing*[98] ou encore la technique utilisant un moyen de piratage appelé « Man-in-the-Middle » ou attaque de l'homme du milieu pour recueillir les informations confidentielles données par l'internaute sur le site

[97] Bensoussan (A), un nouveau métier, le tiers certificateur, se profile sur internet, OnLine Journal, 15 décembre 1995.

[98] Les fraudeurs récupèrent les données personnelles de l'utilisateur de la carte, principalement par le biais de courriels non sollicités renvoyant l'utilisateur vers des sites frauduleux ayant l'apparence de sites de confiance : https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/fraude-a-carte-paiement

Selon l'étude Gartner, les attaques par hameçonnage continuent de peser financièrement sur les consommateurs et les institutions financières, la tendance étant vers une augmentation du volume et une baisse des montants. L'étude a montré que plus de cinq millions de consommateurs américains avaient subi un préjudice financier suite à des attaques d'hameçonnage entre septembre 2007 et septembre 2008, soit une progression de 39,8 % du nombre de victimes en un an. 6 Gartner, Inc. "Banks Need to Strengthen User Authentication While Appeasing Consumers." Mai 2010. ID G00158229.

visité. Afin de maintenir la confusion, il arrive que l'utilisateur soit ensuite redirigé vers la vraie adresse du site web, sur lequel l'authentification lui est à nouveau demandée[99].

120. L'élément moral[100] du délit est simple à caractériser. En effet, le seul fait d'usurper l'identité d'autrui et lui porter atteinte, manifeste l'intention de nuire de l'usurpateur.

121. L'usurpation de l'identité électronique est désormais sanctionnée. La Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (LOPPSI II)[101] adoptée par l'Assemblée nationale française le 16 février 2010a élargi l'usurpation d'identité [102] au domaine électronique, et la sanctionne des mêmes sanctions qu'une usurpation d'identité hors ligne (art. 226-4 -1C. Pénal fr.) [103].

---

[99] Cette technique ne peut réussir que si le pirate peut imiter chaque point d'extrémité tout en garantissant la satisfaction de l'autre. Le recours à une authentification SSL utilisant une autorité de certification fiable apporte une protection forte contre les menaces MitM. Lorsque la validation du certificat repose sur l'utilisateur, il est possible que celui-ci ne valide pas correctement les certificats du serveur et qu'il déclique les messages d'avertissement. Dès lors, en cas d'utilisation d'une solution d'authentification à base de certificats, la responsabilité incombe habituellement à la banque, qui doit vérifier si le certificat de l'utilisateur est valide et ne pas autoriser l'ouverture d'une session si le certificat ne correspond pas à celui qui se trouve dans son système informatique.

[100] Si l'atteinte à l'honneur et à la considération sont particulièrement plus simples à déceler, le trouble à la tranquillité est plutôt difficile à mettre en pratique. Il pourrait en être ainsi *« si le désagrément s'accompagne d'une pénétration, effective et délibérée, dans la sphère personnelle de la victime. Concrètement, cela pourrait être retenu si l'usurpateur interfère dans les relations personnelles que la victime entretient avec le ou les tiers abusés, ou encore s'il provoque des sollicitations injustifiées de la part d'inconnus, directement sur la messagerie électronique ou le téléphone[100]».* Et si l'intention de nuire n'est pas caractérisée ? C'est courant dans les réseaux sociaux qu'une personne utilise une photographie d'une autre (ou d'une star pour rendre son profil attractif), elle usurpe de ce fait son identité mais ne lui porte nullement atteinte. Normalement, le seul fait d'usurper l'identité d'autrui abstraction faite de l'intention de nuire doit être retenu pour qualifier le délit d'usurpation d'identité.

[101] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite loi LOPPSI II, JORF n°0062 du 15 mars 2011 p 4582.

[102] Verbiest Th., Cuignet P, « La création d'un délit d'usurpation d'identité numérique », disponible sur : http://www.droittechnologie.org/actuality-1316/la-creation-d-un-delit-d-usurpation-d-identite-numerique.html

[103] L'article dispose que « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération , est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur réseau de communication au public en ligne* ».

122. Au Liban, le code pénal libanais sanctionne l'usurpation d'identité (article 405 et 406). Cependant, ces dispositions ne peuvent être interprétées extensivement pour inclure l'usurpation identitaire en ligne. D'où une telle reconnaissance et sanction de cette criminalité identitaire en ligne est vivement préconisée pour ne pas laisser ces usurpateurs impunis.

Paragraphe 2 : La preuve au niveau des intermédiaires techniques

123. Pratiquement, l'internaute qui veut créer ses pages web ou encore la banque qui souhaite opérer en ligne doit en général s'adresser à un professionnel pour héberger ses pages sur les serveurs.

124. L'hébergeur met à la disposition de son abonné, à titre gratuit ou onéreux, un espace mémoire sur un serveur informatique pour stocker[104] des informations, de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par l'abonné et les rend accessibles au public sur le réseau ou héberger divers serveurs logiciels (serveur web et serveur e-mail) (article 6-I-2 de la LCEN).

125. Mais le rôle primordial de l'hébergeur réside dans sa capacité de déterminer l'auteur véritable des communications et créateur du contenu en ligne En effet, le Conseil d'Etat français déclare que « *les données conservées associées à l'adresse IP par le fournisseur d'accès permettent la traçabilité de l'activité d'un internaute (les sites visités, la date et l'heure, les documents téléchargés, la participation à un espace de discussion, les messages électroniques expédiés et reçus) aussi longtemps que ces données sont conservées* ».

[104] Les parties au contrat d'hébergement doivent s'accorder précisément sur le volume de l'espace de stockage et capacité mémoire offerte dans le cadre de l'hébergement ainsi que sur la disponibilité de cet espace.

126. Il est, de ce fait, tenu d'une obligation de conservation de certaines données (art. 6 II 1 de la LCEN[105] et art. 14 EComleb). La durée et les modalités de conservation de ces données sont établies par le décret en Conseil d'État pris après avis de la CNIL. Le Conseil d'Etat français a considéré que ces données conservées ne doivent pas être détruites trop vite « *afin de faciliter les poursuites et l'établissement de la preuve des infractions* ». Constatant que le délai de prescription légale des délits est de trois ans, que la durée de conservation des données relatives aux appels téléphoniques par France Télécom est de un an et que la CNIL recommandait alors un délai de conservation maximal d'un an, le Conseil d'Etat proposait, sous réserve d'expertise, d'adopter une durée de conservation d'un an. La LCEN apporte toutefois une modification importante puisque ces données ne pourront plus être communiquées qu'à un juge (disposition similaire envisagée dans l'article 17 Ecomleb).

127. L'hébergeur peut être contraint à communiquer des éléments d'identification[106], des informations confidentielles relatives à l'auteur des actes suspicieux ou illicites (tels que le nom d'un internaute ayant commis une infraction). Cette obligation est très délicate du fait qu'elle a trait à la vie privée de la personne et ses données personnelles. D'où l'exigence d'une autorisation du juge des référés. Faute de quoi, l'hébergeur qui communique spontanément et sans autorisation judiciaire les éléments commet une faute.

128. Selon Ecomleb, les données conservées par les prestataires techniques sont soumises au secret professionnel, toutefois ce secret n'est opposable à l'autorité judiciaire (art. 11 Ecomleb).

129. Le non-respect de cette obligation a été sanctionné par la jurisprudence sur le fondement de l'article 1242 du Code civil[107].

---

[105] Cet article dispose que les hébergeurs « *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires* ».

[106] TGI Paris 27 février 2006.

[107] C. App de Paris, 10 février 1999, Estelle Hallyday c/ Valentin Lacambre : Gaz. Pal., 5-6 avril 2000, jur. P. 19 note Ch. Caron : l'anonymat engageant la responsabilité de l'hébergeur.

130. Nous concluons que la capacité légale du client internaute à la transaction bancaire en ligne et son identification par la banque constitue un volet de la sécurisation des transactions bancaire en ligne. A ce volet s'ajoute un autre relatif aux procédés d'authentification de la transaction bancaire en ligne. Cette authentification se fait par le biais de la signature électronique soit par une tierce personne certificatrice.

Titre 2 : Sécurisation du consentement du client internaute et de ses données personnelles

131. La protection du client internaute, comme tout consommateur, est l'enjeu majeur du législateur.

132. Avant d'énumérer les obligations incombant à chaque partie à la transaction bancaire en ligne, il est intéressant de rappeler qu'il leur incombe, avant tout, de contracter de bonne foi [108] . En outre, ils ont l'obligation de respecter minutieusement leurs obligations respectives selon les principes fondamentaux « *pacta sunt servanda* » et ceux qui gouvernent la *lex mercatoria*[109].

133. Au Liban, la Banque du Liban oblige les banques, opérant par voie électronique, à se conformer sans restriction ni réserve aux principes d'honnêteté, d'intégrité, et de transparence (art. 2 Décision 7548[110] et art. 2 de la Décision no.7493). Ces conditions relatives aux obligations sont essentielles pour mettre en place une relation contractuelle valide et fiable.

134. En droit français, et sous le titre de « Règles de bonne conduite », l'article L. 533-11 du Code monétaire et financier invoque les principes de loyauté, d'honnêteté et professionnalisme et impose aux prestataires de servir au mieux les intérêts des clients.

[108] Le Code Civil français indique que les contrats doivent être exécutés de bonne foi (art. 1134 al. 3 devenu 1104). Le COC dispose que les conventions « *doivent être comprises, interprétées et exécutées conformément à la bonne foi, à l'équité et aux usages* » (art.221). Les principes UNIDROIT indiquent que « les parties sont tenues de se conformer aux exigences de la bonne foi dans le commerce international. Elles ne peuvent exclure cette obligation ni en limiter la portée » (article 1.7).

[109] La *lex mercatoria* désigne les principes usages et pratiques des « marchands » dans le commerce international. Il s'agit des usages et coutumes des marchés. : www.lexinter.net/JF/lex_mercatoria.htm.

[110] BDL, Décision de base sur les opérations financières et bancaires par voie électronique, 3 mars 2000.

135. S'y ajoute une série d'obligations[111] à savoir l'obligation de classer la clientèle (professionnels et non professionnels); l'obligation d'information (permettant au client de comprendre la nature du produit ou service et les risques liés); et l'obligation de proposer aux clients des produits adaptés (après vérification de leur niveau d'expérience et de connaissance pour comprendre et mesurer les risques).

136. Dans un premier temps, nous allons constater qu'informer le client internaute constitue un des piliers de protection du consentement (Chapitre 1), tandis que dans un second temps nous allons traiter de la protection des données personnelles (Chapitre 2).

[111] Insérée dans le Code monétaire et financier français par l'ordonnance n° 2007-544 du 12 avril 2007.

Chapitre 1 : Informer, un pilier de protection du consentement

137. L'obligation d'information[112] c'est le devoir de communiquer au client, d'une manière objective, des données ou faits connus du professionnel, prestataire de services. Consacrée par la jurisprudence, cette obligation a été réaffirmée par les textes législatifs[113] et les autorités de tutelle pour la fourniture de produits et services financiers, en général, et renforcée pour les produits et services financiers délivrés par internet, en particulier.

138. Cette obligation d'information est primordiale parce qu'elle a un impact sur le consentement du client surtout dans un secteur délicat comme celui du secteur bancaire. Ainsi, selon les principes généraux du droit des contrats, pour être valable, le consentement ne doit pas être donné par erreur ou détourné par violence ou dol (art. 1130 Code civil, art.177 COC). En effet, le client doit être assuré que ses transactions et ses intérêts sont protégés s'il recourt à des prestations bancaires en ligne. Ceci passe par une compréhension suffisante des prestations bancaires en ligne par le client.

139. D'ailleurs nous considérons que cette obligation d'information ne devrait pas constituer un fardeau pour la banque. Au contraire, elle contribue au développement de la relation de confiance entre la banque et le client.

140. Quelles sont les informations nécessaires au client contractant une transaction bancaire en ligne ? En outre, à qui incombe la charge de la preuve de l'accomplissement de cette obligation d'information ? Nous allons formuler dans ce qui suit le contenu de l'information (Section 1) avant d'aborder la preuve de cette information (Section 2).

[112] Cette obligation n'est pas nouvelle, les législations protectrices du consommateur revendiquent à plusieurs niveaux l'information du consommateur.

[113] Art. L.111-1 du Code de la consommation français et art. 4 du Code de la consommation libanais et art. L. 312-1-1 et L. 314-12 du Code monétaire et financier et l'ordonnance n° 2009-866 du 15 juillet 2009.

Section 1 : Les modalités de l'information

141. L'obligation d'informer est la conséquence naturelle du fait que la banque est la partie la plus expérimentée dans le domaine financier et l'auteur principal et actif du contenu de la transaction. Nous considérons que l'obligation d'information est un accessoire et un moyen introductif du service financier rendu par la banque.

142. Nous allons déterminer dans un premier temps le contenu de l'information (Paragraphe 1), pour exposer ensuite les procédés et moyens de l'information (Paragraphe 2) et pour contrer enfin le démarchage ou publicité en ligne en vue de sécuriser le client internaute (Paragraphe 3).

Paragraphe 1 : Le contenu de l'information

143. L'information porte, d'une part, sur le prestataire (identité, adresse, courrier électronique, numéro de registre du commerce, numéro d'immatriculation auprès de l'autorité de surveillance, numéro de TVA, identité du représentant du prestataire et d'autre part sur le produit ou le service (caractéristiques du produit ou service, prix, taxes et autres frais, modalité de paiement ou d'exécution, risques, existence d'un droit de rétractation, durée, possibilité et moyens de corriger les erreurs).

144. Sur la même lignée, la Banque du Liban[114] soumet la banque, à «une obligation totale de transparence » dans ses relations avec ses clients. Par conséquent, la banque est tenue de « présenter de manière claire et précise » les indices et produits dérivés, les bénéfices et leur modalité de calcul, tous les risques dont le client peut souffrir, et toutes autres informations de nature à procurer au client une meilleure clarté et précision. Elle doit mettre à la disposition de ses clients une brochure relative aux différents services et une formule de contrat préalablement agréés par la Banque du Liban qui fixe à son tour le minimum d'informations à transmettre par les banques.

[114] L'article 2 de l'Arrêté de la BDL no 7493 et Arrêté du 24 déc. 1999 relatif aux indices et produits financiers dérivés et programmes de dépôt et autres produits financier, les règlements bancaires presses BDL p.372. 1.

145. L'article 1127-1 Code civil français exige que toute offre de contrat sous forme électronique proposée par un professionnel comprenne cinq éléments limitativement énumérés à savoir: les différentes étapes à suivre pour conclure le contrat, les moyens techniques permettant à l'utilisateur, avant la conclusion du contrat, d'identifier les erreurs commises dans la saisie des données et de les corriger, la langue proposée pour la conclusion du contrat, en cas d'archivage du contrat les modalités de cet archivage et les conditions d'accès au contrat archivé, les moyens de consulter par voie électronique les règles professionnelles et commerciales applicables à la transaction.

146. En outre, d'autres types d'information peuvent être mis à la charge de la banque. Par exemple, les juges libanais[115] ont conclu que la banque qui n'arrive pas à encaisser le chèque déposé par son client est tenue de l'en informer dans les plus brefs délais, et que cette obligation d'information est fondamentale sous peine d'engager la responsabilité du banquier pour manquement à ses obligations d'information et de célérité.

147. Notons qu'une nouvelle obligation est venue s'adjoindre à l'obligation d'information, à savoir l'obligation d'explication[116]. Cependant, il ne faut pas confondre «information » et «conseil»[117]. Le conseil sert à orienter[118] alors que l'information est destinée à éclairer. Par conséquent, le devoir de conseil[119] incite le client à opérer un choix sur des opportunités disponibles alors que l'obligation d'information repose sur des critères objectifs et précis.

148. L'obligation de conseiller et de renseigner le client internaute non professionnel fait partie du devoir d'information de la banque, qui doit lui fournir une information et des explications d'autant plus détaillée et complète lorsque ce client se révélera être peu compétent. Les banques françaises confirment qu'information et conseil répondent à des logiques très différentes, non seulement en termes commerciaux mais aussi juridiques.[120]

---

[115]TPI de Beyrouth, 13 juil. 1998: RJL 1998, p.936.

[116] Elle a été instaurée par la loi 2010-717 du 1er juillet 2010 qui a transposé la Directive 2008/48/CE du 23 avril 2008 relative aux contrats de crédit aux consommateurs et par conséquent a abrogé la Directive 87/102/CEE du Conseil, JOCE L133, 22 mai p.66-92

[117] Cass. Civ. 1ere, 20 dec. 2012, no. 11-28202.

[118] Lamy Droit du financement, 2011, no. 3317.s

[119]Leclerc P, L'obligation de conseil du banquier dispensateur de crédit, RJDA 1995, p.322.

[120] Livre Vert sur les services financiers de détail dans l'union, 2007.

149. L'information, selon M. DANJAUME[121], doit être considérée comme une chose inerte. Il ne peut donc y avoir de responsabilité du fait de la chose « information » que s'il y a contact entre la chose et la personne, et ce dernier est établi entre l'information fournie par la banque de donnée et le client via l'écran.

150. Enfin, nous invoquons un nouvel élément qui aide à instaurer la transparence et à éclairer le consommateur : c'est la technique de comparaison entre les sites des banques. Les sites de comparaison[122] consolident l'information du consommateur puisqu'ils le préviennent de l'existence de plusieurs produits et services et l'aident à les évaluer, ce qui renforce sa capacité à prendre de bonnes décisions et à faire des choix plus convenables à sa situation.

Paragraphe 2 : Procédés et moyens de l'information

151. Ces informations doivent être fournies par la banque préalablement à tout engagement du client et doivent être claires, exactes et facilement compréhensibles (art. L341- 12 du code monétaire et financier[123] et art 3 de la loi libanaise de consommation). La délivrance de l'information se caractérise par sa gratuité, ce qui n'exclut pas de fournir un service d'information optionnel et complémentaire rémunéré.

152. La banque informe le consommateur par écrit ou « *par lettre nominative ou courrier électronique dédiés* »[124] ou par le moyen de «*supports durables*».

---

[121] DANJAUME G, La responsabilité du fait de l'information, JCP G, 1996, I, p. 3895s.

[122]Rapport de l'AEAPP sur les bonnes pratiques en matière de sites web comparateurs (Good Practices on Comparison Websites) – janvier 2014.

[123] L'article L341- 12 du code monétaire et financier précise que « *ces informations, dont le caractère commercial doit apparaître sans équivoque, sont fournies de manière claire et compréhensible par tout moyen adapté à la technique de communication à distance utilisée* ». L'article 3 de la DCE 2002 impose d'informer le consommateur préalablement à la conclusion du contrat à distance « *en temps utile avant que le consommateur ne soit lié par un contrat à distance ou par une offre, il reçoit les informations concernant le fournisseur, le service financier, le contrat à distance, le recours* ».

[124] Article 53 de la loi libanaise no 659-du 4 février 2005 sur la protection du consommateur.
L'article 321-68 dispose que « *lorsqu'ils exercent une activité de réception et transmission d'ordres pour le compte de tiers ou d'exécution d'ordres pour le compte de tiers ou de compensation, les prestataires habilités établissent avec chacun de leurs donneurs d'ordres une convention de services écrite* » ; ces dispositions sont

153. L'article 2-f de la DSF définit le support durable comme étant « *tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permanente et de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations ont destinées et qui permet la reproduction à l'identique es informations stockées* ». Cette définition est complétée par les exemples énumérés dans le considérant 20 de la DCE incluant notamment les disquettes informatiques, les cédéroms, les DVD et le disque dur de l'ordinateur du consommateur sur lequel le courrier électronique est stocké, mais ils ne comprennent pas les sites internet, sauf ceux qui satisfont aux critères spécifiés dans la définition des supports durables.

Paragraphe 3 : Sécurisation du client quant au démarchage ou publicité en ligne

154. Le législateur français oblige les professionnels à fournir aux consommateurs une information loyale et honnête dont ceux-ci ont besoin et sanctionnent les publicités mensongères ou trompeuses, qui portent atteinte au consommateur (art. L.121-2 à 121-7 du CConsom). Le législateur français[125] a renforcé la protection du client internaute face à un démarchage ou une publicité en ligne, en considérant qu'« *est interdite la prospection*[126] *directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen*» (article 22)[127].

---

applicables en l'espèce puisqu'elles ont été reprises, en substance, par les articles 314-49 et 314-59 du Règlement Général de l'AMF.

[125] La LCEN et la loi. n° 2003-706, 1er août 2003 relative à la sécurité financière : JO n°177, 2 août 2003 p. 13220 qui a modifié les règles de publicité de crédit à la consommation afin de renforcer l'information du consommateur et qui a reformé la définition du démarchage bancaire et financier afin de mieux protéger les démarchés profanes.

[126] «*Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services*» (CP et T, art. L.34-5).

[127] Modifiant l'article L. 34-5 du Code des postes et télécommunications

155. En droit libanais, la loi de 2005 sur la protection du consommateur a consacré le quatrième chapitre à la notion de « publicité trompeuse » et la définit de manière extensive « *la publicité effectuée par tout moyen, relative à un produit ou un service contenant une offre, une annonce ou une allégation mensongère ou, rédigée en des termes, qui, directement ou indirectement trompent le consommateur ou l'induisent en erreur*» (art 11). Dans la même perspective, ECOMLEB interdit le démarchage et la promotion non sollicités envers des personnes qui n'y ont pas consenti au préalable (texte à intégrer sous l'article 41-1 du code de commerce libanais).

156. D'ailleurs le législateur a été ferme au sujet du consentement préalable du consommateur. D'où la sanction du spamming[128] ou pollupostage ou pourriels[129] qui consiste en « l'envoi massif, et parfois répété, de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles le destinateur n'a jamais eu de contact et dont il s'est procuré l'adresse électronique dans les espaces publics de l'Internet (forums de discussions, listes de diffusion, annuaires, sites web, etc.)»[130]. C'est une méthode avantageuse[131] de marketing en ligne qui permet aux entreprises d'accéder rapidement, directement et massivement aux internautes par le biais de leur boite aux lettres électroniques ou email. Elle implique la collecte des informations personnelles des personnes visées.

[128] Le mot spam est à la base une marque d'un produit alimentaire américain - boite de conserve de viande de porc SPAM, acronyme de "*Spiced Porc And Meat*".

[129] En français, le spam est indiqué par l'expression « Pourriel » qui est la combinaison québécoise entre le mot « poubelle » et le mot « courriel ».

[130] Définition de la CNIL dans son rapport sur le publipostage électronique. Il est également défini par l'article L. 341-1 du Code monétaire et financier comme étant un acte de démarchage bancaire ou financier toute prise de contact non sollicitée, par quelque moyen que ce soit, avec une personne physique ou morale déterminée, en vue d'obtenir de sa part un accord sur la réalisation par une personne habilitée à démarcher d'une opération sur instruments financiers ou d'une opération connexe ; la fourniture par une personne habilitée à démarcher d'un service d'investissement ou d'un service connexe ; la réalisation par une personne habilitée à démarcher d'une opération sur bien divers ; et la fourniture par une personne habilitée à démarcher d'une prestation de conseil en investissement.

[131]Ce marketing permet en réalité de réduire considérablement l'ensemble des frais engagés par une entreprise et permet une expansion plus large de sa campagne publicitaire.

157. S'agissant d'une fourniture de services non sollicités[132], le spamming constitue une pratique abusive et est légalement[133] prohibée. Aux Etats-Unis, certains Etats[134] prohibent et sanctionnent d'une lourde peine d'amende l'envoi de courriers électroniques à caractère commercial non sollicités par leurs destinataires.

158. D'où le législateur européen [135] a envisagé une faculté « *opt-in* » c'est-à-dire l'exigence d'un consentement préalable et exprès du destinataire et « *opt-out* » ou droit d'opposition de la part du destinataire et son droit de choisir de ne pas recevoir de mails (article 10 de la DCE 1997) et a laissé aux Etats membres la possibilité de choisir entre ces deux facultés. Certains pays tels l'Allemagne, l'Italie, la Finlande, l'Autriche et le Danemark ont consacré l'« *opt-in* » pour réglementer la pratique du spamming sur leurs territoires.

159. La France a consacré le système de l' « *opt-out* » pour la prospection commerciale par courrier électronique non sollicité (article L. 121-20-5 du Code Consomm). Parallèlement, au Liban, le système d' «*opt out*» a été adopté dans l'avant-projet ECOMLEB[136].

[132] Les professeurs Thierry BONNEAU et François DRUMMOND dans leur ouvrage sur le droit des marchés financiers relèvent que les sites ne constituent pas en eux-mêmes des actes de démarchage, qu'ils aient ou non des liens hypertextes car la nécessité de cliquer sur une icône pour aller sur le site exclut la qualification de démarchage. Selon ces professeurs le comportement actif de l'internaute qui se connecte au forum ne paraît pas conciliable avec la qualification de démarchage. Toutefois, dans la mesure où cet internaute n'a pas consenti à la réception du message, on peut considérer qu'il est démarché. Droit des marchés financiers, Thierry Bonneau et François Drummond, Ed. Economica, février 2002

[133]La loi « Informatique et liberté » du 6 janvier 1978, les directives européennes du 24 octobre 1995[133], du 20 mai 1997 et du 15 décembre 1997, et la LCEN.

[134] Washington loi du 25/03/1998 ; Californie loi du 26/09/1998 et Névada en 1999.

[135] la DCE 20 mai 1997 dite « directive vente à distance », consacre le système de « l'opt-out »

[136] Projet d'article 41-2 à intégrer dans le code de commerce qui dispose que « tout message de démarchage ou promotion non sollicité doit clairement indiquer l'adresse à laquelle le destinataire des messages pourra exiger qu'il soit mis fin à de telles communications. Il est précisé par l'article 41-3 que le contrevenant aux dispositions des deux articles précédents s'expose à des dommages-intérêts et pourra être contraint sous astreinte de s'y conformer ».

160. L’article 7 du Règlement Général des Données Personnelles de 2018 impose un consentement préalable exprès des consommateurs « opt in » pour l'utilisation d'automates d'appels ou de télécopieurs dans des opérations de prospection directe avec la faculté de retirer ce consentement discrétionnairement.

161. La pratique du spamming a été condamnée pour la première fois en France, par le TGI de Paris dans un jugement rendu le 15 janvier 2002 dans l’affaire "Yahoo" et "J'accuse" [137]. Le juge a considéré que le spamming est une pratique « déloyale et gravement perturbatrice » et contrevenant ainsi au contrat passé entre l'auteur du spam et son fournisseur d'accès à internet.

[137] En l’espèce, l’internaute spammeur avait engagé une action contre ses FAI (Free et Liberty-Surf) pour rupture unilatérale de contrat, ces derniers ayant coupé ses accès Internet devant l’importance des *spams* constatés. L’internaute a donc été condamné à payer une indemnité à ses FAI pour procédure abusive. Ce jugement applique les dispositions de plusieurs directives européennes prohibant ce type de pratique.

Section 2 : La preuve d'exécution de l'obligation d'information

162. Le client internaute a le droit de recevoir la totalité des informations dont il en a besoin. L'article L121-20-16 du code de la consommation qualifie les informations obligatoires d'ordre public. La banque doit aussi délivrer des informations complémentaires lorsqu'un incident se produit. Par conséquent, au cas d'un problème dans l'opération de paiement, la banque, prestataire de services de paiement, doit retrouver la trace de l'opération et notifier à l'utilisateur le résultat de sa recherche.

163. Nous allons aborder, dans un premier temps, l'obligation d'informer en fonction du statut du client (Paragraphe 1) et, dans un second temps, exposer les moyens de preuve de l'exécution de cette obligation (Paragraphe 2).

Paragraphe 1 : L'obligation d'informer en fonction du statut du client

164. La Décision de base de la BDL no. 11947 du 12 février 2015 règlementant les modalités des opérations bancaires et financières avec les clients impose aux banques dans son premier article de « *cultiver les clients, de les éveiller, et de clarifier leurs droits, en publiant des programmes d'éveil et de culture dans leurs siège social et leurs sites électroniques* ». cette obligation est assez floue et lourde. Nous nous demandons avec le professeur Mr. DIAB[138] si cette obligation d'établir des programmes d'éveil et de culture financière des citoyens ne doit pas peser sur les institutions publiques plutôt que de mettre ce fardeau à la charge des banques du secteur privé.

165. Les Principes directeurs de la Banque mondiale pour le traitement de l'investissement étranger incluent l'obligation de traiter sur un pied d'égalité l'ensemble des investisseurs, qualifiés, institutionnels, professionnels ou occasionnels.

[138] Diab N., Le droit de l'investisseur à l'information sur les marchés financiers, Revue Al-Adl 2015, no.3 p. 1274.

166. Par conséquent, la banque pourra difficilement, en cas de contentieux, s'exonérer de sa responsabilité quant à l'exécution de son obligation d'information en invoquant la qualité de professionnel averti du donneur d'ordre. De ce fait, l'information à délivrer est celle exigée pour les donneurs d'ordre « *sans aucune compétence professionnelle, ni expérience particulière en matière d'investissement financier* »[139].

167. Cependant, un arrêt a considéré qu'« *aujourd'hui il n'est pas besoin d'être un spécialiste en informatique pour connaitre la signification générale de certains termes techniques* »[140]. Ceci semble logique mais sans pour autant résulter en une exemption de la banque de donner des informations appropriées aux clients quelques soient leurs compétence. Après tout, se fier aux apparences ou aux constations personnelles restent subjectif.

168. Au Liban, la faute du banquier est appréciée en fonction du degré d'expérience du demandeur de renseignement « *ou de la formulation plus ou moins encourageante ou assurée du renseignement fourni. En effet, si le renseignement concernant la solvabilité d'un client est donné sans aucune réserve, le demandeur sera largement incité et encouragé à contracter avec celui qui jouit d'un tel crédit ; au cas où ce renseignement s'avère erroné, le banquier sera largement responsable. Il en ira autrement si la banque avait formulée des réserves en incitant le demandeur de vérifier lui-même la situation commerciale du client ; dans ce cas, il y aura lieu à une exonération totale ou partielle du banquier* »[141].

169. La BDL impose un traitement équitable et professionnel des clients, et de tenir compte de l'expérience et *background* de leur capacité à comprendre les opérations et appréhender les risques et profits, et s'assurer de la compatibilité du produit offert avec sa situation et ses besoins (art 3 Décision BDL 11947.

[139]C. Appel de Paris, 15ème Chambre - Section B 20 octobre 2006.
[140] T. com. Paris, 5 mai 2004, Ste Peyre c/Société Silog, Expertises 2004, p. 278.
[141] GHANNAGE (J), Le devoir de vigilance du banquier Ed. Sader 1996, p.20.

170. En matière d'investissement financier, il faut distinguer entre investisseur qualifiée et investisseur profane. L'article L411-2 du Code monétaire et financier français définit l'investisseur qualifié comme une personne, physique ou morale, « *disposant des compétences et des moyens nécessaires pour appréhender les risques inhérents aux opérations sur instruments financiers* ». cette distinction a un impact sur l'obligation d'information pesant à la charge de la banque. L'obligation est simplifiée et allégée quand la banque s'adresse à un investisseur qualifié.

Paragraphe 2 : Les moyens de preuve de l'exécution de l'obligation d'informer

171. Pour engager la responsabilité de la banque, le client peut se contenter d'alléguer devant les juges qu'il a été mal informé. Il s'agit là de l'application d'un principe général prétorien[142] selon lequel c'est à la charge du professionnel qu'incombe incontestablement la preuve de l'exécution de son obligation d'information[143] en démontrant que le client a été dument informé et a bien reçu sur support durable les informations préalables et que celles-ci ont été conservées par le client et n'ont pas été assujetties à des modifications (art. 15 de la DCE). Ces conditions sont assez complexes et impliquent un besoin de recourir à un support papier mais elles posent certainement une équivalence entre le support papier et le support durable[144].

172. La preuve se fait par tout moyen. Ainsi, tout acte ou fait peut servir de preuve que le client a été bien informé[145]. Toutefois, l'ignorance du client ne doit pas être admise aussi facilement comme c'était le cas auparavant notamment pour l'informatique[146].

---

[142]Cass. Civ 2e, 8 avr. 2004 : Bull. Civ. 2004, II, n° 163.

[143] Cass. 1ere Civ.13 fev. 1996, no. 09411726 et 94-12440 : Bull. I, no. 84 ; 29 avr.1997: Bull. I, no. 132 ; 15 mai 2002: Bull. I, 132.

[144] DEFOSSEZ Michel, « Droit communautaire, protection du consommateur de crédit et promotion du commerce électronique », Revue de Droit Bancaire et Financier, juillet-aout 2004, p. 284 (Dossier commerce électronique et opérations bancaires).

[145] Cass. 1ere Civ. 14 oct. 1997, no. 95-19609: Bull. I, no. 278.

[146]Cass. Com., 24 mars 1997, Brother, RJDA 1998, no.967 faisant allusion à "l'évolution prévisible des techniques qu'un acheteur professionnel pouvait subodorer ; CA Toulouse, 25 janvier 2001, FRS c/Société Actipole, JCP E 2001, p. 1001, note Le TOURNEAU (Ph).

173. Notons que les banques libanaises ont toujours recours à la technologie Out-of-Band (OOB) qui permet de mieux vérifier l'identité d'un utilisateur via un canal distinct (téléphone). Le recours à un canal distinct réduit le risque de corruption à la fois de l'internet et du canal additionnel. Lorsqu'un utilisateur initie une transaction (transfert de fonds par exemple), les informations peuvent être enregistrées et renvoyées à l'utilisateur par l'intermédiaire d'un appel téléphonique automatique ou d'un SMS pour vérification (envoi d'un code secret que le client doit insérée dans la case créée à ce propose) avant traitement de la transaction. La réponse de l'utilisateur est donnée soit par serveur vocal interactif[147], soit au clavier de l'ordinateur.

174. Cependant M. CLEMENT apporte une nuance à savoir que « *la responsabilité de la banque pour défaut d'information ne pourra être engagée que dans l'hypothèse où le manquement porte sur des informations utiles pour le client. Toutes les informations qui peuvent présenter un intérêt direct pour le client et dont la connaissance conditionne la réussite de l'opération doivent être communiquées* »[148].

175. La violation de l'obligation d'information est sanctionnée par l'annulation de la transaction (art. 1112-1 CCiv fr.) à condition que ce manque d'information ait eu des conséquences sur le consentement de la partie non informée.

176. Avant d'être une obligation légale, l'obligation d'information est « *un principe déontologique central où se rejoignent les impératifs de transparence et d'exécution parfaite des ordres du client* »[149]. L'information du client internaute est effectivement un pilier de protection de son consentement cependant cette protection doit s'étendre pour englober la protection des données personnelles en ligne.

[147] En anglais « Interactive Voice Response », IVR.

[148] CLEMENT (J-F), « Le banquier, vecteur d'informations », RTD Civ. 1997 p. 203 ; LABRUNIE (F), « Le devoir d'information du banquier et le secret professionnel », Gaz. Pal. 05 déc. 2000 n° 340, p. 22 ; SAINT-ALARY (B), « Aspects juridiques et pratiques de la tarification bancaire » (Dalloz, Edition 2016); COHEN-BRANCHE M., Tarification, relation de clientèle et opacité (conférence 30 mai 2005).

[149] Pezard A. et Eliet G., Droit et déontologie des activités financières – Comparaison internationale, Montchrestien, 1997, p.29.

Chapitre 2 : La protection des données personnelles en ligne

177. À l'ère de l'électronique, les informations personnelles sont devenues des «ressources naturelles »[150] que les géants du monde numérique (Google, Microsoft, Facebook) [151] se disputent et dont ils récoltent des revenus considérables. Il est par conséquent indispensable d'assurer la protection permanente des données personnelles et sensibles où qu'elles se trouvent mais aussi d'en limiter l'accès aux seules personnes autorisées, notamment en matière de banque en ligne[152].

178. A côté de ces géants virtuels, nous pouvons qualifier les banques comme une source et un lieu privilégié d'observation et d'analyse des situations des personnes physiques et morales étant donné le nombre et la variété d'informations collectées par les banques. D'où la nécessité de leur soumission à des obligations strictes à ce sujet.

179. Les données personnelles (données à caractère personnel) sont des informations qui permettent d'identifier une personne physique directement ou indirectement, telles que, à titre énumératif non exhaustif, nom, prénom, date de naissance, numéro de téléphone, adresse postale ou mail, identifiant de connexion informatique (adresse IP d'un ordinateur),

[150] CNIL, La protection des données personnelles, un atout pour la France et l'Europe, 28 septembre 2012 http://www.cnil.fr/la-cnil/actualite/article/article/la-protection-des-donnees-personnelles-un-atout-pour-la-franceetleurope/?tx_ttnews%5BbackPid%5D=2&cHash=c61b164e31b63e98669869fd5c44db7d__.

[151] Le 13 mai 2014, la Cour de justice de l'Union européenne a rendu son fameux arrêt qui oblige essentiellement Google à donner satisfaction aux internautes ressortissant de l'Europe qui demandent le retrait de résultats qui les concernent, consacrant ainsi l'existence d'un droit au déréférencement (sorte de droit à l'oubli light) sur le net. Un an plus tard, le 1er octobre 2015, la même Cour de justice a invalidé le régime juridique dit du « *Safe Harbor* » qui permettait aux entreprises américaines d'importer aux USA des données personnelles de citoyens européens. Celui-ci a été jugé invalide en raison des révélations d'Edward Snowden sur le programme PRISM, par lequel la NSA accèderait aux données stockées aux Etats-Unis.

[152] Un cybercriminel, disposant d'un nombre suffisant d'informations personnelles sur un individu peut commettre illégalement au nom de la victime et pour son compte des actes pécuniaires (falsification de chèques et vol de courriers électroniques ou plus sophistiquées comme les logiciels espions et l'exploration de données sur les réseaux sociaux). Dans une étude réalisée par la Verizon Business RISK Team, 74 % des failles de données provenaient de sources externes et 91 % de tous les cas concernés étaient liés à la criminalité organisée. Le rapport montrait également qu'une des cibles principales de la cybercriminalité était les services financiers et le vol des informations concernant le numéro d'identification personnelle (NIP) ainsi que les données relatives au compte bancaire : Verizon Business RISK Team. "2009 Data Breach Investigations Report." 2009. MC13626 0409. Web.

plaque d'immatriculation de véhicule, empreinte digitale ou génétique, photo, numéro de sécurité sociale, enregistrement vocal, données génétiques, etc.[153].

180. Certaines données sont sensibles parce qu'elles touchent à des informations qui peuvent donner lieu à discrimination ou préjugés tels qu'une opinion politique, sensibilité religieuse, engagement syndical, appartenance ethnique, orientation sexuelle, situation médicale ou idées philosophiques.

181. Conscient de l'insuffisance de protection des données personnelles qu'assurait la directive du 24 octobre 1995 face aux réseaux sociaux et moteurs de recherche, la Commission européenne a promulgué en 2016 le « Règlement Général sur la Protection des Données » (RGPD)[154], entré en vigueur très récemment en mai 2018. Ce règlement a le mérite d'uniformiser, au niveau européen, la réglementation sur la protection des données, de responsabiliser davantage les entreprises en développant l'autocontrôle, et de renforcer et mieux adapter les droits des personnes à l'évolution numérique[155].

182. La banque du Liban, a transposé les dispositions principales du RGDP dans sa décision de base 13 septembre 2018 [156]et a recommandé aux banques libanaises de prendre toute mesure nécessaire pour être en accordance avec les dispositions et l'esprit du RGDP.

183. La protection des données est un « droit fondamental » selon le premier considérant du RGPD. Elle est assurée à un double niveau d'une part, par les droits accordés au propriétaire des données (Paragraphe 1) et d'autre part, par les obligations imposées au professionnel (Paragraphe 2).

---

[153] Tribunal correctionnel de Privas, 3 sept. 1997: http://www.cyberlex.org/haas/coquine.htm, note HAAS G. et TISSOT O.

[154] Règlement 2016/679 du Parlement Européen du 27 avril 2016 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) mis en vigueur mai 2018.

[155] Bien que récemment adopté, le RGPD fait déjà fait l'objet de vives critiques de la part de certains observateurs. La principale inquiétude réside dans le fait que le RGPD constituerait, au niveau européen, un véritable frein à toutes les formes d'innovation (surtout intelligence artificielle) dont la concrétisation nécessite la mise en œuvre d'un traitement massif de données : Rizk (P.A) « Le RGPD va-t-il ralentir l'Union Européenne en matière d'intelligence artificielle ? » https://www.actuia.com/actualite/rgpd-va-t-ralentir-lunion-europeenne-matiere-dintelligence-artificielle/.

[156] Décision de base no. 12872 du 13 septembre 2018 (Circulaire 146) relatif aux procédures de conformité avec le Règlement Européen de la protection des données personnelles.

Section 1 : Les droits accordés au client concernant ses données personnelles

184. Les droits de la personne dont les données personnelles sont collectées, traitées, transférées ou même usurpées sont dorénavant protégés par le RGDP, sous l'égide de la CNIL[157]. En France, ces droits étaient déjà régis par la loi Godfrain de 1998[158], toutefois, le législateur français va devoir transposer le contenu de ce règlement en droit interne. Au Liban, ces données sont protégées par le secret bancaire.

185. L'apport principal du RGDP consiste en l'obtention préalable du consentement écrit, clair et explicite de l'internaute avant tout traitement de ses données personnelles, en l'assurance que les enfants en-dessous d'un certain âge (quinze ans) aient bien reçu l'aval de leurs parents avant de s'inscrire sur un réseau social.

186. Les droits accordés à la personne concernée sont précisément le droit d'accès, le droit de rectification, le droit à la portabilité des données, le droit à la limitation du traitement, le droit à l'oubli[159] numérique ou droit d'effacement et enfin le droit d'opposition.

187. En premier lieu, la personne concernée a un droit d'accès[160] aux données personnelles en vertu de l'article 15 RGDP. Ainsi, toute personne jouit du droit de demander du

[157] Les Guides de la CNIL « La sécurité des données personnelles », Edition 2018.

[158] La loi Godfrain du 5 janvier 1988 (loi nº 88-19) relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage. Nommée d'après le député RPR Jacques Godfrain, c'est l'une des lois pionnières concernant le droit des nouvelles technologies de l'information et de la communication (NTIC)., après, notamment, la loi Informatique et libertés de 1978, qui introduit la notion de système de traitement automatisé de données (STAD) et prévoit plusieurs dispositions corrélatives de la loi Godfrain (notamment concernant les obligations du responsable du traitement quant à la garantie de la sécurité des données - art. 34).https://www.legifrance.gouv.fr.

[159] Ce droit à l'oubli, qui est un droit de la personnalité, vise à protéger la vie privée des individus qui, à un moment de leur existence se sont retrouvés impliqués dans un événement qui a été médiatisé. L'idée des juges qui ont créé ce droit est que, si au moment des faits, par exemple au cours d'un procès, des éléments concernant la vie privée d'un individu peuvent être rendus publics au nom du droit à l'information, cette exception est liée à « l'actualité » de ces faits. Par conséquent, quand, des années plus tard, une personne décide de publier de nouveau ces mêmes informations, la personne concernée, qui ne pouvait empêcher leur parution à l'époque des faits, pourrait s'y opposer au nom du « droit à l'oubli ».

responsable de traitement des données d'obtenir les informations relatives à la finalité du traitement, au destinataire auquel ces informations ont été ou seront communiquées, et spécifiquement si ces destinataires se trouvent dans des pays tiers ou sont des organisations internationales, la durée de conservation ou encore l'existence d'un profilage[161].

188. De même, la personne jouit d'un droit de rectification, dans les meilleurs délais, des informations inexactes (art. 16 RGDP). Ce droit inclut également le droit de compléter les informations incomplètes.

189. La personne bénéficie également du droit à l'oubli[162] ou de suppression qui est un démembrement du droit d'accès. Ce droit consiste à exiger du responsable du traitement que ces données soient effacées lorsqu'elles ne sont plus nécessaires au regard des finalités de leur collecte. Ainsi, la personne dont les informations sont enregistrées au FICP[163] ou Centrale des Risques auprès de la BDL, a le droit, moyennant certaines conditions, de demander la suppression de son affichage sur la liste des récalcitrants[164].

---

[160] Le droit d'accès de la personne dont le crédit a été refusé par exemple s'exerce en envoyant à la banque un courrier en joignant une photocopie de sa pièce d'identité. Suite à cette demande, la banque est tenue de délivrer une copie des informations qu'il détient sur cette personne dans ses fichiers, sans motivation de la décision de refus du crédit, la banque jouissant d'un pouvoir discrétionnaire d'accorder ou non un crédit.

[161] Le terme profilage est défini à l'article 4 du RGDP « *utiliser les données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pur analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la sante, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

[162] Ce droit existe dans l'art. L.333-4, I alinéa 2 du C. Consom. A la base, le droit à l'oubli est une notion de création prétorienne de plusieurs juridictions du fond. On peut la définir comme le principe selon lequel «*toute personne qui s'est trouvée associée à un événement public, même si elle en a été le protagoniste, est fondée à revendiquer un droit à l'oubli et à s'opposer au rappel d'un épisode de son existence* » TGI Paris, 25 mars 1987 *: D. 1988, somm. p. 19.* Il faut noter que la Cour de cassation, dans l'arrêt Monange (Cass. 1re civ. 20 nov. 1990, *Dame Monanges c/ Kern et autres* : JCP G 1992, II, 21908, note J. RAVANAS), semble avoir refusé de reconnaitre ce principe. Pourtant, la doctrine a largement critiqué cette décision, considérant le droit à l'oubli légitime.

[163] En France, le fichier national des incidents de remboursement des crédits aux particuliers (ou FICP) liste l'ensemble des personnes ayant été par le passé incapables de rembourser à échéance un crédit. Il est géré par la Banque de France. Le FICP a été créé par la loi du 31 décembre 1989 relative à la prévention et au règlement des difficultés liées au surendettement des particuliers et des familles afin de donner aux établissements de crédit un élément d'appréciation sur la solvabilité des personnes qui sollicitent un crédit.

[164] Dans son guide sur les données personnelles et refus de crédit, la CNIL reprend les conditions de l'article L. 333-4, II, 2 du code de la consommation relatives à la suppression de cette inscription à savoir dès la régularisation de la dette, à défaut, à l'expiration d'un délai de 5 ans ; en cas de procédure de surendettement,

190. De plus, la personne est investie d'un droit à la portabilité de ses données ce qui lui permet de s'approprier ses propres données et donc d'en demander la restitution afin de pouvoir les stocker et les réutiliser pour son usage personnel, comme bon lui semble mais aussi les transférer à un autre responsable, l'un des objectifs affichés de ce nouveau droit consistant à faire jouer la concurrence entre les différents responsables de traitement (à l'image de ce qui existe en matière de portabilité des numéros de téléphone par exemple). Le responsable de traitement ne pourra pas s'opposer à la demande de la personne concernée.

191. La personne jouit par ailleurs d'un droit à la limitation du traitement lorsque le responsable n'en a plus besoin, notamment lorsque le traitement est illicite.

192. Enfin, la personne a le droit à tout moment de s'opposer au traitement des informations fournies pour des fins de prospection commerciale ou pour le profilage. Une fois ce droit exercé, le responsable doit cesser de traiter de ces données sauf s'il justifie l'existence des motifs légitimes et impérieux pour le traitement qui prévaut sur les intérêts et droit et libertés de la personne concernée. Ce droit s'exerce gratuitement et par le biais de spécimens en ligne. Concernant l'efficacité de ce droit, elle est extrêmement restreinte dans certains cas, le motif légitime étant une notion très vague et non délimitée par le règlement. Ce droit se heurte par ailleurs à la réticence des banques qui sont tentées de conserver ces données afin de proposer d'autres services ou pour les transmettre à d'autres établissements du même groupe (établissements de crédit, compagnies d'assurance).

193. Notons que la CNIL soucieuse de supprimer les données personnelles des personnes qui le souhaitent, a mis en place, en juin 2010, un système de « plainte en ligne»[165] qui aide notamment les personnes désireuses à supprimer leurs données.

à l'expiration d'un délai de 10 ans ou dès le règlement intégral des dettes auprès de tous les créanciers figurant au plan ou au jugement. Ce droit ne s'applique pas dans la mesure où le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information, ou pour une obligation légale ou pour motifs d'intérêt public, ou à l'exercice de droits en justice.

[165] http://www.cnil.fr/vos-libertes/plainte-en-ligne/.

Section 2 : Les obligations à la charge de la banque traitant des données personnelles

194. Les données bancaires et financières traitées sont investies d'une sensibilité telle que le niveau de protection à mettre en place par la banque doit être particulièrement important.

195. En espérant mettre fin à ce marché noir des données personnelles, le RGDP a prévu des sanctions importantes et assez dissuasives de manière à obliger les entreprises à agir avec plus de transparence dans la collecte de données à caractère personnel. Des amendes administratives peuvent ainsi être imposées par les autorités de protection des données, et s'élèvent potentiellement à la somme de 10 à 20 millions d'euros ou de 2% à 4% du chiffre d'affaires mondial de l'entreprise, sachant que l'organisme retiendra le montant le plus élevé (art. 83 du RGDP).

196. Nous allons traiter l'exigence d'informer le client sur le sort de ses données personnelles (Paragraphe 1) avant de donner un aperçu sur les autres obligations imposées quant aux données personnelles (Paragraphe 2).

Paragraphe 1 : Exigence d'informer le client sur le sort de ses données personnelles

197. Le responsable du traitement au sein de la banque, lors de la collecte les données d'une personne, doit lui fournir un certain nombre d'informations dont la liste figure aux articles 13 et 14 du RGPD. Ces informations sont notamment l'identité du responsable du traitement ou de son représentant et ses coordonnées ; la finalité et base juridique du traitement ; les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale.

198. S’y ajoutent les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent: a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée; b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données; c) l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci; d) le droit d'introduire une réclamation auprès d'une autorité de contrôle; e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données; f) l'existence d'une prise de décision automatisée, y compris un profilage.

199. Ces informations peuvent être fournies par écrit ou oralement à la demande de la personne concernée lorsque son identité est démontrée par d’autres moyens, ou par voie électronique lorsque cela est approprié. L’information doit être communiquée de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs, simples et gratuitement.

Paragraphe 2 : D’autres obligations nouvellement édictées

200. Le RGDP[166] vise à responsabiliser davantage les entreprises dans leur traitement des données à caractère personnel. Cela se traduit par les nouvelles obligations édictées.

[166] Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

201. L'un des apports du RGDP est de créer le statut du « responsable de traitement[167] » mais aussi du « sous-traitant [168]». L'unique contact avec les autorités se fait par le biais du représentant légal de l'entreprise. Certaines responsabilités seront toutefois partagées avec le sous-traitant, qui devra respecter des obligations spécifiques en matière de sécurité et de confidentialité. En cas de faille de sécurité au niveau du sous-traitant, un régime de dualité de responsabilité du sous-traitant et de l'entreprise cliente (précisément le responsable des traitements au sein de cette entreprise) a été conçu. En conséquence, les entreprises devront revoir les contrats signés avec les sous-traitants en intégrant des clauses concernant les DCP.

202. Le responsable doit documenter toutes les mesures et procédures en matière de sécurité des données dans un registre de traitement qu'il met à la disposition de la CNIL pour but de contrôle. Ce registre permettra de constituer une base de données des traitements, mais pourra aussi servir à centraliser et à suivre toutes les démarches de conformité mises en œuvre par l'entreprise.

203. De nouvelles responsabilités[169], plus accrues qu'auparavant, sont mis à la charge du responsable en relation avec la sécurisation des données. Ainsi, le responsable de traitement doit mettre en place des mesures techniques et organisationnelles appropriées (par exemple la *pseudonymisation*[170] et test d'intrusion) pour réduire les risques sur les données de manière effective.

---

[167] L'article 1 du RGDP définit le responsable du traitement comme étant «la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

[168] L'article 1 du RGDP définit le sous-traitant comme étant « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

[169] C'est un des changements les plus notables du nouveau régime : les obligations de déclarations préalables (« les déclarations CNIL ») sont supprimées et remplacées par l'obligation pour le responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles pour s'assurer et démontrer la conformité du traitement au Règlement, dans une logique de « *compliance* », étant entendu que les autorités de contrôle (la CNIL en France) seront chargées de vérifier le respect de l'ensemble de ces obligations.

[170] La *pseudonymisation* est définie par l'article 1 du RGDP : « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir

204. En outre, le responsable de traitement est tenu d'effectuer une analyse d'impact, avant la réalisation d'un traitement. S'il ressort de cette analyse que le traitement présente un risque élevé pour les droits et libertés des personnes, notamment en cas d'utilisation de « nouvelles technologies », il doit prendre des mesures pour minimiser ces risques.

205. Un nouveau principe de « *Privacy By Design* » est établi. Il concerne toute la démarche visant à prendre toutes les mesures protectrices des droits des personnes en amont (dès la conception d'un produit ou d'un service) et tout au long du cycle de vie des données (de leur collecte à leur suppression).

206. Finalement, le RGDP invite à l'élaboration de codes de conduite destinés à contribuer à la bonne application du règlement (art.40). Ces codes serviront à instruire le consommateur et le professionnel et à répudier les tentatives de fraude à ce propos.

207. Le RGDP encadre strictement le mode de gestion des cookies[171] ou témoins de connexion ou encore traceurs. Le législateur communautaire a voulu encadrer les cookies parce qu'ils servent notamment à collecter des données relatives aux clients, afin de leur proposer des offres personnalisées en fonction de leurs préférences[172]. Le RGDP exige la mention de la finalité[173] du cookie, du droit d'opposition de l'utilisateur et l'acceptation implicite de l'utilisateur si celui-ci décide de poursuivre sa navigation. Le bandeau d'information ne devra pas disparaître tant que l'utilisateur n'aura pas poursuivi sa navigation (en ouvrant une nouvelle page par exemple). Aucun cookie ne pourra être

---

recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »

[171] Ce sont des enregistrements d'informations par le serveur dans un fichier de texte situé sur l'ordinateur du client, que ce serveur peut ultérieurement relire et modifier.

[172] Pour citer quelques exemples, un navigateur garde en mémoire les informations de connexion, les identifiants voire les langues de préférence, ce qui permet aux internautes de ne pas avoir à constamment configurer leur programme. Au-delà de l'aspect pratique, les critiques de ce système soulignent le fait que les cookies sont incompatibles avec une politique stricte de confidentialité. En effet, la plupart des cookies sont appliqués afin de pointer certains aspects du comportement des utilisateurs et par exemple aider les acteurs du Web à mieux cibler leurs publicités.

[173] Les cookies sont parfois installés d'une façon clandestine et à l'insu du titulaire de l'appareil. Cette façon de procéder est très contestable et constitue généralement une violation de la vie privée.

déposé si l'utilisateur rebondit sur la page – sauf les cookies [174] nécessaires au bon fonctionnement du site.

208. Le RGDP[175] a également préconisé la nomination d'un délégué à la protection des données. C'est le *« data processing officer »* (DPO) qui est chargé de toute question relative à la protection des données personnelles et notamment informer et conseiller le responsable de traitement ou le sous-traitant, et coopérer avec l'autorité de contrôle. Cette nomination est obligatoire lorsque le traitement est effectué par une autorité ou organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle (article 37-1-a) ; *ou si* « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées » (art. 37-1-b). Depuis la décision de base no. 12872 de la BDL, les banques libanaises sont tenue de nommer un DPO chargée de la protection des données personnelles.

209. En cas de faille de sécurité ou violation de données personnelles, le responsable doit notifier la CNIL et les personnes concernées dans un délai de 72 heures. Les personnes physiques concernées devront être informées « dans les meilleurs délais » si la faille ou la violation de données comporte un risque élevé pour les droits et libertés.

210. Au Liban, l'avant-projet ECOMLEB a proposé une autorité de protection de données personnelles qui serait une autorité administrative indépendante. Sa mission est d'informer les personnes concernées et de veiller au bon traitement des données personnelles.

[174] https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi

[175] Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

211. En outre, notons que la pratique a été avant-gardiste et n'a pas attendu la législation. Ainsi, pour maitriser la circulation des données, des organismes ad hoc « nettoyeurs de réputation » ont été mis en place pour assurer aux abonnées, un monitor sur leurs données qui les alerte lorsque leur donnée est présente sur un site. Aux Etats Unis, nous retrouvons *Reputation defender*[176] ou et en Angleterre « *e-reputation* ». Si la publication de la donnée en question est contre le gré du client, l'organisme s'occupe de sa suppression ou modification[177]. En France, une start-up dénommée «*Reputation Squad* »[178] est établie et tend à préserver l'image et la réputation en ligne de ses clients et accompagne ces derniers dans la démarche de suppression de leurs données personnelles. Au Liban, aucun véhicule n'est envisagé à ce sujet. Les personnes morales font elles-mêmes par le biais de leur e-marketing personnel chargé des comptes de réseaux sociaux en font ce devoir.

212. La sécurisation de la transaction bancaire en ligne au niveau contractuel est assurée lorsque le client internaute est capable, identifié et authentifié que ce soit par sa signature électronique ou par des tiers certificateur mais aussi lorsque le consentement et les données personnelles du client internaute sont protégés.

213. La sécurisation du cadre contractuel est nécessaire mais pas suffisante. D'où la nécessité d'élargir la panoplie de la sécurisation pour englober le cadre institutionnel. Ainsi la transaction doit être sécurisée sur le plan technique et pratique technique.

[176] http://www.ecrans.fr.ReputationDefender-nettoyeur-d.html
[177] Voir sur ce point : « Les nettoyeurs du Net », Le Monde 13.01.2010, article consultable sur : http://www.lemonde.fr/technologies/article/2009/11/23/les-nettoyeurs-du-net_1270862_651865.html
[178] http://www.reputationsquad.com

Partie 2 : Sécurisation du cadre institutionnel

214. L'internet offre de facto une envergure internationale et une omniprésence aux activités s'opérant en ligne. Cette ubiquité a créé un doute concernant l'applicabilité du droit national à ces activités.

215. Il est vrai qu'il n'y a pas une cyber-législation ou *lex electronica* propre aux activités et transactions en ligne. Pour autant, cela ne veut pas dire qu'il y a un vide juridique en matière d'internet, ce que confirme le Conseil d'Etat français, dans son rapport le 2 juillet 1998[179] statuant sur les problématiques juridiques engendrées par l'apparition d'internet. Ce rapport commence par affirmer que « *contrairement à ce que l'on entend parfois, l'ensemble de la législation existante s'applique aux acteurs d'Internet, notamment les règles de protection du consommateur et celles qui garantissent le respect de l'ordre public. Il n'existe pas et il n'est nul besoin d'un droit spécifique des réseaux* ». Ce constat est réconfortant. Il n'est toutefois pas toujours vrai du fait que les activités en ligne se sont développées d'une façon telle que les droits nationaux s'avèrent insuffisants à régir leur diversité.

216. En tout état de cause, « *que ce soit en droit français ou en droit libanais, les tribunaux, en l'absence de textes spécifiques règlementant de manière complète et claire une opération bancaire complexe et originale, sont souvent obligés de revenir au droit commun civil et commercial et surtout de se référer aux usages de la pratique bancaire qui sont leur principal point de repère* »[180].

[179] Analyse des questions juridiques suscitées par le développement d'internet et mise en évidence des adaptations nécessaires du droit. Les principales conclusions sont les suivantes : - ne pas créer un droit spécifique à Internet, - protéger les données personnelles et la vie privée, - favoriser les échanges par une confiance accrue des acteurs (sécurité des transactions électroniques, reconnaissance de la valeur juridique du document et de la signature électroniques, cryptologie, adaptation de la fiscalité, droit des marques...), - valoriser les contenus par la protection de la propriété intellectuelle et la lutte contre la contrefaçon, - lutter contre les contenus et comportements illicites, - adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications.

[180] Safa Gannage J, Devoir de vigilance du banquier , op. cit. no. 23

217. Dans cette deuxième partie, nous allons exposer les moyens de sécurisation des transactions en ligne au niveau technique (Titre 1) et au niveau juridique (Titre 2).

Titre 1 : Sécurisation technique des transactions bancaires en ligne

218. La sécurisation des transactions en ligne ne peut être limitée aux efforts, bien que glorieux du législateur. D'où le rôle crucial des techniciens et informaticiens qui se sont engagés à collaborer à la sécurisation des transactions bancaires en ligne étant donné que ces dernières sont dotées d'une nature informatique et technique au-delà de leur aspect légal. Ainsi nous constatons l'existence d'une série de dispositifs techniques sécuritaires en constante amélioration.

219. L'activité bancaire, étant une activité sensible, a été l'objet d'un système de règlementation assez rigide auquel s'ajoute un système de contrôle et de tutelle bien établi. Ces systèmes de réglementation et de contrôle sont-ils applicables au niveau des activités bancaires en ligne ? Doivent-ils être modifiés ou nuancés pour être compatibles avec la nature virtuelle de ces activités en ligne ? La banque en ligne serait-elle assujettie à de nouvelles obligations ?

220. Nous allons démontrer que la banque en ligne est, à quelques différences près, une banque classique (Chapitre 1), pour exposer ensuite la sécurisation au niveau du cadre organique (Chapitre 2).

Chapitre 1 : La banque en ligne, une banque classique ?

221. Le livre blanc[181] de la Banque de France prévoit que réaliser des opérations bancaires en ligne ne constitue pas un type nouveau d'activité. Le réseau joue simplement le rôle d'un nouveau media ou moyen permettant l'exercice de ces opérations à distance, sans considération de frontières géographiques.

222. D'ailleurs, la DSF 2002 souligne ce principe en définissant, dans son article 2, le fournisseur de services comme étant « *toute personne physique ou morale, publique ou privée, qui, dans le cadre de ses activités commerciales ou professionnelles, est le fournisseur contractuel des services faisant l'objet de contrats à distance* ».

223. Quelle serait l'institution habilitée à fournir des prestations et conclure des services bancaires en ligne ? Toute banque nationale est-elle habilitée à exercer des activités bancaires et financières sur internet ou devrait-elle obéir à quelques obligations supplémentaires et obtenir une autorisation spécifique pour l'exercice des opérations en ligne ?

224. Nous allons aborder dans en premier lieu l'agrément requis pour l'exercice des activités bancaires et l'étendue de cet agrément (Section 1) avant de présenter l'identification de la banque en ligne (Section 2).

[181] Conseil d'Etat français, Internet et les réseaux numériques, Paris, éd. La Documentation française 1998.

Section 1 : L'agrément et son étendue

225. L'agrément implique que les entreprises qui traitent des activités financières avec des tiers disposent des qualités adéquates, notamment d'une compétence convenable et de moyens techniques et financiers suffisants.

226. Nous allons démontrer l'exigence et la nécessité d'un agrément pour l'exercice des activités bancaires en ligne (Paragraphe 1) avant d'indiquer l'étendue de cet agrément (Paragraphe 2).

Paragraphe 1 : L'agrément, condition nécessaire et garantie de sécurisation

227. En France et au Liban, comme dans la plupart des autres pays d'ailleurs, l'exercice des activités bancaires est strictement réservé aux établissements dotés d'un agrément et soumis à une surveillance particulière. Ainsi pour effectuer des activités bancaires en ligne, le prestataire doit être, de prime abord, habilité (c'est-à-dire obtenir un agrément)[182] à exercer lesdites activités hors ligne, ces nouvelles techniques en ligne étant des activités complémentaires.

228. Au Liban, l'article 128 du code de la monnaie dispose que l'accès à la profession bancaire est subordonné à un agrément délivré par la BDL qui jouit d'un pouvoir discrétionnaire à ce propos (article 131 Code de la monnaie) et à l'inscription sur la liste des banques agréées auprès de la BDL (article 136 du Code de la monnaie).

[182] Article L511-10 modifié par la loi n°2010-1249 du 22 octobre 2010 - art. 12 (V) du Code de la monnaie : « Avant d'exercer leur activité, les établissements de crédit doivent obtenir l'agrément délivré par l'Autorité de contrôle prudentiel mentionné au 1° du II de l'article L. 612-1. L'Autorité de contrôle prudentiel vérifie si l'entreprise satisfait aux obligations et l'adéquation de la forme juridique de l'entreprise à l'activité d'établissement de crédit. Elle prend en compte le programme d'activités, les moyens techniques et financiers mis en œuvre. L'Autorité apprécie également l'aptitude de l'entreprise requérante à réaliser ses objectifs de développement dans des conditions compatibles avec le bon fonctionnement du système bancaire et qui assurent à la clientèle une sécurité satisfaisante. L'Autorité peut refuser l'agrément en l'absence d'honorabilité et compétence nécessaires ainsi que l'expérience adéquate à leur fonction».

229. En fait, l'obtention d'un agrément préalable constitue une exception au principe général de la liberté du commerce et de l'industrie. Mais cette exception est amplement justifiée par plusieurs préoccupations, dont notamment la protection du public, la surveillance de la monnaie et du crédit, le bon fonctionnement des marchés de capitaux, qui nécessitent que les établissements qui effectuent à titre habituel des opérations de collecte, de dépôts, ou de distribution de prêts soient soumis à un contrôle particulier.

230. En France, l'autorité compétente pour accorder cet agrément[183] c'est l'Autorité de Contrôle Prudentiel et de Résolution (ACPR)[184] qui est une autorité administrative indépendante dont la mission est de veiller à la préservation de la stabilité du secteur financier et à la protection des clients, assurés, adhérents, et bénéficiaires des personnes soumises à son contrôle[185].

231. L'agrément suppose la conformité à un code de conduite et des normes strictes que l'autorité compétente exige et surveille l'application. En vue d'accorder l'agrément, l'autorité de contrôle vérifie si l'entreprise satisfait à certaines obligations telles que le capital minimum[186], la forme juridique[187]. Elle prend en compte, dans son évaluation, le programme d'activités de cette entreprise, les moyens techniques et financiers prévus ainsi que la qualité des apporteurs de capitaux et, le cas échéant, de leurs garants. L'autorité peut refuser l'agrément en l'absence d'honorabilité, incompétences, ou manque d'expérience adéquate à leur fonctionnement (article L511-10 code monétaire fr.).

---

[183] T. Bonneau, Droit bancaire : les conditions de délivrance de l'agrément et les libertés communautaires, Montchrestien, 4e éd. 2001, n° 187. Bonneau T., Drummond F, Droit des marchés financiers : Economica, 1ere éd. 2001, n° 389. Adde, J. Pardon, Les quiproquos des reconnaissances mutuelles : RD bancaire et bourse 1992, p. 237.

[184] L'ACPR est prévu par l'article L612-1 modifié par Ordonnance n°2016-351 du 25 mars 2016 - art. 1. Elle est venue remplacer le Comité des établissements de crédit et des entreprises d'investissement (CECEI) qui était investi de ce pouvoir par la loi bancaire du 24 janvier 1984 et la loi de modernisation des activités financières du 2 juillet 1996. L'ACPR dispose du pouvoir de prendre des mesures de police administrative et d'un pouvoir de sanction.

[185] Aux Etats-Unis, les activités bancaires sont régies par le « United States Code » et la procédure d'agrément est largement contrôlée par l' « *Office of the Comptroller of the Currency* » (OCC) au sein du «*Department of the Treasury* » selon le titre 7 du Code de Réglementation Fédérale.

[186] Article L. 511-11, L. 511-13 : « Les établissements de crédit et les sociétés de financement doivent disposer d'un capital initial libéré entre un million et cinq millions d'euros». En droit libanais, le capital minimal est devenu sept milliards livres libanaises.

[187] En droit libanais la banque doit être constituée en une société anonyme (article 126 Code de la monnaie).

232. Au Liban, pour exercer des activités bancaires en ligne, le seul agrément ne suffit pas. Une notification préalable à l'autorité de contrôle est requise préalablement à tout commencement d'activité en ligne (article 3 de la Décision de base no. 7548 de la BDL). La BDL a réservé les activités bancaires électroniques aux banques, sous condition d'un préavis à la BDL, et aux institutions financières, sous condition d'une autorisation préalable de la BDL relative à l'exercice d'activités bancaires via internet[188].

233. Nous considérons que l'agrément constitue une garantie de sécurisation juridique pour le client internaute. Sans l'agrément, le client internaute ne pourra point avoir accès à ses droits et ne sera point protégé en cas d'actes abusifs ou délictuels subis.

Paragraphe 2 : L'étendue de l'agrément

234. Un prestataire agréé dans son Etat d'origine pour des activités hors ligne doit-il obtenir un nouvel agrément s'il exerce en ligne la même activité ? La réponse doit, en principe, être négative[189]. L'agrément du pays d'origine doit pouvoir chapoter les activités bancaires en ligne.

235. Le site internet de la banque n'est, en effet, qu'un outil pour rendre accessibles à distance et même de l'étranger les services approuvés initialement et ne rend point la banque en situation d'exercice illégal de la profession sur d'autres territoires que celui de son siège social. En revanche, c'est la destination du site à des clientèles non-résidentes qui peut amener celui-ci à agir sur le territoire d'autres Etats[190].

[188]Article 2 de la Décision Intermédiaire de la BDL no. 11445 du 6 juin 2013: La pratique des opérations financières et bancaires par les moyens électroniques impose aux banques et à tous les établissements inscrits auprès de la BDL ou soumis son contrôle, les établissements de change exclus, d'aviser préalablement la BDL de leur volonté d'exercer entièrement ou partiellement par n'importe lequel des moyens électroniques, l'activité qui lui est allouée, et ce 30 jours avant la date de lancement ou de commercialisation anticipée de cette activité ou de tout amendement à une activité préalablement notifiée à la BDL.

[189] Sousi-Roubi V. B., Directives bancaires et commerce électronique : quelle articulation ?, Les Echos, 31 janv. 2001, p. 11. Costes L., Ribeyre M.-A., Une meilleure articulation européenne entre commerce électronique et services financiers : Lamy, droit du financement, avr. 2001, Bull. A, n° 118.

[190] Banque de France, Livre Blanc 2000, op cit, p.15-16.

236. Si le site bancaire est destiné à la seule clientèle résidente, cela suppose que la prestation de service bancaire sur internet est englobée par l'agrément de base qui octroie la qualité de banque à l'entreprise par l'autorité de tutelle compétente.

237. De même, l'article 2 (c) de la directive DCE 2000[191] précise que la présence et l'utilisation des moyens techniques et technologiques requis pour fournir le service ne constituent pas en tant que tel un établissement du prestataire. Par conséquent, le prestataire doit respecter les règles de son lieu d'établissement et non celles du pays où il intervient.

238. En conclusion, en France, l'activité en ligne n'est pas une activité de nature différente de l'activité hors ligne, de sorte que son exercice n'implique pas un agrément préalable lorsque les activités hors ligne sont permises dans le cadre de l'agrément du pays d'origine[192].

239. Cependant, si l'établissement bancaire vise, par le biais de l'internet, à opérer des activités bancaires dans un autre pays, et cible de ce fait des clients non-résidents, cet établissement sera alors obligé de s'en soumettre au droit de cet autre pays et de solliciter l'agrément de l'autorité de contrôle locale.

240. Au Liban, la BDL est ferme à ce sujet. L'article 3-3 de la décision no. 7548 oblige les établissements étrangers, voire les branches des établissements étrangers, à obtenir une autorisation préalable à tout exercice d'activité bancaire si ces opérations ou offres de services sont destinées à la clientèle libanaise.

241. Enfin, la banque doit exercer ses activités en ligne conformément au contenu de son agrément et doit maintenir sa situation adéquatement compatible avec les législations nationales.

---

[191] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).

[192] MATHIEU ME, Transactions bancaires et financières à distance, Juris classeur, Banque-Crédit-Bourse, 2004, Fasc. 125.

Section 2 : Identification de la banque en ligne

242. La source des problèmes majeurs sur internet réside dans l'absence d'identité sur internet et d'identification des opérateurs. En effet, il existe une multitude d'identités sur internet, la plupart déclaratives, certaines dupliquées ou certifiées mais aucune universelle[193]. C'est le sens de la l'expression « *sur internet, personne ne sait que tu es un chien* »[194] ou aussi « *personne ne sait que tu es un robot* »[195].

243. Nous allons décrire dans un premier temps l'identification de la banque en ligne par un nom de domaine (Paragraphe 1) et puis nous intéresser dans un deuxième temps à la sécurisation du nom du domaine (Paragraphe 2).

Paragraphe 1 : Identification de la banque en ligne par un nom de domaine

244. Dans le monde virtuel, le contact entre la banque et le client sur internet se fait sur le réseau informatique de la banque, qui servira d'identification électronique et de plateforme pour l'exercice des activités bancaires et la conclusion des transactions avec les clients.

245. Ce nom de domaine peut avoir une vocation étendue ou limitée[196]. Ainsi par exemple, une banque libanaise peut se suffire du domaine d'ordre national ou souhaiter avoir une vocation internationale[197]. Le nom du domaine peut aussi être doté d'un « label »[198] qui sous-entend sa conformité aux principes de transparence, de loyauté, et d'honnêteté. Ainsi

---

193 http://reseau.fing.org/blog/view/51641/identite-certification-et-confiance-numerique-dans-la-banque-sur-internet.

194 «On the Internet, nobody knows you're a dog ».

195 D'ailleurs, Mr. Éric SCHMIDT, président-directeur général de Google préconise la nécessité de mettre fin à l'anonymat parce qu'il freine le développement de l'internet.

196Les noms de domaine dont l'extension est « com », « net », «org », « edu » sont appelés des « gTLD » Generic Top Level Domain Name. Les noms de domaine comportant une extension définie une combinaison de lettre relative à des pays sont dénommés « ccTLD » Country Code Top Level Domain.

197 Au plan national (www.xyz.com.lb) au plan international (www.xyz.com).

198 Ce label de qualité est accordé par des autorités qui contrôlent la conformité de la banque aux normes à l'échelle interne et externe. Ce contrôle est entrepris de façon continue.

le client internaute, en repérant le label sur le site de la banque, s'assure qu'il s'agit d'un site authentique.

246. La nature juridique du nom du domaine a fait l'objet de plusieurs controverses doctrinales. Certains auteurs ont considéré qu'il s'agit d'une simple dénomination. Pour eux, un site est une[199] des « facettes d'internet »[200]. C'est un support et non un service en soi[201]. D'autres l'ont qualifié d'« enseigne sous laquelle une entreprise exploite, sur le réseau internet, un établissement virtuel auquel une clientèle peut s'adresser pour obtenir des biens et services »[202]. Par conséquent, le nom de domaine constitue un élément de propriété immatérielle[203]. Nous considérons que le nom du domaine dépasse sa fonction comme simple dénomination et constitue pratiquement une *res electronica*[204]. D'où nous témoignons de nos jours des magasins en ligne (e-stores) virtuels auxquels s'adresse la clientèle pour obtenir des biens et services. D'ailleurs, il existe des entités ou même banques qui opèrent exclusivement en ligne.

247. La banque doit s'identifier en mettant à la disposition de ses clients un minimum d'informations générales y relatives.

248. En droit français, ces informations obligatoires sont le nom du prestataire, l'adresse de son siège social, ses coordonnées (adresse de courrier électronique facilitant la communication directe et efficace), le numéro d'immatriculation au registre du commerce, l'autorisation et l'autorité de surveillance à laquelle son activité est soumise, l'ordre professionnel auprès duquel il est inscrit[205], son titre professionnel et l'état membre dans

[199] L'autre facette étant les blogs ou sites personnelles.
[200] TGI Paris, ref., 20 nov. 2000, Yahoo c/ LICRA et UEJF, Comm. Com. Electr. 2000, no. 132, note J.C. GALLOUX.
[201] Cass. Com. 13 déc. 2005, Ste Soficar c/ Ste Le Tourisme Moderne, D. 2006, AJ p. 63, obs. C Manara.
[202] LOISEAU George, Nom de domaine et internet : turbulence autour d'un nouveau signe distinctif, Dalloz 1999, Chronique, p. 245. Voir aussi en jurisprudence TGI Paris, 8 avr. 2005, Ministères public c/ Nicole T., RLDI sept 2005, p.31.
[203] Cyril Fabre, noms de domaine. De l'identifiant technique à une nouvelle forme de droit de propriété incorporelle par destination ?, Legalis.net 2002/3 p.8.
[204] CA Paris, 18 oct. 2000, Virgin interactive, D2001, p.1379, note Loiseau G.
[205] Conformément à l'article 24-I de la loi 96-597 du 2 juillet 1996 de modernisation des activités financières.

lequel il a été octroyé, une référence aux règles professionnelles applicables et aux moyens d'y accéder, son numéro de TVA (art. 19 de la LCEN).

249. L'information doit également porter sur l'existence de procédés de collecte automatique de données (cookies) [206] ainsi que des mesures de sécurité garantissant l'authenticité du site, l'intégrité et la confidentialité des informations transmises sur le réseau.

250. En droit libanais, les décisions no. 207 et 7548 de la BDL imposent aux banques d'indiquer sur leurs sites électroniques leur numéro d'enregistrement à la BDL ainsi que la date de l'octroi de leurs agréments.

251. En l'absence d'encadrement légal des contrats électroniques, les transactions bancaires en ligne doivent être précédées par la conclusion d'une convention spéciale à ce sujet qui va gouverner la relation virtuelle de la banque et du client. Cette convention contient, entre autres, des clauses relatives à l'acceptation de recevoir des alertes et des messages, à l'obligation d'aviser la banque de toute information requise par cette dernière sous peine de suspendre ou annuler le service en ligne. Le client est aussi tenu d'informer la banque de tout changement concernant son adresse électronique ou numéro de téléphone sous peine d'exonérer la banque de toute responsabilité découlant de tout préjudice à cet égard. La convention peut également contenir une clause d'exonération de la banque du secret bancaire notamment au sujet de l'exécution de cette convention en cas de compte joints.

[206] Les cookies sont des fichiers envoyés sur le disque dur de l'ordinateur des personnes qui visitent un site. Ces fichiers enregistrent des informations quand le visiteur accède au site et lors de ses connexions futures. Le visiteur sera donc, suivi dans sa navigation. L.CARON, Protection des données personnelles sur Internet et enjeux du commerce électronique, in. La galaxie Internet, Paris, UNICOMM, 1998, p. 159.
[207]Décision Intermédiaire no. 11445 du 6 juin 2016

Paragraphe 2 : Sécurisation du nom du domaine

252. Le titulaire d'un nom de domaine n'en est pas réellement propriétaire. Pratiquement, le nom de domaine est loué et réservé auprès d'un registre. La réservation du nom de domaine est libre et la bonne foi du titulaire présumée. Des contrôles aléatoires sont effectués et le registre réclame alors une preuve de la légitimité du dépôt du nom de domaine. Si le titulaire n'est pas en mesure d'en fournir, le registre peut alors désactiver son nom de domaine avant même la date d'expiration prévue.

253. Nous allons étudier la sécurisation juridique du nom de domaine (A) avant d'en envisager l'aspect technique (B).

A- Approche juridique

254. En vue de protéger son nom du domaine, la banque doit, a priori, l'enregistrer auprès de l'autorité compétente (en France l'« Association Française des Entreprisses d'Investissement » (AFNIC)[208] et au Liban, « *Lebanese Domain Registry* » (LBDR)[209]).

255. Le problème principal concernant les noms de domaine réside dans l'absence d'investigations lors de son enregistrement, la règle étant « premier arrivé, premier servi ». D'où la possibilité d'enregistrer le nom de domaine d'autrui. En France, comme au Liban, la protection du nom de domaine est renforcée du fait de l'exigence préalable de déposer le nom de domaine comme une marque[210], ce qui implique des mesures légales protectrices contraignantes.

[208]Association Française des Entreprisses d'Investissement, La fourniture de services et de produits financiers à l'épreuve d'Internet : Quel environnement juridique pour les prestataires de services d'investissements ?, Rapport d'un groupe de travail constitué par le Comité juridique de l'AFEI, Octobre 2000, p.22-23.

[209]Ce registre est institué au sein de l'Université Américaine de Beyrouth (AUB) : www.aub.edu.lb/lbdr

[210] Au Liban: l'enregistrement des marques se fait auprès du bureau de protection de la propriété intellectuelle au sein du Ministère du Commerce et de l'Economie. En France, l'autorité chargée de l'enregistrement des marques c'est l'Institut National de la Propriété Industrielle (INPI).

256. Le nom du domaine n'est pas protégé par des dispositions légales spéciales alors que cela s'avère être une nécessité du fait que les noms des domaines constituent un bien de valeur pour les entreprises et toute usurpation ou imitation de ce nom de domaine peut causer des dommages considérables[211]. Dans cette absence de droit spécifique, la protection du nom du domaine peut se fonder sur le droit commun notamment sur les notions d'abus de droit, contrefaçon de marques, ou même concurrence déloyale.

257. En outre, la banque doit sécuriser techniquement le nom de domaine par le biais de mesures prudentielles. En effet, la banque qui connecte son infrastructure informatique sur internet doit disposer d'une politique de sécurité adéquate pour atteindre les objectifs de sécurisation, assurer l'organisation au sein de la banque et prévenir les utilisations malveillantes de cette infrastructure.

B- Approche technique

258. Certains protocoles techniques ont été créés en vue d'assurer la sécurisation des transactions en ligne. Il s'agit tout d'abord de la technique de cryptage des données « *Secure Socket Layer* » (SSL) dont la banque a recours pour protéger ses connexions avec ses clients en assurant le transport de ces données sous forme illisibles ou du moins incompréhensibles au public.

259. Il y a en outre le « *Transport Layer Security* (TLS)[212] qui est le protocole de sécurisation des échanges sur internet le plus répandu et implémenté par un grand nombre de banques et de sites de commerce électronique dans le but de protéger les transactions de leurs clients. Le TLS peut être considéré comme une garantie de résistance aux attaques malveillantes puisqu'il créé un canal sécurisé entre deux machines communiquant sur internet ou sur réseau interne. Ce protocole n'utilise pas la puce de la carte bancaire, mais

[211] Notons que la résolution des litiges relatifs au nom du domaine est possible en ligne. L'organisme international « *Internet Cooperation for Assigned Names and Numeric Internic* » (ICANN) a établi un recours automatique à l'arbitrage.

[212] Le TLS est venu remplacer le « *Secure Socket Layer* (SSL)», en 2001 suite au rachat du brevet de Netscape par l'IETF (Internet Engineering Task Force).

crypte son numéro ce qui permet à la fois de garantir une session chiffrée, de préserver la confidentialité et l'intégrité des données échangées, et d'assurer à la fois l'authentification du serveur et du client. Ce protocole se base sur un certificat électronique fondé sur un procédé cryptographique à clé publique.

260. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui a publié un document intitulé « la bonne utilisation des protocoles SSL/TLS »[213], le protocole TLS est constitué de deux sous protocoles[214] « *le protocole TLS Record qui a pour but de chiffrer les connexions avec un algorithme symétrique et de vérifier leur intégrité* » et *« le protocole TLS Handshake qui a pour fonction d'identifier les deux parties, de leur permettre de négocier les algorithmes et les clés de session utilisées par le protocole TLS Record et de remonter des alertes »*.

261. Ce système a, toutefois, des faiblesses notamment au niveau du stockage des informations. Par exemple, au cas où le site n'est pas correctement protégé (par le biais des « firewalls »), rien n'empêche un pirate d'accéder aux numéros des cartes qui y sont stockées et de s'en servir. Certaines banques utilisent l'algorithme RSA (*Secure Server Certification Authority*) pour sécuriser leurs sessions, par le biais du protocole SSL développé par Netscape. Ce protocole est aujourd'hui utilisé par la plupart des sites sécurisés, du fait de sa souplesse et de sa compatibilité avec la plupart des navigateurs web. Il emploie une clé de cryptage de 40 bits pour les transactions et 128 bits pour le cryptage du certificat. Ce qui souligne un degré de sécurité assez suffisant par rapport au flux des informations qui transitent sur le réseau[215].

262. Avec un système SSL, la sécurité a été sensiblement améliorée et les risques pour le client grandement réduits, comparés à l'époque où le paiement par internet était encore une technologie émergente, bien que, comme tout système de chiffrement, le SSL/TLS ne pourra jamais être totalement infaillible.

---

[213] Document émis par le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques (CERTA) n° 2005-REC-001 du 1er mars 2005 : http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001/

[214] http://www.certa.ssi.gouv.fr/site/CERTA-2005-REC-001/

[215] Cas de Firefox sur d'anciennes versions.

263. Pratiquement, l'internaute peut reconnaître qu'une transaction est chiffrée selon plusieurs indications soit l'URL dans la barre d'adresse commence par la présence d'un « s » dans « https » et non « http » (https://...) ; soit affichage d'une clé ou d'un cadenas, dont l'emplacement varie selon le navigateur généralement à gauche de la barre d'adresse mais aussi dans la barre inférieure de la fenêtre. Les navigateurs peuvent ajouter d'autres signes, comme le passage en jaune de la barre d'adresse du navigateur.

264. Le troisième protocole c'est le « *Chip-Secure Electronic Transaction* (C-SET) » qui a pour objectif d'assurer les paiements sur internet en s'appuyant sur le standard SET avec utilisation d'un logiciel de lecteur de carte bancaire à puce. Le client doit donc être équipé d'un lecteur de carte sécurisé.

265. Les protocoles de chiffrement constituent un mécanisme qui repose sur une grande complexité calculatoire, qui rend en principe impossible la déduction de la clé privée à partir de la clé publique, mais cette impossibilité est limitée dans le temps. Un code aussi compliqué soit-il, finit par être cassé, déchiffré, ce qui augmente le risque de son interception et partant de là le décodage du message et le détournement des informations. Néanmoins, le recours à ces protocoles reste recommandé pour renforcer la confidentialité, l'intégrité et l'authentification des données et transactions.

266. Après avoir limité l'exercice de l'activité bancaire aux seules entités dotées d'un agreement à ce sujet, nous allons exposer les mesures de sécurisation incombant à la banque en ligne.

Chapitre 2 : Les mesures de sécurisation incombant à la banque

267. Le Comité de Bâle[216] a proposé plusieurs mesures indispensables pour prévenir, détecter et encadrer les fraudes en ligne dans le but de les réduire et par conséquent limiter les risques opérationnels des banques. Il s'agit entre autre de pare-feu, mots de passe, technique de cryptage avec une évaluation permanente du niveau effectif de sécurité des systèmes informatiques et la mise en place d'une politique de communication pour sensibiliser les clients aux enjeux de la sécurité.

268. D'où, nous estimons qu'une unité de risque soit instaurée dans toute banque opérant en ligne, spécialisée en termes de technicité et de législations. Cette unité sera responsable de prévenir les risques et menaces en ligne vu que la banque ayant des dysfonctionnements et problèmes techniques se trouve parfois en déni de service ce qui cause des dommages à la fois à la banque et aux clients. Cela engendre une atteinte à sa réputation, une crise de confiance, et lui cause une perte de crédibilité non seulement au niveau des clients, mais aussi au niveau du public et de ses concurrents.

269. Cette unité est recommandée également au niveau étatique. La Commission européenne, consciente de la vulnérabilité des systèmes et moyens de sécurisation a créé une agence chargée de la sécurisation des réseaux et de l'information. C'est la « ENISA [217]» qui a pour mission de fournir une assistance et des conseils sur la mise en œuvre technique et organisationnelle des exigences de sécurité issues des différentes règlementations en la matière. Nous considérons qu'une telle agence a un rôle pionnier dans le succès et la sécurisation du secteur bancaire en ligne. D'où la nécessité d'instituer une agence similaire au Liban.

[216] Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, op.cit.
[217] *European Union Agency for Network and Information Security* (en français Agence Européenne chargée de la sécurité des réseaux et de l'information) instituée par le Règlement Communautaire no. 460/2004 du 10 mars 2004.

270. En vue de protéger les transactions en ligne, plusieurs obligations incombent à la charge de la banque en ligne. Nous allons traiter deux obligations majeures et principales à savoir l'obligation de sécurité (Section 1) et l'obligation de remboursement (Section 2).

Section 1 : Les mesures internes de sécurité, contrôle et sécurité des systèmes informatiques

271. Le banquier est généralement tenu d'une obligation de sécurité qui devient plus délicate quand il s'agit d'opérations sur internet. Cette obligation se manifeste par un devoir de ne pas exposer sa clientèle à un quelconque danger[218] sauf si le danger est causé par un fait externe[219].

272. En matière de transactions bancaires en ligne, l'obligation de sécurité concerne également les systèmes mis en place par la banque (art. 321-67 du règlement général de l'AMF). La banque est tenue de contrôler le système adopté et de prendre toutes mesures pour éviter d'exposer ses clients à des risques causés par ce système à l'exception du cas où le client bien informé du risque accepte de l'encourir. Dans ce cas, la banque se trouve exonérée[220].

273. La banque opérant en ligne est tenue de prendre des mesures internes de sécurité (Paragraphe 1) auxquelles s'ajoute une obligation de confidentialité (Paragraphe 2).

Paragraphe 1 : Les mesures internes de sécurité

274. La banque offrant des services sur internet est tenue de prendre des mesures de sécurité adaptées pour garantir la sécurité et la continuité de son infrastructure et système informatiques, l'intégrité et la confidentialité de ses données financières, des données de ses clients, l'authentification de leur origine, mais aussi faire face à tous les abus et risques pouvant émaner de l'internet.

---

[218] CA Rouen, 16 janv. 1979, JCP E 1981, II, 13506, no. 16. Les juges ont décidé que la banque était responsable mais responsabilité partagée du fait que la cliente avait pénétré dans la salle des coffres bien que le personnel l'avait averti de l'heure tardive, et qui a été enfermé.

[219] CA Paris, 4 mars 1987, D.1987, p. 288, obs. Vasseur. CA Paris 13 Nov. 1992, JCP 1993, pan. 177, I, 301 obs. Gavalda et Stoufflet.

[220] Cass. Com., 2 dec. 1980, no 79-11.231, Bull. Civ. IV, no. 400.

275. D'où l'unanimité des banques instaure un département spécialisé pour la sécurisation de l'infrastructure informatique « IT Département[221] ». Ce département est responsable entre autres du suivi et traitement des menaces internet et leur examen à la lumière des mesures de sécurité et technologies adoptées (logiciel, matériel, langages de programmation, cryptographie, etc.), de la réalisation périodique d'examens spécialisés en matière de sécurité. Il assure également un cadre de filtrage pour l'échange de courriels et d'autres fichiers et messages avec l'extérieur. Il veille à l'archivage, l'analyse et le suivi des fichiers historiques d'événements (logs) techniques adaptés et avertit des risques potentiels.

276. En outre, la banque emploie à cet égard des liens contrôlés entre l'internet et l'infrastructure informatique propre, telles que des *firewalls*, des *proxys servers*, des *mail-relays*, des scanners antivirus et des scanners de contenu, ou d'autres solutions de sécurité similaires. Ces liens doivent être correctement conçus, configurés et sécurisés. La banque est par ailleurs particulièrement attentive à la prévention des liaisons réseaux non contrôlées et insuffisamment protégées avec l'extérieur (réseaux sans fil, *modems, back doors*, etc).

277. En cas de dysfonctionnement du système de réception d'ordres, la banque est tenue d'informer les utilisateurs de la nature et de la durée prévisible de cette panne des systèmes informatiques et d'avoir un système de secours ou des modes alternatifs tels le téléphone ou la télécopie. Également, la banque doit avoir un personnel disponible pour réparer dans les brefs délais les incidents des systèmes informatiques.

278. Au Liban, la BDL s'est contentée, dans sa décision no. 7548 de lister les obligations sans entrer dans les détails de technicité et sans imposer aux prestataires un système de sécurité déterminé. De même, les banques doivent remettre à la Direction des Marchés de la BDL ainsi qu'à la Commission de Contrôle des Banques, tout amendement apporté aux règlements de leurs activités et les règles techniques qu'elles suivent pour exécuter les opérations électroniques.

[221] IT = *Department of Information Technology*

279. Notons que la banque renforce de plus en plus ses modes de sécurisation pour combler toute faille. Cependant, l'intervention de la banque est normalement a posteriori. Une fois la menace détectée, la banque fait ses investigations, détecte les causes de cette menace et prend les mesures adéquates pour contrer les futurs préjudices.

280. En tout état de cause, cette obligation de sécurité est une obligation de moyens[222]. Par conséquent, il incombe au client de prouver le non-respect de cette obligation par la banque. Ainsi, il pourrait être reproché à la banque sa négligence et cette dernière sera jugée en comparaison à ce qu'une autre banque, se trouvant dans les mêmes circonstances, aurait fait.

281. Ainsi, une banque américaine[223] a été condamnée à payer 800,000 dollars pour ne pas avoir mis en œuvre des mesures de sécurité adaptées. Ce procès faisait suite à la demande de remboursement de fonds non recouvrés au motif que le vol était survenu à cause d'un manquement de la banque, qui, selon ce client, n'avait pas de mesures de sécurité adaptées. Il s'agit certes d'une réaction inhabituelle face à un incident de faille de données, mais il montre bien l'importance de la sécurité et de la responsabilité dans le secteur des services financiers.

282. Le demandeur insistait que la banque avait une infrastructure informatique très faible à laquelle s'ajoute l'inadvertance et le défaut de vigilance de la part de la banque. Celle-ci n'a pas réagi après avoir noté plusieurs indices mettant en œuvre une activité frauduleuse tels que des dizaines de transferts ont été effectués durant une très courte période (deux ou trois jours), avec des montants en dehors de la marge habituelle des transferts initiés par le client. De ces faits relatés, nous constatons une vraie réticence de la part de la banque, ce qui justifie les dommages et intérêts auxquels elle a été jugée.

[222] Routier (R), Obligations et Responsabilités du banquier, 2005, p. 108, no. 221-11
[223]http://www.computerworld.com/s/article/9149218/Bank_sues_victim_of_800_000_cybertheft

283. Dans ce contexte, un numéro de carte bancaire saisi ou stocké à l'occasion d'une transaction en ligne doit être rigoureusement sécurisé par le site de la banque, en respectant les dispositions de la délibération de la CNIL du 19 juin 2003[224] sur ce point. Le non-respect de cette obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300,000 euros d'amende[225].

284. Lesdites sanctions, bien que justifiées, sont selon notre opinion exagérées. Une sanction proportionnelle aux pertes subies et manque à gagner seront équitables. Toutefois, le législateur a poussé le plafond des sanctions pour freiner tout abus ou réticence à ce sujet.

Paragraphe 2 : La possibilité du recours contre le fournisseur d'accès à internet

285. Les opérations sur internet impliquent une multitude d'acteurs derrière les coulisses qui contribuent à la réalisation d'une même transaction. Ces acteurs intermédiaires sont l'opérateur de télécommunications[226], les fournisseurs d'accès (FAI ou « *Internet Access Providers* »), les fournisseurs d'hébergement, les fournisseurs de services d'informations/ de contenu ou éditeurs.

286. L'obligation principale du fournisseur d'accès[227] consiste à rendre disponible d'une façon continue (24/7) l'accès à son centre serveur sans interruption. Cette obligation étant

[224] Délibération n° 03-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance.

[225] Article 226-17 du code pénal modifié par l'article 14 de la loi n°2204-801 du 6 août 2004 sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JO du 7 août 2004.

[226] Ce sont les sociétés de services du secteur public ou privé qui exploitent un réseau de télécommunications ouvert au public. L'opérateur peut être propriétaire de la structure physique du réseau ou en louer l'usage à un autre opérateur ou autre personne. Lamy Droit de L'Informatique et des Réseaux, éd 2007, no. 4248 p. 643

[227] Les activités du fournisseur d'accès sont énumérées à l'article 12 al2 de la DCE 2000 : le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission. Le rôle du fournisseur se limite à permettre l'accès au serveur et ne s'étend point au contenu de ce serveur et réseaux y référant. Par exemple, le serveur de messagerie reçoit les emails et les renvoie aux boites électroniques des destinataires.

une obligation de résultat[228], la seule défaillance de la part du fournisseur engage sa responsabilité[229].

287. Le fournisseur d'accès est également responsable de la suspension de ses services sans préavis. La cour d'appel française[230] a jugé que le prestataire de services qui s'engage à permettre un accès illimité à l'internet, ne peut pas interrompre arbitrairement, quelles que soient les raisons même techniques, l'accès au réseau à l'issue d'une certaine période de communication.

288. Les autres obligations du fournisseur notamment le taux et la vitesse de transfert des informations circulant à partir de son centre serveur restent plus légères et sont considérées comme étant des obligations de moyen et ce lorsque les performances du réseau ne dépendent pas de lui. Cependant les parties au contrat peuvent en décider autrement. En d'autres termes, ces obligations secondaires peuvent être conçues comme nécessaires et primordiales ce qui les rendent au rang d'obligation de résultat. Ainsi le fournisseur d'accès, ne respectant pas la vitesse de transmission indiquée dans sa publicité, fut condamné à des dommages et intérêts ainsi qu'à rétablir la vitesse initialement prévue.[231]

289. Le fournisseur annexe généralement la Netiquette[232] aux contrats d'abonnement pour la rendre applicable aux clients qui, normalement consentent à la respecter lors de la conclusion de leurs contrats d'abonnement. Le non-respect de ce code peut entrainer la suspension ou coupure du compte[233].

---

[228] TGI Paris, 5 avr. 2005, UFC Que chisir c/ Tiscali.

[229] T.com. Paris, 23 mars 2000, ISA c/Omniséquence, Expertises 2000 p. 355

[230] C. Appel Versailles, 14 mars 2001, Ste AOL Bertelsmann Online France, Gaz Pal. 2002, 1, somm. P.261.

[231] TGI Paris, 19 oct. 2004, Assoc. Les utilisateurs du cybercable, Comm. Com. Électr. 2005, no.9, note L. Grynbaum.

[232] La nétiquette est une charte qui définit les règles de conduite et de politesse recommandées sur les médias de communication mis à disposition par Internet. Il s'agit de tentatives de formalisation d'un certain contrat social pour l'Internet. S'il ne fallait retenir qu'une seule règle : ce que vous ne feriez pas lors d'une conversation réelle face à votre correspondant, ne prenez pas l'Internet comme bouclier pour le faire. À cette notion de courtoisie et de respect de l'autre viennent ensuite se greffer des règles supplémentaires relatives aux spécificités de plusieurs médias.

[233] La première décision française à reconnaitre la légitimité d'une coupure de compte sur la base de la netiquette a été rendue en 2001 par le TGI Rochefort-sur –Mer et puis par le TGI Paris en 2002.

290. Les contrats d'abonnement avec le fournisseur contiennent communément une clause de non responsabilité quant au contenu des communications[234]. Cela va de la nature du rôle du fournisseur qui se limite à fournir uniquement le transfert des informations puisqu'il est quasiment impossible de mettre à la charge du fournisseur une obligation de contrôle vu le nombre des informations circulant. Cependant cette exonération de responsabilité est soumise à trois conditions cumulatives à savoir que le prestataire n'est pas à l'origine de la transmission, ne sélectionne pas le destinataire de la transmission et ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission (art.12 DCE 2000/31/CE et art. 6 de la LCEN) [235].

291. Toutefois, cette exemption de responsabilité n'empêche « *pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation* » (art. 12 al3).

292. Concernant la nature juridique du contrat de fourniture de ce service, celle-ci a suscité des discussions doctrinales. Pour certains, comme son nom l'indique, c'est un contrat de fourniture de services, donc un contrat d'entreprise. Cependant la fourniture de ce service est dans la majorité des cas gratuite, ce qui affaiblit l'adoption de la catégorie de contrat d'entreprise, ce dernier se caractérisant par son caractère onéreux (art. 1710 CCiv. et 624 COC).

[234] Cette position a été illustrée notamment par un arrêt de la Cour d'appel de Lyon du 22 juin 2000 qui a jugé que « *France Télécom qui assure le fonctionnement du réseau par lequel sont diffusées les informations auprès des clients n'est pas tenue d'exercer un contrôle sur le contenu des messages transmis* » CA. Pau., 14 oct. 1999, France Telecom, JCP E 2000, p. 873.

[235] Aux Etats Unis (Digital Millenium Copyright Act américain du 28 octobre 1998), en Europe (directive 2000/31 du 8 juin 2000) et en France (LCEN), le régime de responsabilité consiste en une limitation de responsabilité du fournisseur d'accès à internet puisqu'il n'est pas soumis à une obligation de surveiller les informations qu'il transmet ou stocke, ni à l'obligation générale de rechercher des faits ou des circonstances révélant des activités illicites (art. 6 I,7 de la LCEN). De même, il n'est donc tenu à aucune action positive de contrôle ou d'enquête, ni à l'obligation de filtrer préventivement les informations » (Directive 2000).

293. D'autres le considèrent comme un contrat de transport puisqu'il s'agit de transport d'informations. Mais le contrat de transport implique le transport de choses matérielles ou de personnes. Par conséquent, inclure les informations et la *res electronica* parmi les éléments matériels transportables semble logique mais métaphorique. Il nous semble difficile d'appliquer le contrat de transport sur les transactions en ligne vu les caractéristiques virtuelles des choses, des moyens de transport et des transporteurs.

294. M. LE TOURNEAU opte pour la qualification de « *location d'un espace disque* »[236], le client bénéficiant d'un droit d'usage intermittent d'un réseau pour parvenir à un serveur, par abonnement, comme c'est le cas du téléphone ou la télécopie.

295. Nous considérons que ce contrat est tellement original qu'il ne peut se voir libellé par une des étiquettes ou appellations relatives aux catégories de contrats nommés traditionnels. Par conséquent, selon notre avis, il s'agit d'un contrat sui generis qui implique une nouvelle nature juridique qui lui octroie un aspect adéquat vu l'immatérialité de l'objet, du contrat et de son exécution.

Paragraphe 2 : Les mesures externes de sécurisation

296. La cryptologie a le mérite de satisfaire aux objectifs de sécurisation des transactions bancaires en ligne à savoir l'authentification des interlocuteurs, la confidentialité des données échangées (ces dernières sont transmises avec un haut degré de sécurité, seules les personnes autorisées y ont accès grâce à une session chiffrée rendant la communication incompréhensible), l'intégrité des données échangées (assurer que les données envoyées d'un côté sont bien celles qui sont reçues de l'autre côté sans modification ou altération), et la non répudiation (garantie que le client ne puisse nier être l'auteur de la transaction)[237]. S'ajoute à ces objectifs, le rôle essentiel de cette technique qui est de constituer une preuve

[236] Le Tourneau, Philippe « Contrats Informatiques et Electroniques », Dalloz Ed. 2006, p. 295

[237] C'est le cas du protocole SSL qui est le plus utilisé à l'heure actuelle dans le monde. En France le protocole Etebac permet d'assurer cette fonction de non-répudiation. Il est principalement utilisé pour les relations banque-entreprises. Pour les relations banque-particuliers, la solution Cyber-Comm permet d'assurer la non-répudiation des paiements par cartes bancaires sur internet par l'adjonction d'un lecteur sécurisé de cartes à puces à l'ordinateur individuel.

notamment l'identification de l'auteur émetteur des messages ou ordres et certifier le contenu des transactions et la signature électronique de l'auteur.

A- Le recours a la cryptologie comme procédé de sécurisation des transactions bancaires en ligne

297. La cryptologie [238] ou écriture secrète [239] est l'un des éléments fondamentaux de sécurisation pour la banque en ligne. Elle consiste en la transformation de données lisibles dans une forme illisible pour la personne qui ne détient pas la clé de décryptage. Ainsi les transactions sont protégées grâce à un code secret qui assure leur transmission d'un ordinateur à un autre et de garantir la confidentialité en utilisant des algorithmes, à l'aide de clés ou de mots de passe qui sont détenus par les utilisateurs pour coder et décoder les documents.

298. Cette technique est adoptée jusqu'à nos jours dans les domaines militaire, diplomatique, et fut, pour longtemps, exclusivement réservée aux données sensibles de haut niveau échangées (défense nationale, gouvernements, armées, services secrets) avec un monopole étatique[240].

[238] La cryptologie, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie — l'écriture secrète – et la cryptanalyse – l'analyse de cette dernière.
Le cryptage du message passe par une procédure particulièrement complexe. En premier lieu, le message encodé est condensé grâce au mécanisme du hachage qui lui confère une empreinte numérique. Une fois signé à l'aide de la clé privée, et condensé par l'expéditeur, le message est en second lieu envoyé à son destinataire qui le décode grâce à la clé publique. Si, à la comparaison, les deux messages condensés sont identiques, on peut affirmer dans ce cas que la signature électronique a bien rempli son rôle, et que le message n'a pas été altéré ou détourné lors de sa transmission.

[239] Certains comparent la cryptologie à la sténographie qui consiste à dissimuler dissimulation : son objet est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit, Johnson NF, Seganography : http://www.jjtc.com/Steganography/

[240] La loi n°90/1170 du 29 décembre 1990 sur la réglementation des télécommunications a prévu initialement l'utilisation des moyens cryptographiques dans le but de « préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, tout en permettant la protection des informations et le développement des transactions sécurisées » (article 28 de la loi du 29 décembre 1990).

299. Elle a été jugée indispensable pour la sécurisation et la confidentialité des transmissions en ligne des données bancaires sensibles, ce qui a poussé le législateur[241] à accorder, dans un premier temps et sous conditions restrictives[242], la possibilité de recourir à cette science secrète pour finir par la libéraliser complètement[243].

300. Depuis cette libéralisation, aussi bien les personnes physiques, les entreprises que les banques peuvent avoir recours aux moyens de cryptologie qui sont définis comme étant « *tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité* ».

301. D'ailleurs la fourniture des prestations de cryptologie[244] est rigoureusement encadrée par la LCEN et elle requiert une déclaration auprès du premier ministre (Art. 31, I LCEN). Les prestataires qui assurent cette fourniture sont assujettis au secret professionnel dans les conditions prévues aux articles 226-13 et 226-14 du code pénal et art 31 II de la LCEN, et sont responsables au titre de ces prestations *«nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions*»[245].

---

[241] La loi n°96-659 du 2 juillet 1996 est venue ensuite « semi libéraliser » le secteur de la cryptologie, en modifiant sensiblement la loi du 29 décembre 1990 par l'instauration de trois régimes : la liberté, l'autorisation préalable et la déclaration. Ces deux derniers régimes, selon l'article 28,3° de la loi du 29 décembre 1990 modifiée, sont définis par décret en particulier, les décrets n° 98-101 du 24 février 1998 et n°98-102 du 24 février 1998, n°99-199 du 17 mars 1999 et n° 99-200 du 17 mars 1999.

[242] Sont soumis à autorisation préalable du premier ministre, la fourniture, l'importation de pays n'appartenant pas à la Communauté européenne, et l'exportation aussi bien des moyens que des prestations de cryptologie lorsqu'ils assurent des fonctions de confidentialité. (Art. 28, 2°, a de la loi du 29 décembre 1990). Pour tous les autres cas, une simple déclaration au premier ministre suffit (art. 28, 2°, b).

[243] LCEN : titre III intitulé « De la sécurité dans l'économie numérique ».

[244] Par prestation de cryptologie on entend « *« toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie* ». Article 29 alinéa 2 de la LCEN.

[245] Article 32 de la LCEN.

302. Nous concluons que ces restrictions législatives et cette responsabilité renforcée à la charge des prestataires de service de cryptologie sous peine de sanctions administratives et pénales prévues aux articles 34 et 35. Ce qui consolide le recours à la cryptologie restrictivement pour des fins de sécurisation et souligne une lutte contre l'utilisation de la cryptologie à des fins délictueuses[246].

303. En effet, vu son mécanisme et sa complexité en algorithme et calcul, la cryptologie assure une sécurisation qui rend en principe impossible la déduction de la clé privée à partir de la clé publique, néanmoins cette impossibilité est limitée dans le temps. En fait, les hacheurs de code (*hackers*) trouveront tôt ou tard le moyen de cassé, déchiffré même le code le plus compliquée, ce qui lui ouvre la porte au détournement des informations.

304. La cryptologie à travers ses deux volets (symétrique et asymétrique)[247], est largement utilisée pour sécuriser aussi bien les sites des entreprises que ceux des banques. En effet, plusieurs protocoles de sécurité se sont succédés à travers les années afin d'assurer le chiffrement des données sensibles qui peuvent circuler en ligne en particulier les données personnelles et financières qui sont fournies lors des paiements sur Internet.

[246] ABI RIZK G.D., L'Internet au service des opérations bancaires et financières, opt.cit. p 101.

[247] Il existe deux principaux types de protocoles de sécurisation des sites bancaires à savoir la cryptologie symétrique et la cryptologie asymétrique.
La cryptologie symétrique se base sur une seule clé secrète que l'émetteur et le destinataire d'un message détiennent, aussi bien pour chiffrer le message que pour le déchiffrer.
La cryptographie est dite asymétrique ou à « clé publique » lorsque les algorithmes de cryptage et de décryptage sont différents. Le mécanisme repose sur un algorithme dit RSA. Cet algorithme est fondé sur deux clés distinctes mais complémentaires: l'une est publique (eut être connue de tous les utilisateurs en raison de sa publication dans un annuaire) pour chiffrer et l'autre est privée (gardée secrète, et ne peut être connue que par son détenteur) pour déchiffrer les données confidentielles échangées. La cryptographie asymétrique permet à la fois d'assurer un envoi sécurisé des messages et réaliser des signatures électroniques dites cryptographiques.

B- D'autres techniques de sécurisation de paiements en ligne comme nouvelles opportunités pour la banque en ligne

305. Devant la recrudescence des fraudes en ligne liée à l'utilisation de la carte bancaire, deux services de sécurisation du paiement en ligne protégés par des procédés cryptologiques ont vu le jour. Il y a d'une part le service 3D Secure qui repose sur une authentification renforcée du titulaire de la carte bancaire et le service e-carte bleue qui évite la communication en ligne du numéro de la carte bancaire.

1- Le service 3D Secure

306. Dans le cadre du renforcement de de sécurisation des paiements en ligne[248], et dans la lutte contre l'utilisation frauduleuse de numéros de carte de paiement sur internet (notamment par usurpation d'identité), Visa et MasterCard ont mis en place depuis 2001 le système 3D Secure[249]. Il s'agit d'un protocole sécurisé de paiement sur internet gratuit qui assure l'authentification du véritable titulaire de la carte bancaire par le moyen de certificats électroniques.

[248] Cette sécurisation sera plus établie avec l'émergence de l'Europe des paiements unifiée (SEPA = Single Euro Payment Euro).

[249] L'activation du système 3D Secure se fait lors du premier achat sur le site d'un commerçant 3D Secure en France ou à l'étranger qui affiche le logo *« Verified by Visa »* ou *« Mastercard Secure Code »*. L'opération d'authentification consiste à saisir le numéro de la carte bancaire[249] , et du numéro de téléphone mobile, et créer un mot de passe. Ensuite, il convient ensuite de répondre aux questions obligatoires postées pour achever la phase d'enregistrement. A chaque transaction 3D Secure, la fenêtre 3D Secure affiche les 4 derniers chiffres du numéro de téléphone saisi auparavant et envoie le code d'authentification à usage unique par texte téléphonique ou sms.
Il suffit ensuite d'insérer ce code dans la fenêtre 3D Secure à l'endroit indiqué afin d'achever la transaction. Par mesure de sécurité, en cas de saisie erronée du code à usage unique, le paiement en ligne ne peut avoir lieu. Dans certaines situations, il arrive que la personne qui souhaite effectuer un paiement en ligne ne reçoive pas le code à usage unique, dans ce cas, elle doit cliquer sur un lien qui s'affiche sur l'écran « je n'ai pas reçu mon code » afin de pouvoir s'authentifier via le mot de passe saisi lors de l'enregistrement au service 3D Secure pour continuer la transaction. Si dans le cas extrême, l'authentification échoue en raison du non envoi du code à usage unique et de l'absence d'affichage du lien précité, la transaction sera abandonnée sur le site du commerçant 3D Secure.

307. Ce mécanisme d'authentification recommandé par l'Observatoire de la sécurité des cartes de paiement a recommandé, dans son rapport de 2010[250], et par le Gouverneur de la Banque de France en juin 2010[251], est de nos jours adopté non seulement la majorité des banques françaises mais aussi une grande partie des e-commerçants[252]. Il s'inscrit dans un processus de paiements en ligne déjà actif en Europe.

308. Le service 3D Secure garantit une grande sécurité juridique contre les transactions déloyales (par utilisation frauduleuse de la carte bancaire) en ligne car le système d'authentification obligatoire renforce la confiance des internautes au niveau du paiement en ligne et d'un autre coté protège les e-commerçants contre les risques d'impayés pour contestations des acheteurs, puisqu'il réalise un transfert de la responsabilité financière vers les banques de ces derniers.

309. Toutefois, le risque de cette technique réside dans le cas de détention illégitime de la carte bancaire où le malveillant détourne le numéro de la carte et téléphone mobile, et effectue en toute illégalité une transaction 3D Secure. Cependant cette lacune n'est pas inhérente aux transactions en ligne, elle est également présente pour la carte classique.

2- L'e-carte bleue

310. L'e-carte bleue est un mécanisme envisagé particulièrement dans le but de renforcer la sécurité juridique des transactions bancaires qui ont lieu en ligne et de protéger les cartes bancaires du trafic illégal. Elle permet d'effectuer des paiements à distance (internet ou téléphone) sans la communication du numéro de la carte bancaire réelle. La sécurité est assurée par un protocole de chiffrement de données par clé publique (RSA) et par un certificat électronique (*Verisign*). Son utilisation est sécurisée par la saisie d'un mot de passe et d'un identifiant envoyés au titulaire légitime de la carte bancaire.

---

[250] https://www.banque-france.fr/sites/default/files/medias/documents/oscp-rapport-annuel-2010.pdf.

[251] http://www.google.fr/url?sa=t&rct=j&q=3d%20secure%20banque%20de%20france&source=web&cd=2&ved=0CGgQFjAB&url=http%3A%2F%2Fwww.banque-france.fr%2Fobservatoire%2Ftelechar%2Fetat-des-lieux-rapport-annuel-2010-observatoire-securite-cartespaiement-0711.pdf&ei=etkPUJThDMi00QW5_4GoBA&usg=AFQjCNE-WgmlwcDeSoAiOoZs5IZCFtFsnQ.

[252] Les agences de voyages (SNCF, Air France), les opérateurs de la téléphonie mobile (Orange, SFR, Bouygues télécom et Free), etc.

311. Adoptée aujourd'hui par la majorité des banques françaises et libanaises, cette carte consiste en l'octroi d'un numéro de carte virtuel à usage unique utilisable auprès de tous les commerçants qui acceptent le paiement par carte bancaire ou carte bleue VISA pour la durée et le montant que le client détermine au moment de la création de ce numéro. Ce service a donc le mérite de renforcer leur confiance dans le paiement à distance du fait qu'il évite la communication et la circulation du numéro réel de la carte bancaire lors de la conclusion de la transaction en ligne.

312. Les transactions réalisées avec l'e-carte bleue présentent les mêmes garanties, assurances, et règles de gestion que ceux qui peuvent être réalisés avec la carte bancaire réelle. Les transactions apparaissent sur les relevés de compte de la carte bancaire réelle. Il convient donc de garder un historique des paiements qui ont été effectués avec le service e-carte bleue.

313. Toutefois, malgré cette mesure de sécurisation, les cartes bancaires sont les cibles de grands nombres de techniques de piratage notamment le skimming [253] ou piratage de cartes bancaires. Les transactions en ligne restent des transactions à distance dans lesquelles existe l'incertitude d'identifier si c'est le titulaire légitime qui reçoit les identifiants et le mot de passe, et qui les saisit au moment du paiement en ligne. Le code piraté constitue une marchandise de valeur qui sera vendue au plus offrant ou utilisée pour accéder aux comptes des utilisateurs pour des fins de cybercriminalité. Notons d'ailleurs que les mots de passe piratés sur un site utilisé pour des buts de communications est un moyen pour pirater des informations plus importantes et rentables à savoir les adresses bancaires ou autres étant donné que beaucoup de gens utilisent le même identifiant et le même mot de passe pour plusieurs sites.

[253] Le terme *skimming* vient de l'anglais «*to skim*», écrémer. Le *skimming* consiste à dupliquer les coordonnées bancaires stockées sur la bande magnétique des cartes bancaires et code NIP. Grâce à ces informations, le « pirate » créé un clone de la carte bancaire. : les pistes magnétiques de la carte de paiement sont copiées dans un commerce de proximité ou dans des distributeurs automatiques à l'aide d'un lecteur à mémoire. Le cas échéant, le code confidentiel est capturé à l'aide d'une caméra ou par le biais d'un détournement du clavier numérique. Dans certains pays comme les Etats-Unis, la puce électronique (plus sécurisée) n'est pas utilisée pour valider un paiement par carte. La bande magnétique suffit. https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/fraude-a-carte-paiement

Section 2 : Des autres obligations à la charge de la banque

314. En vue de protéger le client internaute, partie faible, le législateur a obligé la banque à sécuriser les transactions en ligne sous peine de rembourser le client.

315. Nous allons relater l'obligation de remboursement à la charge de la banque (Paragraphe 1) pour développer ensuite le secret bancaire en ligne (Paragraphe 2).

Paragraphe 1 : Obligation de remboursement à la charge de la banque

316. L'obligation de sécuriser la transaction se traduit par le remboursement au client des sommes débitées dans tous les cas d'opération non autorisée de sa carte bancaire (en cas de vol, détournement, utilisation frauduleuse), et d'opération mal exécutée à condition que le client n'ait pas commis un agissement frauduleux ou qu'il n'ait pas satisfait intentionnellement ou par négligence grave aux obligations d'assurer la sécurité des dispositifs de sécurité personnalisés. L'établissement jouit d'un délai de soixante-dix jours pour effectuer l'opération et ce délai peut être prorogé à 120 jours (L. 133-18 et s. du Code monétaire et financier).

317. Cependant, l'article L132-4 du Code monétaire et financier dispose que la responsabilité du titulaire d'une carte n'est pas engagée si le paiement contesté a été effectué frauduleusement, à distance, sans utilisation physique de sa carte. De même, sa responsabilité n'est pas engagée en cas de contrefaçon de sa carte au sens de l'article L. 163-4 et si, au moment de l'opération contestée, il était en possession physique de sa carte.

318. Dans les cas prévus, si le titulaire de la carte conteste par écrit avoir effectué un paiement ou un retrait, les sommes contestées lui sont créditées sur son compte par l'émetteur de la carte ou restituées, sans frais, au plus tard dans le délai d'un mois à compter de la réception de la contestation.

319. En effet, le Code monétaire et financier français prévoit que le titulaire de la carte bancaire doit être remboursé s'il n'a pas autorisé l'opération de paiement et ce depuis la loi du 15 novembre 2001, modifiée à plusieurs reprises depuis sa promulgation.

320. En matière de virement électronique, la Cour de cassation a affirmé que les banques sont soumises à une obligation de vérification des ordres de transfert. L'action avait été formée contre la banque réceptionnaire de l'ordre de paiement sur le fondement de la responsabilité délictuelle de l'article 1240 du Code civil, qui suppose que le demandeur démontre une faute et un préjudice ainsi qu'un lien de causalité entre eux. La compagnie d'assurances n'avait pas agi contractuellement contre sa propre banque, qui avait transmis les ordres à la banque de l'employée indélicate, car elle l'estimait sans doute dépourvue de moyens de vérifications adéquats.

321. En matière de carte bancaire, la Cour de cassation[254] a décidé qu' *« en cas de perte ou vol d'une carte bancaire, il appartient à l'émetteur de la carte qui se prévaut d'une faute lourde de son titulaire, au sens de l'article L. 132-3 du code monétaire et financier, d'en rapporter la preuve ; que la circonstance que la carte ait été utilisée par un tiers avec composition du code confidentiel est, à elle seule, insusceptible de constituer la preuve d'une telle faute* ». En d'autres termes, la banque n'était pas en mesure de rapporter la preuve de la faute lourde du titulaire de la carte. Cette solution a été confirmée par la suite, à de nombreuses reprises.

322. Par cinq arrêts rendus le 18 janvier 2017[255], la Cour de cassation française a rappelé qu'un établissement financier doit apporter la preuve qu'un utilisateur d'un moyen de paiement, qui nie avoir effectué un achat, a agi frauduleusement ou a communiqué à un tiers ses données personnelles ou identifiants par sa négligence (phishing)[256], il ne peut pas se baser sur des suppositions pour refuser le remboursement des sommes indûment débitées.

---

[254] Cass. Com., 2 oct 2007
https://www.courdecassation.fr/jurisprudence_2/chambre_commerciale_574/arret_n_10826.html
[255]https://www.legalis.net/actualite/achats-frauduleux-en-ligne-la-banque-doit-prouver-la-faute-de-son-client/
[256] Cass. Civ, Ch. com., arrêt du 18 janvier 2017- Crédit mutuel de Wattignies / M. X. :
https://www.legalis.net/jurisprudences/cour-de-cassation-civile-ch-com-arret-du-18-janvier-2017/.

323. La Cour de cassation a statué que les tribunaux de première instance avaient justement accueilli les demandes de remboursement, faute pour la banque d'avoir apporté la preuve d'une fraude ou d'une négligence de ses clients.

324. Le client internaute est surtout protégé par le biais des délais d'exécution entre le moment de la réception de l'ordre de paiement et le crédit sur le compte de la banque du bénéficiaire (art. L. 133-13 du Code monétaire et financier fr.).

325. En droit libanais, l'exécution de la transaction bancaire en ligne est régie, pour les cas non prévus par le code de la monnaie et du crédit, par les dispositions du droit commun notamment le COC. Il serait souhaitable d'avoir une harmonie législative en la matière.

Paragraphe 2 : Secret bancaire requis en ligne

326. Qui dit activité bancaire, dit confidentialité. L'obligation de confidentialité est une condition inhérente à la nature même de l'activité bancaire et un outil de protection du client[257].

327. Comme nous l'avons déjà développé, la banque est tenue de bien connaitre son client. Pour ce, elle obtient des informations de nature confidentielles ou du moins relatives à sa vie privée. Cependant, une fois collectées, les données doivent être conservées minutieusement par la banque comme un bon père de famille et ne doivent pas être utilisées pour des buts autres que pour le besoin des transactions bancaires.

328. La BDL impose le secret bancaire en ligne[258] ainsi les dispositions de la loi du 3 septembre 1956 relative au secret bancaire sont applicables aux transactions bancaires en ligne.

[257] Credot F.J, Le secret bancaire, son étendue et ses limites, la fourniture de renseignements commerciaux par les banques, LPA 17 fev. 1993, p.8 –T. Bonneau, Communication de pièces et secret bancaire, RD bancaire et fin. 1995, p.94. Le secret professionnel est défini par Cabrillac et Mouly comme étant la non révélation par les agents des banques et des établissements financiers des secrets reçus es-qualité, en dehors des hypothèses où la loi le commande ou l'autorise »[257] Cabrillac M. et Mouly, Ch., Masson, Droit Pénal de la Banque et du Crédit, Collection Droit Pénal des Affaires dirigées par M.E. Cartier, 1982, p. 109.

329. Cette loi impose un secret absolu à toute personne en rapport direct ou indirect avec l'activité bancaire, ainsi que toutes les personnes qui ont connaissance, de par leur qualité[259] ou leur fonction[260]. Ainsi, sont soumises au secret bancaire non seulement les banques établies au Liban mais aussi les banques qui sont des agences de sociétés étrangères, et les succursales des banques étrangères au Liban[261].

330. Avec son effet « *ergaomne*s »[262], le secret bancaire s'impose à toutes les personnes qui travaillent au sein de la banque en quelque qualité soit-elle : membres du conseil d'administration [263] , commissaire au gouvernement, commissaire de surveillance, fonctionnaire, employé, ou conseiller (art. 72 tel modifié par le DL n° 8658 du 21 août 1974). Et cette opposabilité du secret bancaire s'étend à la société-mère de la banque, nonobstant la nature de l'activité de la société-mère et même si la société-mère est elle-même une banque[264].

331. La violation par le banquier de son obligation de confidentialité engage sa responsabilité pour le préjudice causé. Les banques sont soumises en cas de violation du secret par un de leurs dirigeants ou leurs employés, à des peines sévères à savoir l'amende

---

[258] Article 5-3-b de la Décision Intermédiaire de la BDL no. 11445 du 6/6/2013 : « *le secret professionnel à tous les établissements non bancaires qui effectuent des opérations de virement de fonds par des moyens électroniques à l'intérieur du Liban, doivent se conformer à ce qui suit…la conservation du secret professionnel et l'endossement, vis à vis des tiers, de toute responsabilité résultant des opérations entreprises par l'établissement ou ses branches ou emplacements / points de services de virements (Points of Electronic Transfers) opérant dans ses agences ou par l'intermédiaire de sous-agents ou de tout établissement avec qui ils ont une relation contractuelle* ».

[259] CA Paris, 20 mars 1990, D. 1992, somm. P.31, obs. M. Vasseur : l'associé n'est pas en qualité de demander la communication d'informations confidentielles.

[260]Beyrouth, 15 déc.1981: Hatem fasc.174 p.504. Bey, 10 nov. 1960, Chamseddine, Droit comm.1985, p. 182.

[261] Le secret bancaire s'étend à la banque de l'Habitat.

[262]SOUMRANI, Solidité du secret bancaire de la loi du 3 septembre 1956, Al Adl 1997, 1.

[263] En droit français, aux termes de l'article L571-4 code monétaire et financier français, les membres du conseil d'administration, même non banquier, sont tenus du secret professionnel sous les peines prévues à l'article 226-13 du code (un an d'emprisonnement et de 15,000 euros d'amende selon l'article 226-13 du code pénal français). De même, l'article L511-33 stipule que « *tout membre d'un conseil d'administration et, selon le cas, d'un conseil de surveillance et toute personne qui, à un titre quelconque, participe à la direction ou à la gestion d'un établissement de crédit, d'une société de financement ou d'un organisme mentionné à l'article L.511-6 ou qui est employée par l'un de ceux-ci est tenu au secret professionnel* ».

[264]CA Paris, 8 oct 1981, D. 1982, IR p. 124, obs. M. Vasseur.

et l'emprisonnement (art. 226-13[265] code pénal français, et art. 8[266] de la loi du 3 Septembre 1956) [267]. Ces peines ne sont applicables qu'en cas de violation intentionnelle.

332. Le banquier peut être aussi sanctionné pour du délit de divulgation d'informations susceptibles de porter atteinte à la réputation des personnes. Les juges ont sanctionné un banquier pour violation du secret bancaire et divulgation d'informations discrètes pour avoir adressé à des commerçants une liste informative de personnes supposées présenter un risque[268].

333. Cependant, le banquier ne doit pas se voir reproché de ne pas avoir renseigné le bénéficiaire du paiement sur les difficultés financières de son client[269].

334. Notons qu'à l'échelle internationale, la loi sur les échanges d'informations fiscales a été édictée récemment en octobre 2017. Le législateur libanais réticent au début pour ne pas troubler le secret bancaire, la pierre angulaire du secteur bancaire libanais, finit par l'adopter. Dorénavant, les banques libanaises ont l'obligation d'identifier les clients qui seront concernés et en septembre 2018 les échanges deviendront automatiques et annuelles.

335. Nous prévoyons que le secret bancaire sera, en quelque sorte, ébranlé en matière de banque en ligne vu les législations anti-blanchiment et celles relatives aux échanges d'information et transparence fiscale.

336. D'autres obligations de nature plutôt pratique et pragmatiques sont requises pour renforcer la sécurisation des transactions bancaire en ligne. Celle-ci serait encore renforcée par la présence d'une protection des droits par voie des juridictions.

---

[265] L'article 226-13 du Code pénal français : "La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende".

[266] La sanction prévue est l'emprisonnement de trois mois à un an.

[267] Le code pénal libanais a prévu le secret professionnel à l'article 579 « Quiconque ayant à raison de son état, de sa fonction, de sa profession ou de son art, connaissance d'un secret, le révélera sans juste motif, ou bien l'utilisera à son profit personnel ou au profit d'un tiers sera puni d'un emprisonnement d'un an au plus et d'une amende ne dépassant pas quatre cent mille livres libanaises si le fait est susceptible de causer un préjudice même moral ».

[268]CA Rennes, 13 janv. 1992, d. 1993, somm. p.54, obs. Vasseur ; JCP E 1993, INTERET, 432, note Gavalda.

[269] CA Lyon, 7 déc. 2001, no 1999/06589, Media Overseas c/Banque Populaire Loire et Lyonnais.

Titre 2 : Sécurisation pratique des transactions bancaires en ligne

337. Les banques ont recours à toutes les techniques possibles pour assurer la sécurisation des transactions faute de quoi elles risquent leur réputation et leur clientèle. D'ailleurs, selon un sondage réalisé en France par Gemalto[270], 44 % des personnes interrogées ont déclaré qu'elles changeraient de banque en cas de violation de la sécurité.

338. Les transactions bancaires en ligne, étant dotées d'un caractère pratique, requièrent en plus de la sécurisation législative et juridique, une certaine vision pratique et des mesures préventives et stratégiques. Ceci étant dit, les acteurs principaux restent la banque et le client internaute qui doivent mettre en œuvre toute mesure afin d'assurer la sécurisation de la transaction bancaire en ligne, en général, et leurs intérêts, en particulier.

339. En outre, le renforcement de la sécurisation se réalise, en dernier lieu, par le recours à la justice au cas de préjudice.

340. Nous allons exposer la sécurisation technique incombant à la charge de la banque en ligne (Chapitre 1) et les obligations incombant à la charge du client internaute (Chapitre 2).

[270] https://www.gemalto.com/france/banque/ebanking/dsp2/authentification-forte-du-client.

Chapitre 1 : Mesures de sécurisation incombant au client internaute

341. Le client internaute contribue également à la sécurisation des transactions bancaires sur internet. Certains devoirs pèsent sur lui tels que la coopération, la transparence, le renseignement, la prudence, la discrétion. Ces devoirs peuvent être classés en deux devoirs principaux à savoir devoir de coopération et devoir de vigilance.

342. Cependant, il faut clarifier que ces devoirs sont plus qualifiés de précautions que d'obligations, le principe restant la responsabilité de plein droit des banques (art. 15.I LCEN). Les seuls cas d'exonération de responsabilité prévus sont la faute du client, le fait imprévisible ou insurmontable du tiers ou le cas de force majeure.

343. Nous allons présenter les deux obligations majeures qui incombent au client internaute, à savoir le devoir de coopération (Section 1) et le devoir de vigilance (Section 2).

Section 1 : Devoir de coopération du client internaute

344. De prime abord, le client internaute s'impliquant dans des transactions bancaires sur internet a un devoir de coopération. Ce devoir n'est pas nouveau puisque dans tout contrat, pèse sur le client une obligation de coopération, particulièrement lorsque son objet est complexe et délicat. Ce devoir est plus vigoureux en présence d'un contrat intuitu personae comme le contrat bancaire qui a trait à l'argent du client. D'ailleurs, le devoir de coopération doit exister durant toute la vie du contrat, et ce dès la genèse du contrat et même lors des pourparlers[271].

345. Le fondement de ce devoir contractuel réside dans la bonne foi qui doit gouverner les rapports contractuels, et qui est pratiquement implicite et d'ordre public. Elle ne serait explicitement stipulée que pour en préciser les modalités, ce qui est nécessaire en présence d'un client non professionnel.

346. En outre, le client internaute est tenu de préciser ses besoins et les objectifs qu'il vise à atteindre de l'opération bancaire requise. Cette obligation de coopération ne doit pas cependant dégénérer en immixtion dans la réalisation de l'opération et dans la compétence. En tout état de cause, le client reste profane et c'est la banque, en tant que professionnel, qui est tenue de résister à certaines demandes et suggestions jugées risquées.

347. Le client internaute doit coopérer avec la banque prestataire de service en ligne et doit être honnête et transparent pour former avec la banque une complicité sécuritaire face aux criminels en ligne.

[271]F. Diesse, l'exigence de la coopération contractuelle dans le commerce international : L'application du devoir de coopération: Le domaine d'application de la coopération contractuelle - Les fondements du devoir de coopération dans le commerce international / Les fonctions de l'exigence de la coopération contractuelle: Un rôle essentiellement interprétatif du contrat - Un rôle subsidiairement normatif.

348. Le client internaute est tenu de consulter les consignes de sécurité publiées par la banque sur son site à propos des opérations bancaires électroniques régulièrement et les respecter à la lettre ce qui permet de protéger son ordinateur et ses informations personnelles contre tout accès non autorisé et garanti en outre une plus grande sécurité en matière d'opérations bancaires électroniques assez délicate.

349. Nous l'avons déjà développé que la banque est tenue d'une obligation d'information de ses clients. Cependant, il faut noter avec M. JOURDAIN [272] que «l'obligation de renseignement ne commence que là où cesse l'obligation de se renseigner soi-même ». Comme corollaire à l'obligation d'information ou de conseil incombant à la charge de la banque, le client est tenu de s'informer, et ce surtout s'il est un client professionnel. Tout bon professionnel doit se renseigner avant de contracter, dans la mesure de ses capacités pour veiller à ses propres intérêts. Nous concluons qu'un client qui se renseigne est un client qui effectue convenablement sa transaction et contribue donc à la sécurisation de celle-ci.

350. Le client internaute doit être habile et réagir intelligemment vis-à-vis de toute tentative d'escroquerie. En cas de doute, le client doit contacter sa banque dans les plus brefs délais pour se renseigner, mais aussi pour alerter la banque de tout ce qu'il considère suspicieux [273] . D'ailleurs, la majorité des banques ont un département de services clientèle « Hotline » disponible pour tous renseignements téléphoniques en cas de mouvements inhabituels.

351. La défaillance du client internaute dans sa tâche de coopération pourra être invoquée par la banque pour se décharger, au moins partiellement, de la responsabilité d'erreurs ou de retards.

[272] Jourdain (P), Le devoir de se renseigner, contribution à l'étude de l'obligation de renseignement, D. 1983, Chronique 139.

[273] C. App. d'Aix-en-Provence 8e Ch. Audience publique du jeudi 15 décembre 2016 N° de RG: 14/12661 (disponible sur Légifrance). La banque a été condamnée à rembourser le client en considérant que le client a dument alerté la banque.

Section 2 : Devoir de vigilance du client internaute

352. Le client internaute doit être prudent dans ses activités bancaires en ligne. Pratiquement, il peut adopter quelques mesures simples qui serviront de précautions effectives. Il doit porter toute l'attention nécessaire a priori et a posteriori de l'accomplissement de sa transaction bancaire. De ce fait, il contribue significativement à la sécurisation.

353. Le client internaute est tenu de conserver ses données confidentielles[274] telles que le mot de passe, le code secret ou NIP et prendre toutes précautions possibles (sachant que les mots de passe peuvent être facilement obtenus par des moyens non sophistiqués tels indiscrétion, devinette, fouille dans corbeille et observation par-dessus l'épaule ou *shoulder-surfing*[275]). Ces données ne doivent pas être divulguées par email ou document susceptible de perte ou vol. Le même code ou mot de passe ne doit pas être le même que pour les autres services en ligne (messagerie, sites social media, etc.) qui sont beaucoup moins sécurisés voire contrôlés pour des buts de hacking. Les experts en informatique conseillent de changer régulièrement le mot de passe et surtout d'adopter un mot de passe compliqué (alphanumérique qui combinent à la fois lettres et chiffres).

354. Le client internaute ne doit pas appuyer sur des liens contenus dans des emails reçus puisque la plupart de ces liens infectent son ordinateur par un logiciel malveillant ou atterrir sur un site d'hameçonnage. Et ultimement, il ne doit pas croire aux messageries lui accordant des cadeaux généreux, de gros lots, un héritage d'une personne décédée sans héritiers, etc. Techniquement, la banque ne demande jamais le NIP au téléphone pour les services de banque en ligne. Seuls des escrocs avec un faux nom d'expéditeur en demanderont par email les données d'accès personnelles.

[274]Article L. 133-16 et 17 du code monétaire et financier français.

[275] En sécurité informatique, regarder par-dessus l'épaule (anglais : *Shoulder surfing*) est une technique d'ingénierie sociale utilisée pour dérober de l'information à une personne. Il existe deux façons de réaliser l'attaque, la première, assez rapprochée, consiste à regarder par-dessus l'épaule de la personne espionnée en tentant d'observer les données qu'elle introduit dans des champs. La seconde, plus éloignée, implique l'utilisation de jumelles ou d'appareils adaptés, tels que des micros ou des caméras-espion. (wikipedia 2018).

355. Le client internaute est tenu d'être prudent en se connectant à son compte bancaire en ligne. Il est recommandé d'utiliser son propre ordinateur (muni d'antivirus efficace) sachant que tout est visible sur un réseau de connexion public, les ordinateurs publics peuvent toujours contenir des enregistreurs de frappe (ou *keyloggers*[276]) et d'autres programmes malveillants[277]. Il est de même préconisé de se déconnecter proprement de son compte sur le site de la banque et encore mieux, d'effacer l'historique après chaque connexion puisqu'en matière d'informatique, le navigateur[278], par défaut, garde en mémoire les données d'accès.

356. Le client internaute doit taper lui-même directement dans son navigateur l'adresse du site web de la banque pour contourner les malwares ou techniques *phising* qui sont capables de rediriger vers un site malveillant qui amènera la victime à entrer à son insu ses identifiants et mots de passe alors que l'internaute se croit connecté au site de sa banque.

357. En outre, lorsqu'il transfère de l'argent, le client internaute doit être prudent en donnant ordre de paiement à sa banque. Il doit bien lire les informations et le contenu de sa demande de transfert et s'assurer de l'adresse email[279] du bénéficiaire demandant le virement.

---

[276] Nommé aussi virus « Cheval de Troie », il s'introduit dans une place et se multiplie et infecte tous les appareils du réseau. Sa mission n'est pas de détruire mais d'ouvrir les portes de la ville pour y faire pénétrer le pirate qui a désormais accès à l'ordinateur dès que son utilisateur se connecte à internet. Le cas échéant, un tel cheval envoie par courrier électronique au pirate les informations et données rencontrées. Pratiquement, le pirate prend le contrôle à distance du système informatique.

[277] Le logiciel espion est téléchargé gratuitement pour camouflage (programme de jeux ou vidéos). Une fois installé sur l'ordinateur de l'internaute, il met en place un programme d'espionnage du clavier ou lance un script de récupération de mot de passe et les codes secrets.

[278] Le virus « Man-in-the-Browser » (MitB) infecte le navigateur web de l'internaute en modifiant et interceptant les données transmises par l'internaute avant qu'elles ne parviennent au mécanisme de sécurité du navigateur. Ce virus modifie les pages web et le contenu des transactions de manière indétectable par l'internaute et l'application hôte. En principe, dès que la machine de l'internaute est infectée par ce logiciel malveillant, le pirate peut effectuer exactement les mêmes actions que l'utilisateur de la machine et peut agir en son nom. Si l'utilisateur se connecte sur son compte en banque, le pirate peut effectuer toutes les opérations bancaires que l'utilisateur est lui-même en mesure d'effectuer. En étant invoqué par le navigateur lors de la navigation sur Internet, ce code peut reprendre la session à son compte et effectuer des actions malveillantes à l'insu de l'utilisateur.

[279] Nous témoignons récemment une nouvelle mode d'escroquerie c'est l'envoi de mails par faux créditeurs qui imitent les adresses des vraies créditeurs en changeant une seule lettre dans l'adresse qui passe effectivement inaperçue. Les débiteurs paient leurs dettes en suivant les instructions des faux mails.

358. Le client internaute peut également, lorsqu'il fait des achats en ligne et en vue d'éviter les fraudes bancaires et des prélèvements automatiques non désirés, opter pour des cartes bancaires prépayées qui ne comportent pas d'autorisation de découvert et ne sont pas reliées à son compte bancaire bien que chargée préalablement par les fonds de celui-ci.

359. Ainsi, lors des opérations de paiements, le transfert peut se faire dans l'anonymat total et le client internaute n'a plus besoin de communiquer des informations personnelles ou relatives à son compte bancaire. La carte bancaire prépayée est l'artère principale des activités commerciales et bancaires en ligne.

360. Enfin, bien que les articles L. 133-16 et 17 du code monétaire et financier imposent à l'utilisateur d'un service de paiement de prendre « *toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés* »[280] et d'avertir le prestataire de service de toute utilisation non autorisée de son instrument de paiement ou de ses données personnelles, toutefois les articles L. 133-19 et 23 imposent à la banque d'apporter la preuve de la fraude qu'elle invoque ou de la négligence de son client. Cette preuve ne peut pas consister en la simple déduction du fait que le titre de paiement ou les données confidentielles aient été utilisés pour effectuer des actes frauduleux.

361. Ainsi les juges[281] libanais ont débouté le client internaute de sa demande de remboursement aux motifs de sa négligence de préserver ses identifiants relatifs à ses activités bancaires électroniques. Dans ce cas, le client allégeait que le système de la banque était piraté et demandait par conséquent son remboursement des sommes piratées. La banque avait demandé la nomination d'un expert pour inspecter ses systèmes

[280] Cass. Civ. Ch. Com. Fin. Et eco. , 28 mars 2018, pourvoi no. 16-20.018 :« Si, aux termes des articles L. 133-16 et L. 133-17 du code monétaire et financier, il appartient à l'utilisateur de services de paiement de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés et d'informer sans tarder son prestataire de tels services de toute utilisation non autorisée de l'instrument de paiement ou des données qui lui sont liées, c'est au prestataire qu'il incombe, par application des articles L. 133-19, IV, et L. 133-23 du même code, de rapporter la preuve que l'utilisateur, qui nie avoir autorisé une opération de paiement, a agi frauduleusement ou n'a pas satisfait, intentionnellement ou par négligence grave, à ses obligations. Cette preuve ne peut se déduire du seul fait que l'instrument de paiement ou les données personnelles qui lui sont liées ont été effectivement utilisés ».

[281] C.App. de Beyrouth, arrêt rendu le 19/7/2018, Pharaon c/ Crédit Libanais - non publié.

informatiques et le rapport d'expertise avait déclaré que les systèmes de la banque étaient hautement sécurisés. Après interrogation du demandeur, ce dernier divulgua qu'il partageait ses identifiants et son mot de passe relatifs à son compte bancaire en ligne avec quatre autre personnes. Les juges ont donc exempté la banque du remboursement. Cet arrêt, que nous jugeons audacieux, a le grand mérite d'être parmi les premières décisions judiciaires libanaises qui montre la sensibilisation des juges au monde virtuel et leur impartialité dans l'investigation.

362. Ainsi nous constatons, que la naissance des litiges est inévitable en matière de transactions bancaires en ligne. Quelle serait la juridiction compétente en la matière ?

Chapitre 2 : Sécurisation juridique, la résolution des litiges relatifs aux transactions bancaires en ligne

364. Le bon déroulement et la sécurisation des transactions bancaires en ligne se réalisent également au niveau judicaire par le biais de la résolution des litiges devant les juridictions. Il s'agit d'une sécurisation juridique.

365. Vu leur vocation internationale, les transactions bancaires en ligne ont généré des conflits de nouvel ordre. Ce sont les conflits en ligne qui impliquent des acteurs multiples, des droits multinationaux, des cultures différentes et des éléments d'extranéité. D'où la nécessité de l'instauration des règles et moyens de résolution de litiges adaptées à ce réseau de communication et de transaction.

366. Le droit a bien évolué et nous avons déjà exposé les principales initiatives législatives en matière d'internet en général et en matière de banque en ligne en particulier. Cependant, les mécanismes juridiques classiques ne permettent pas d'assurer précisément une sécurisation adéquate à ce réseau ce qui engendre l'incertitude des acteurs en ligne et créée une ambiance en faveur des cybercriminels. Par conséquent, il serait judicieux de se demander s'il ne fallait pas imaginer des juridictions spécialement conçues pour l'internet sachant que celui-ci a facilité les transactions en ligne et que les modes de résolution de litiges y afférant devraient l'être également.

367. Ainsi, les personnes concernées peuvent soumettre leurs litiges aux systèmes juridictionnels étatiques mais elles ont parallèlement le choix d'opter pour des systèmes *ad hoc* spécifiques au monde virtuel. La technologie permet à certains égards de pallier les failles des systèmes judiciaires étatiques et des règles de droit international privé.

368. Nous allons exposer sommairement le contentieux en la matière et les recours judiciaires (Section 1) pour prouver que le passage aux modes alternatifs de règlement des litiges en ligne est essentiel pour une justice compatible avec le monde virtuel, les recours extrajudiciaires (Section 2).

Section 1 : Recours judiciaires en matière de conflits relatifs aux transactions bancaires en ligne

369. En cas de conflits au sujet des transactions bancaires ne ligne, il serait toujours souhaitable de chercher un accord à l'amiable. En l'absence de réussite de cette tentative de règlement amiable, une mise en demeure peut être notifiée suivie de l'engagement d'une procédure judiciaire.

370. Cependant, par application des principes du droit international, il ne serait pas éventuel de déterminer le lien de rattachement puisque les parties ne peuvent pas être localisées, ni d'ailleurs le lieu de la conclusion de la transaction et l'exécution de l'obligation principale.

371. Les conflits engendrés par les transactions bancaires en ligne peuvent être d'ordre délictuel (Paragraphe 1) ou d'ordre contractuel (Paragraphe 2).

Paragraphe 1 : En matière délictuelle

372. La compétence des juridictions étatiques en matière délictuelle est fondée sur la règle générale du droit procédural à savoir la juridiction compétente est celle du ressort de laquelle se trouve le domicile du défendeur ou lieu où le dommage est survenu[282]. La jurisprudence en matière d'internet est en conformité avec ce principe[283].

373. Le problème se pose au niveau de la détermination de ce domicile et la localisation du lieu du dommage sachant que le déroulement de la transaction est absolument virtuel.

[282] En droit libanais, articles 96 et 102 CPC. Droit français articles 42 à 46 du NCPC. En droit européen, Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000. En droit international, article 5-3° de la Convention Bruxelles du 27 septembre 1968.

[283] TGI Nanterre, Référé, 13 octobre 1997, affaire Société SG2 c/ Brokat Informations System GmbH (Allemagne). CJCE, 30 novembre 1976, Rec. 1976, p. 1735.

374. En droit libanais, ce sera le domicile du client internaute dont il a fait preuve lors de la conclusion de la transaction et en cas inverse, si la banque est défendeur au procès, c'est le tribunal dont ressort le siège social de la banque. En droit français, les mêmes règles s'appliquent avec la nuance que le domicile peut également être le lieu de la localisation du serveur. Rappelons que le site de la banque n'est qu'une enseigne et ne dote pas la banque de la possibilité de changer de siège social. C'est la destination de son activité qui change sans aucun effet sur la place de l'émission de cette activité.

375. Au Liban, les litiges relatifs aux transactions bancaires en ligne relèvent de la compétence des tribunaux nationaux. Le procureur général financier joue un rôle important dans la sécurisation des activités sur internet. Le Bureau de la lutte contre la cybercriminalité et de la protection de la propriété intellectuelle mène, suite au transfert du dossier par le procureur général, l'investigation et l'interrogation aux sujets des dossiers qui ont trait à la cybercriminalité. Ce bureau a le mérite de faire intervenir le secteur public dans l'expertise des crimes électroniques.

376. Par ailleurs, en matière des cyber-conflits délictuels nous soulignons la nécessité de renforcer la coopération entre les justices et les polices, notamment au niveau d'organismes comme Europol et Interpol. En outre, la coopération judiciaire doit être allégée pour être compatible avec le caractère virtuel de l'opération et de son mode d'exécution et des formes spécifiques aux réseaux doivent être développées.

Paragraphe 2 : En matière contractuelle

377. En matière contractuelle, la compétence judiciaire reste celle du droit commun. En effet, aucune législation communautaire n'en a apporté une dérogation. La Convention de Bruxelles du 27 septembre 1968 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale a étendu la zone étatique en prévoyant que le défendeur domicilié sur le territoire d'un Etat contractant pouvait être attrait dans un autre Etat contractant « *en matière contractuelle devant le tribunal du lieu où l'obligation qui sert de base à la demande a été ou doit être exécutée.* » (article 5.1.a).

378. Le Règlement n°44/2001/CE du Conseil Européen du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, qui transpose la Convention de Bruxelles, est une référence législative en matière de compétence judiciaire pour le commerce électronique. L'article 5, alinéa 1, du Règlement 44/2001 dispose qu'est compétent le «*tribunal du lieu où l'obligation qui sert de base à l'action a été ou doit être exécutée* ». Ce critère connote un lien entre le tribunal et le conflit.

379. En matière d'internet, le lieu d'exécution de l'obligation litigieuse est difficile à déterminer. Plusieurs locations géographiques peuvent être en relation avec l'exécution du contrat d'où une multiplication de juridictions compétentes compétents ou au contraire aucune juridiction ne s'avère être compétente.

380. Certains auteurs[284] distinguent entre le site web actif et le site web passif. Le premier indiquant que le prestataire dirige ses activités en ligne vers le pays du client internaute et par conséquent les prestations de services sera localisée dans ce pays et ses juridictions seront compétentes. Alors que dans le cas d'un site passif, ce dernier se limitant à diffuser des informations, la prestation de services se localise donc dans le pays du prestataire ce qui implique la compétence des juridictions dudit pays. Suivant cette approche, la localisation de la prestation et son corollaire la compétence juridictionnelle des tribunaux est sujette de la nature du site et de l'activité en ligne.

381. La Cour de Justice des communautés européennes[285] a jugé que le lieu d'exécution d'une obligation pouvait être déterminé volontairement par les parties par une clause du contrat. En effet, une telle possibilité contractuelle permet indirectement de désigner le tribunal compétent, sans être toutefois tenu de respecter les conditions de formes relatives aux clauses attributives de compétence[286] par lesquelles les parties conviennent du juge compétent pour connaitre des différends nés ou à naitre à l'occasion de la transaction. Par conséquent, les cocontractants peuvent, par prudence, inclure dans leur contrat des clauses attributives de compétence à une juridiction déterminée.

[284] MATHIEU M.E, Les services bancaires et financiers en ligne, 2005, éd. Revue Bancaire, p.309
[285] Arrêt du 17 janvier 1980, Rec., 1980, p. 89
[286] ABI RIZK, G.D., L'internet au service des opérations bancaires et financières, op. cit.

Section 2 : Recours extrajudiciaires en matière de conflits relatifs aux transactions bancaires en ligne

382. L'établissement de modes alternatifs de résolution des litiges en matière de consommation fait l'objet de préoccupations européennes depuis une dizaine d'années[287]. La directive sur le commerce électronique, dans le but de garantir de meilleurs moyens de recours par l'utilisation en ligne des mécanismes extrajudiciaires de règlement des différends, y compris par moyens électroniques, a imposé dans son article 17- 1 aux Etats membres de supprimer ou de modifier dans leurs législations les obstacles à cette utilisation. La suite de l'article 17 prévoit que les Etats membres doivent encourager les organes de règlement extrajudiciaires en matière de litiges de consommation à appliquer les principes d'indépendance, de transparence, du contradictoire, de l'efficacité de la procédure, de la légalité de la décision de la liberté des parties et de représentation dans le respect du droit communautaire.

383. Par application de cette directive, la Commission Européenne a créé une plateforme de règlement en ligne des litiges pour permettre aux consommateurs et aux professionnels dans l'Union Européenne de régler leurs litiges relatifs à l'achat en ligne de biens et de services sans aller en justice par un recours à un organisme impartial de règlement des litiges. Les procédures extrajudiciaires sont généralement plus rapides et moins coûteuses que les procédures judiciaires.

[287] Le Livre vert sur l'accès des consommateurs à la justice et le règlement des litiges de consommation dans le marché unique (1993) ;

- la Résolution du Parlement européen sur la communication de la Commission « *plan d'action sur l'accès des* consommateurs à la justice et le règlement des litiges (1996) » ;
- la Communication de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation (1998) ;
- la Recommandation de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation (30 mars 1998) ;
- la Recommandation de la Commission du 4 avril 2001 relative aux principes applicables aux organes extrajudiciaires chargés de la résolution consensuelle des litiges de consommation ;
- et plus récemment le Livre vert sur les modes alternatifs de résolution des conflits relevant du droit civil et commercial du 19 avril 2002 COM(2002) 196 final.

384. L'article 14 de la Directive sur les services financiers du 2002 a incité les Etats membres à instaurer et développer des procédures extrajudiciaires de réclamation et de recours qui soient adéquates pour résoudre les litiges transfrontaliers relatifs aux services bancaires fournis en ligne. Pour les services financiers, le plan d'action pour les services financiers (COM 1999/232) a suggéré que la Commission étudie la possibilité de recourir aux infrastructures actuelles pour régler les litiges transfrontaliers, en reliant les organes nationaux compétents en un réseau européen ad hoc[288].

385. Plusieurs modes alternatifs de règlement des litiges en matière financière en ligne ont été conçus entre autres le FIN-NET (Paragraphe 1) et les Modes Electroniques de Règlement des Litiges (Paragraphe 2).

Paragraphe 1 : Le réseau FIN- NET

386. La Commission Européenne a créé le 16 octobre 2001 le réseau FIN- NET[289] qui est un réseau dont la mission principale est de traiter par voie extrajudiciaire les litiges transfrontières qui oppose le client à son prestataire en matière de services financiers, tant pour les services en ligne que hors ligne, dans le cas où le prestataire de services est établi dans un autre État membre que celui où réside le client. Il regroupe plus de 35 organismes nationaux, qui chapeautent spécifiquement certains services financiers (par exemple, les médiateurs des secteurs bancaire et assurantiel, le médiateur de la Commission des opérations de bourse) ou bien règlent les litiges de consommation en général (par exemple, les chambres de recours pour les consommateurs).

387. Les trois objectifs de ce réseau sont en premier lieu de permettre aux consommateurs d'accéder aisément et en bonne connaissance de cause à un système de règlement extrajudiciaire des litiges transfrontaliers. A cette fin, le réseau aide les consommateurs à déterminer le système le mieux indiqué pour recevoir leurs plaintes, en leur donnant toutes les informations nécessaires dans leur propre langue.

[288] Cette proposition se fonde sur la Recommandation n°98/257 de la Commission du 30 mars 1998.
[289] C'est le Financial Services Complains Network https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-

388. Il sert en second lieu à assurer un échange d'informations efficace entre les différents systèmes européens, de sorte que les recours transfrontaliers puissent être traités aussi rapidement, efficacement et professionnellement que possible.

389. Il vise enfin de faire en sorte que les systèmes de règlement extrajudiciaire des litiges des États membres de l'Union européenne respectent un ensemble commun de principes minimaux. Par conséquent, la plupart des Etats membres ont mis en place des procédures de résolution extrajudiciaire des litiges.

Paragraphe 2 : Les Modes Electroniques de Règlement des Litiges (MERL)

390. L'expression « *Online Dispute Resolution* » (ODR) est une création américaine mais qui s'implante dans les pays européens. Ce sont des modes alternatifs de règlement des litiges qui ont pour dénominateur commun le déroulement du procès exclusivement en ligne et la réunion des colitigants par voie électronique.

391. La nature juridique des MERL réunit en même temps un caractère contractuel avec un caractère institutionnel.

392. L'objectif de ces modes est de fournir aux internautes des moyens rapides et peu couteux. Ils ont le mérite sans doute d'avoir une perspective ciblée des conflits et une expertise poussée par rapport aux tribunaux étatiques.

393. L'arbitrage est le dénominateur commun des résolutions de litiges hors les juridictions. Les cocontractants peuvent consentir de soumettre leur litige potentiel ou survenu à l'arbitrage. Ce moyen de justice privé est bien organisé au plan interne et international. Nous témoignons de nos jours un mécanisme d'arbitrage en ligne dans différents domaines notamment de propriété intellectuelle.

394. Un système de juge virtuel a été mis en place il y a quelques années c'est le Magistrat Virtuel [290]. Il s'agit d'un service autonome de résolution en ligne des différends ou service d'arbitrage en ligne innovateur [291]. Il propose une procédure en ligne facultative et facilement accessible, rapide et peu coûteuse pour résoudre des différends touchant aux utilisateurs fournisseurs de contenu, opérateurs de systèmes et préjudiciables du réseau internet.

395. La procédure se déroulait par échange de courriel. Le demandeur doit remplir un questionnaire et exposer l'affaire et ses demandes. Le Magistrat Virtuel rend sa décision dans les plus brefs délais (trois jours). Le processus est basé sur le consentement des parties à soumettre leur cas à l'arbitrage. Le Magistrat Virtuel avait vocation à régler les différends relatifs à des messages et fichiers au contenu illicite, tel que contrefaçon de droit de propriété intellectuelle, détournement de secrets d'affaires, concurrence déloyale et aussi violation de la vie privée. Ce projet n'a pas connu un succès, le Magistrat Virtuel n'a rendu qu'une décision, il a été confié au *Chicago-Kent College of law*.

396. Nous jugeons que le passage à un tribunal virtuel est encore précoce à ce stage. Peut-être, une fois les activités bancaires gagnent la confiance totale, de tels organismes peuvent être institués. Rappelons d'ailleurs que la matière bancaire est très délicate et suscite des décisions sous l'égide du secteur public.

397. En tout état de cause, si le tribunal virtuel s'avère être acceptable, il reste cependant que l'octroi de l'exequatur aux décisions rendues par de tels organismes pas acceptables par les autorités officielles, du moins pour le moment. Nous pensons qu'avec le temps, un organisme ad hoc sera bien installé et sèmera la confiance à ce propos.

[290] En anglais « *Virtual Magistrate* ».

[291] Ce projet est le fruit de la collaboration entre l'institut du droit de l'Internet et le centre national de recherche pour l'information automatisée aux Etats-Unis.

Conclusion :

398. «*Notre époque est dédiée pour le meilleur et pour le pire, à la technologie, qui permet notamment aux êtres humains de communiquer entre eux par l'intermédiaire des ordinateurs et de se passer en un trait de temps, d'un point à un autre de la planète, des images, des sons et des textes*»[292].

399. Un marché numérique, avec de nouveaux acteurs et de nouvelles techniques était initialement limité aux relations professionnelles puis étendu à la sphère privée pour revêtir un aspect universel. Cela a engendré, en quelques décennies, une véritable révolution des comportements et des façons de faire du consommateur[293].

400. Des milliards de personnes recourent aujourd'hui à internet pour effectuer des transactions bancaires et n'hésitent plus à payer en ligne depuis divers appareils (ordinateurs, tablettes et téléphones mobiles). Cela démontre en effet la confiance placée dans ce nouveau canal et la sécurité qu'il inspire grâce aux moyens de sécurisation mis en place.

401. Les services bancaires en ligne trouvent petit à petit un cadre juridique. Néanmoins, la sécurisation reste un impératif primordial à assurer au niveau de la formation, conclusion et exécution des transactions bancaires. D'ailleurs le défaut de sécurisation porte préjudice à la fois à la banque et au client internaute. En effet, en plus des conséquences directes de l'incident technique, la banque subit une atteinte à son image et une perte de clientèle compte tenu de la «*volatilité de la clientèle internaute*»[294].

[292] GAUTIER P.-Y. & DE BELLEFONDS X. L., De l'écrit électronique et des signatures qui s'y attachent, JCP G, 2000, doctrine, I, 236, p 1113.

[293] Selon l'enquête du CREDOC « Conditions de vie et Aspirations » réalisée en 2017 sur les français :85% dispose au moins d'un ordinateur au domicile, mais la proportion s'élève à 98% pour les 12-17 ans. 4 français sur 5 sont internautes, 85% disposant d'un accès fixe à Internet à leur domicile et 73% d'un smartphone ; 44% des foyers possèdent une tablette tactile. Et ces chiffres sont en constante augmentation.

[294] Mathieu M-E, Les services bancaires et financiers en ligne, éd. Revue Banque, 2005, p. 213, no. 212.

402. Toutefois, veiller assurer la sécurisation des transactions en ligne est une tâche assez complexe à l'apparence d'un « kaléidoscope »[295]. Elle consiste à assurer l'identification des acteurs, et en garantir une authentification, à protéger les systèmes informatiques contre l'accès non autorisée et contre les attaques des logiciels malveillants, assurer la disponibilité des services, à protéger les communications et en garantir la confidentialité.

403. Nous constatons que le recours à la banque en ligne requiert une sécurisation d'un autre rang car il s'agit de la sécurisation psychologique de ses clients en vue de les encourager à faire des transactions bancaires en ligne. D'ailleurs, « dans la vie, rien n'est à craindre, tout est à comprendre »[296].

404. Rappelons que le secteur bancaire a toujours était la cible des criminels. Même à l'ère où le papier était le seul moyen d'effectuer des transactions bancaires, les infractions étaient innombrables et les voleurs étaient aussi innovateurs que les cybercriminels.

405. La sécurisation du nouveau réseau de services financiers fut la préoccupation non seulement du législateur et des autorités de contrôle des banques mais aussi de la banque elle-même. La banque en sécurisant ses transactions, ne vise pas uniquement l'intérêt du client. Il s'agit d'intérêts synallagmatiques. D'une part, assurer la confidentialité et la sécurité des informations financières du client pour le rassurer et semer la confiance en de telles opérations pour qu'il n'hésite pas à acheter et payer en ligne, par crainte des fraudes éventuelles, et d'autre part garder la banque à l'abri des failles et incidences à portée considérable, non seulement sur la situation financière de la banque, mais également sa clientèle et sa réputation comme l'a si bien révélé l'Observatoire des nouveaux Modes d'Authentification (OMODA)[297]. De même les banques ont beau apporter des preuves irréfragables du respect des réglementations de sécurité, elles seront tenues responsables en cas de manquement.

---

[295] Mathieu M-E, Les services bancaires et financiers en ligne, op. cit.

[296] Curie M., chimiste française, Prix Nobel de physique en 1903 puis de chimie en 1911 (1867-1934).

[297] 37 % des Français ne sont pas satisfaits de la sécurité de leurs opérations bancaires et 30 % seraient prêts à changer de banque pour plus de sécurité, révèle l'Observatoire des nouveaux Modes D'Authentification (OMODA) du cabinet Galitt, fondé sur 800 entretiens téléphoniques avec un échantillon représentatif, de la population française et 17 entretiens qualitatifs avec des acteurs de l'écosystème de l'authentification.

406. Mr. DEMOGUE avait bien expliqué le dilemme en relatant « *la conciliation entre la sécurité et l'innovation est délicate, par certains côtés même, impossible, car c'est concilier l'immobilité avec le mouvement, un mouvement avec un autre tout différent, parfois opposé. Il faut faire état des transformations économiques tenant à une intensité plus grande de production, de consommation, de circulation qui rend insupportable les anciennes règles. Comment peut-on concilier ces deux besoins nettement antagonistes : le besoin de sécurité satisfait, qui donne à toute l'armature sociale et spécialement à l'armature juridique toute sa force, sa rigidité, et le besoin de changement, besoin de souplesse qui suppose une organisation sociale et juridique se prêtant à certains changements*».[298]

407. Mais l'ingéniosité humaine fait en sorte que certains se donnent pour mission d'enfreindre ce que les autres légifèrent. D'où la nécessité d'une intervention législative continue pour mettre à jour les dispositions légales englobant les nouvelles techniques et/ou les nouvelles infractions. Notons à ce sujet l'expansion de la banque via téléphone mobile [299] mais surtout la monnaie virtuelle ou électronique [300] ou même le chèque électronique[301].

[298] René DEMOGUE, Les notions fondamentales du droit privé : Essai critique, éd. La mémoire du droit 2001, Réimpression de l'édition de 1911, p. 89-90.

[299] Le paiement via téléphone mobile peut prendre 4 aspects : 1) donner l'ordre par appel téléphonique à la banque (la banque exécute après l'interroger sur son identité) ; 2) envoyer un SMS à la banque (la banque exécute l'ordre après identifier via le numéro de téléphone et le code secret inséré) ; 3)utiliser le téléphone comme devis muni d'un Internet Protocol ; 4) attribuer la facture de la transaction faite à la société télécommunication qui ajoute le montant aux factures de téléphones du donneur d'ordre.

[300] La monnaie électronique est une innovation monétaire. Elle consiste en une réserve de valeur prépayée, stockée sur un support informatique ou électronique. En droit européen, Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE. JO L 267 du 10/10/2009 p 7-17.
Au Liban, la BDL a déjà coupé cours à cette aventurière (Décision 7548).

[301] Le chèque électronique ou cheque en ligne contient les mêmes notions qu'un chèque bancaire en papier (montant, date, nom du bénéficiaire, nom de l'émetteur et sa signature). Pour l'émission de chèque en ligne, sur le site de la banque, il y a un formulaire de chèque avec le montant, l'adresse et le nom du bénéficiaire. Ce dernier reçoit par courrier le chèque émis en ligne. Le chèque électronique implique l'intervention d'un intermédiaire « *clearing house* », généralement c'est une banque.

408. Rappelons que la sécurité est l'affaire de tous. Pas de solution miracle et la sécurité absolue n'existe pas le risque zéro ne peut évidemment pas être garanti mais les mesures prises par les acteurs protagonistes des transactions bancaires en ligne ont abouti récemment à une baisse significative des cas de fraudes en ligne durant l'année passée[302].

409. Le législateur européen a d'ores et déjà réalisé l'importance de la révolution technologique et l'utilisation expansive de l'internet et son objectif était d'assurer un niveau de protection des consommateurs plus élevé dans l'ensemble de l'Union Européenne en souhaitant que les mêmes règles s'appliquent lorsque les consommateurs effectuent une transaction en ligne ou hors ligne dans un magasin local. Le Parlement Européen fut le parrain des activités via internet et grâce à ses interventions, les activités en ligne jouissent d'un cadre juridique et d'un support législatif. Cela est justifié en pratique par l'avancée lente la réglementation européenne avance lentement, laissant aux banques le soin de tester et de choisir les technologies les plus appropriées.

410. Au Liban, un grand besoin s'annonce pour combler les lacunes législatives. Nous ne pouvons pas nous fier au droit commun puisque les lois et codes libanaises datent toujours des années où le Liban étant encore sous le mandat français et il est donc nécessaire de le moderniser. Il serait habile d'édicter une *lex electronica* en s'inspirant du système français et européen.

411. Nous nous demandons, en présence de toutes ces lois et techniques consuméristes, s'il ne faut pas aussi édicter une loi pour la protection du professionnel à l'instar du client consommateur du fait qu'en matière d'activité en ligne et en présence de machines et appareils générant des actes juridiques, la banque en ligne est elle aussi une partie faible voire une victime de plusieurs manœuvres criminelles.

[302] https://www.latribune.fr/entreprises-finance/banques-finance/baisse-historique-de-la-fraude-au-paiement-electronique-784691.html. En plus selon le rapport annuel de l'Observatoire de la sécurité des moyens de paiement (exercice 2016) : « Le taux de fraude sur les paiements à distance, qui s'élève à 0,199 % contre 0,229 % en 2015, est également en baisse sensible pour la cinquième année consécutive ».

412. En l'absence d'une protection législative, un outil pratique peut servir de protection à la banque qui se voit subir un grand fardeau c'est l'assurance[303] contre le cyber risque. Les potentiels clients de ce nouveau produit ou catégorie d'assurance seront non seulement les banques mais aussi toute personne, particulièrement, personne morale effectuant des e-opérations. L'assurance en matière de risque numérique envisagera l'évaluation des d'évaluer les risques en vue de calculer la prime d'assurance. D'où la compagnie d'assurance servirait à amplifier le contrôle de la mise en œuvre des mesures de sécurité numérique possibles pour éviter la survenance d'un sinistre et manifesterait alors des exigences de protection et des nouvelles normes de sécurité.

413. Notons enfin que les banques en ligne doivent assurer la sécurisation de leurs activités en ligne et sophistiquer[304] (tel le modèle des *blockchain*) ces dernières pour maintenir leur place sur internet qui témoigne de nos jours un important bouleversement du secteur des services financiers de détail avec l'apparition de nouveaux modèles d'entreprises et l'implantation des prestataires exclusivement en ligne et des entreprises technologiques financière (telles que *Fintechs*) proposant toute une gamme de services et des prestations transfrontières (virements électroniques, intermédiation de paiements en ligne, agrégation de données financières, financement entre pairs, comparaison des prix) plus rapides, plus réactifs et davantage sur mesure. Nous assistons également à l'arrivée de nouveaux acteurs, qui ne sont pas des prestataires de services financiers classiques. Des médias sociaux, par exemple, vendent désormais des produits financiers.

[303] La BDL a imposé aux banques de contracter des polices d'assurance sur leurs activités en ligne (Décision de base no. 12725 du 28 novembre 2017 (Circulaire 144) relative à la prévention des actes criminels électroniques

[304] En intégrant les technologies numériques les plus récentes telles que les grands livres distribués (*distributed ledgers*), sur le modèle du *blockchain* utilisé par Bitcoin, sont l'occasion de réorganiser les processus internes et de réaliser des économies d'échelle grâce à une standardisation et une automatisation accrues.

Bibliographie

1. Les ouvrages

A

ARAB Younis, Le droit de l'informatique, Union des Banques Arabes, Beyrouth, 2001.

ARAB Younis, Les crimes informatiques, Union des Banques Arabes, Beyrouth, 2002.

ARAB Younis, La confidentialité et la protection des bases de données dans l'ère digitale, Union des Banques Arabes, Beyrouth, 2002.

B

BONNEAU Thierry, Droit bancaire, Montchrestien, 4e éd. 2002.

BONNEAU Thierry, et DRUMMOND France, Droit des Marchés Financiers, Economica, 1ere éd. 2001.

BREESE Pierre, Guide juridique de l'internet et du commerce électronique, Librairie Vuibert, Paris, 2000.

C

CABRILLAC Michel et MOULY Christian, Masson, Droit Pénal de la Banque et du Crédit, Collection Droit Pénal des Affaires dirigées par M.E. Cartier, 1982

CAUSSE Herve, Droit bancaire et financier, Mare & Martin 2015.

D

DEMOGUE René, Les notions fondamentales du droit privé : Essai critique, éd. La mémoire du droit 2001, Réimpression de l'édition de 1911.

H

HAJJAR Wassim, La preuve électronique, Sader 2002

I

ISSA Toni, La régulation légale du réseau internet, Sader 2001

ISSA Toni, Les spécificités des contrats informatiques, Sader 1996

J

JABBOUR Mona et JABBOUR Aref, Le droit et l'internet, Sader 2008

L

LAMY Droit de L'Informatique et des Réseaux, Collection Lamy Droit de l'Immatériel, 2007

LAMY Droit de L'Informatique et des Réseaux - Guide Solutions et applications –Pratique Contractuelle, Collection Lamy Droit de l'Immatériel, 2007

LAMY Droit du financement, 2011.

LE TOURNEAU Philippe, Contrats Informatiques et électroniques, Dalloz, 4e éd. 2006.

M

MAHMASANI, Ghaleb, L'Organisation Bancaire au Liban, Librairie du Liban, 1968.

MANSOUR Sami, La preuve électronique en droit libanais, Revue Al-Adl, 2001.

MARTRES Didier et SABATIER Guy, La monnaie électronique, Que sais-je ? PUF, Paris 1987.

MGHABGHAB Naim, Les risques de l'informatique et de l'internet – les risques sur la vie privée et sa protection, 1998.

N

NAMMOUR Fadi, Droit bancaire, Beyrouth 2012

NASSIF Elias, Le contrat électronique en droit comparé, Al Halabi Law Publishers, éd. 2009.

P

PEZARD Alice et ELIET Guillaume, Déontologie et droit des activités financières : comparaisons internationales, Montchrestien, 1997.

S

SAAD Farouq, Les procédures de l'arbitrage à distance, Sader 2003

SAFA Ghannagé Jocelyne, Le devoir de vigilance du banquier, éd. Sader 1996.

SAFAR Ahmad, L'activité bancaire par les legislations et la sécurité electribue, Revue Annahar, 17 septembre 2001.

2. Articles

B

Basel Committee on Banking Supervision, Risk Management Principles for Electronic Banking, July 2003.

BENSOUSSAN (A), un nouveau métier, le tiers certificateur, se profile sur internet, OnLine Journal, 15 décembre 1995.

BENSOUSSAN (A), Commerce électronique et avenirs des circuits de distribution : de l'expérience des Etats-Unis aux perspectives françaises, aspects juridiques et fiscaux (colloque du 13 mai 1998), Gaz. Pal. 20 octobre 1998.

BENJAMIN Delaunay, Pons-Henry et Jean-Philippe, La procédure répressive de l'ACP mise à l'épreuve, Joly Bourse, 01 nov. 2011 n° 11, p. 585.

BONNEAU Thierry, Communication de pièces et secret bancaire, RD bancaire et fin. 1995.

BOUILHOL Herve, Les aspects juridiques de l'e-banking, Banque & Droit, no. 93, janv-fev. 2004.

BOUTEILLER Patrice, Le nouveau cadre juridique des relations entre les banques et leurs clients, Juris-Classeur, Contrats-Concurrence-Consommation, Chronique, Mars 2002.

C

CABRILLAC Michel et MOULY Christian, Masson, Droit Pénal de la Banque et du Crédit, Collection Droit Pénal des Affaires dirigées par M.E. Cartier, 1982.

CACHARD Olivier, Les modes électroniques de règlements des litiges, Juris-Classeur, Contrats-Concurrence-Consommation, Chronique, Décembre 2003.

CAPRIOLI Éric, De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales ? »

CAPRIOLI Éric, Première décision américaine concernant l'authentification par voie électronique d'un client bancaire Lexis Nexis no. 4, Avril 2010.

CAPRIOLI Éric, Arbitrage et médiation dans le commerce électronique, l'expérience du cuber-tribunal, Revue Arbitrage 1999.

CARON L., Protection des données personnelles sur Internet et enjeux du commerce électronique, in. La galaxie Internet, Paris, UNICOMM, 1998.

CATALA Pierre, L'engagement électronique de l'entreprise, Revue des sociétés: journal des sociétés, ISSN 0242-5424, Nº 2, 2001, p. 258-270.

CHABOT Gérard, La cyber justice : réalité ou non?, Dalloz 2003, Chroniques.

CHAMPAGNE Julien « Les principales menaces de la banque en ligne pour les prestataires de services financiers » (2 septembre 2010).

CLEMENT Jean-François, Le banquier, vecteur d'informations, RTD Civ. 1997.

CNIL, La sécurité des données personnelles, Les Guides de la CNIL. Ed. 2018.

CNIL, Opération Audit de la banque en ligne, étude réalisée au 1er semestre 2005.

COLLIARD Claude-Albert, La machine et le droit privé français contemporain, Mélange L.G.D.J., 1950.

COHEN-BRANCHE Marielle, Tarification, relation de clientèle et opacité (conférence 30 mai 2005).

COSTES Luc., Ribeyre M.A, Une meilleure articulation européenne entre commerce électronique et services financiers : Lamy, droit du financement, avr. 2001, Bull. A.

COUPEZ François et VERBIEST Thibaut, Commercialisation à distance des services financiers : bilan d'un nouveau cadre juridique, Recueil Dalloz 2006, no. 44.

CREDOT F.J, Le secret bancaire, son étendue et ses limites, la fourniture de renseignements commerciaux par les banques, LPA 17 fév. 1993.

D

DANJAUME Géraldine., La responsabilité du fait de l'information, JCP G, 1996, I.

DEFOSSEZ Michel, Droit communautaire, protection du consommateur de crédit et promotion du commerce électronique, Revue de Droit Bancaire et Financier, juillet-aout 2004, p. 284 (Dossier commerce électronique et opérations bancaires).

DIAB Nasri, Le droit de l'investisseur à l'information sur les marchés financiers, Revue Al-Adl 2015.

F

FABRE Cyril, noms de domaine. De l'identifiant technique à une nouvelle forme de droit de propriété incorporelle par destination ?, Legalis.net 2002/3.

G

GUP, BENTON E., The Future of Banking, Ed. Greenwood Press, 2003.

GARTNER, Inc. "Banks Need to Strengthen User Authentication While Appeasing Consumers." Mai 2010. ID G00158229.

GAUTIER P.-Y. & DE BELLEFONDS X. L., De l'écrit électronique et des signatures qui s'y attachent, JCP G, 2000, I, 236.

H

HUET Jérôme, Commerce électronique : loi applicable et règlement des litiges – propositions des grandes entreprises, JCP, Actualité, 1999.

HUET Jérôme et VALMACHINO Stefania, Réflexions sur l'arbitrage électronique dans le commerce international, Gazette du Palais, Recueil Janvier- février 2000.

J

JOSSERAND Louis, La protection des faibles par le droit, Evolutions et Actualités, conférences de droit civil, Sirey 1936.

JOURDAIN P, Le devoir de se renseigner, contribution à l'étude de l'obligation de renseignement, D. 1983, Chronique 139.

L

LACOURSIERE Marc, La responsabilité bancaire à l'ère du commerce électronique : impact des autorités de certification, www.erudit.org.

LABRUNIE F, Le devoir d'information du banquier et le secret professionnel, Gaz. Pal. 05 déc. 2000.

LECLERC Philippe, L'obligation de conseil du banquier dispensateur de crédit, RJDA 1995.

LOISEAU George, Nom de domaine et internet : turbulence autour d'un nouveau signe distinctif, Dalloz 1999, Chronique.

M

MANSOUR Sami, La preuve électronique en droit libanais, Revue Al-Adl 2001

MATHIEU Marie-Elisabeth, Transactions bancaires et financiers à distance, Juris- Classeur Banque - Crédit – Bourse, Cote 2, 2004.

N

NASR, Le secret bancaire, Revue Judicaire libanaise 1961.

R

RITAN Hubert, Le site de commerce électronique : approche technique et juridique, Gazette du Palais, Recueil mars-avril 2000.

RIZK (Pierre-Antoine), Le RGPD va-t-il ralentir l'Union Européenne en matière d'intelligence artificielle ?

S

SAINT-ALARY B, Aspects juridiques et pratiques de la tarification bancaire, (Dalloz, Edition 2016).

SOUMRANI Patrick, Solidité du secret bancaire de la loi du 3 septembre 1956, Al Adl 1997.

SOUSI-ROUBI V. B., Directives bancaires et commerce électronique : quelle articulation ? Les Echos, 31 janv. 2001.

V

VIVANT Michel, Biens informationnels, JCP éd G 1984, I.

VERBIEST Th., CUIGNET P, La création d'un délit d'usurpation d'identité numérique.

VAUPLANE H, CMF ordres de bourse par internet : Banque et droit nov.-déc. 1999.

3. Rapports et Bulletins

Association Française des Entreprisses d'Investissement, La fourniture de services et de produits financiers à l'épreuve d'Internet : Quel environnement juridique pour les prestataires de services d'investissements ?, Rapport d'un groupe de travail constitué par le Comité juridique de l'AFEI, Octobre 2000.

Banque de France, Livre Blanc Internet, quelles conséquences prudentielles ?, 2000

Banque de France, ACPR, Lignes directives relatives à la relation d'affaires et au client occasionnel, Avril 2012.

Commission bancaire (rapport annuel) : « Les nouvelles technologies de la banque à distance : quelles conséquences pour les établissements financiers et leurs autorités de contrôle ? » 1999.

Commission Bancaire, Livre Vert sur les services financiers de détail dans l'Union, 2007.

Commission Bancaire, Livre Vert sur l'accès des consommateurs à la justice et le règlement des litiges de consommation dans le marché unique (1993).

Commission Bancaire, Livre Vert sur les modes alternatifs de résolution des conflits relevant du droit civil et commercial du 19 avril 2002.

Conseil d'Etat français, Internet et les réseaux numériques, 2 juillet 1998, éd. La Documentation française 1998.

CNIL, Opération Audit de la banque en ligne, 2005.

CNIL, Les Guides de la CNIL « La sécurité des données personnelles », Ed. 2018.

Rapport de DANESI René et HARRIBEY Laurence, La cyber sécurité, un pilier robuste pour l'Europe numérique.

Rapport n°458 (2017-2018) du 20 avril 2018.

Fédération Bancaire Française, L'année de la banque en 2016.
Rapport de l'AEAPP sur les bonnes pratiques en matière de sites web comparateurs (*Good Practices on Comparison Websites*) – Janvier 2014.

Ministère de l'Economie et des Finances français, Baromètre du numérique 2017, www. credoc.fr.

Observatoire de la Cyberconsommation, Les paiements sur l'internet, Mai 2005.

Rapport annuel de l'Observatoire, La sécurité des moyens de paiement (exercice 2016).

Document émis par le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques (CERTA) n° 2005-REC-001 du 1er mars 2005.

4. Thèses

BOUCARD François, Les obligations d'information et de conseil du banquier, Thèse de doctorat en Droit Sous la direction de Dominique Legeais, soutenue en 2001.

ABI RIZK, Georges Daladier., L'internet au service des opérations bancaires et financières. Thèse de doctorat en Droit, soutenue en 2002.

BOULAICH BAYSSA Fatima Zahra, Les prestations financières en ligne, Thèse de doctorat en Droit sous la direction Gilbert PARLEANI, soutenue en 2013.

5. Codes, Directives, Lois, Règlements, Circulaires, Décisions

Droit libanais :

- Code de la Monnaie et du Crédit
- Code de Commerce
- Code des Obligations et des Contrats
- Code Pénal
- Loi 3 septembre 1956 relative au secret bancaire
- Loi no. 133 du 26 octobre 1999 relative à la mission de la Banque du Liban
- Loi no. 318 du 20 avril 2001 concernant la lutte contre le blanchiment d'argent
- Loi no 659 du 4 février 2005 sur la protection du consommateur
- Avant-projet sur la communication, l'écriture et les transactions électronique (ECOMLEB), mai 2005.
- Loi n° 44 du 24 novembre 2015 sur la lutte contre le blanchiment de capitaux et le financement du terrorisme. Adoption de l'amendement de la loi n° 318 du 20 avril 2001 relative à la lutte contre le blanchiment des capitaux.
- Loi no. 55 du 27 octobre 2016 relative à l'échange d'information à des fins fiscales.
- Loi du 27 septembre 2018 sur les transactions électroniques.
- Décision de base de la BDL no. 7548 du 3 mars 2000 sur les opérations financières et bancaires par voie électronique (circulaire no. 69).
- Décision Intermédiaire de la BDL no. 12018 du 30 mars 2000 relative aux banques et institutions entreprenant des opérations financières et bancaires par voie électronique (circulaire no. 393).
- Directive de base de la BDL no. 8341 du 24 janvier 2003 (circulaire 92).
- Décision de base de la BDL no. 8710 sur les opérations financières et bancaires par voie électronique, du 29 avril 2004.
- Décision de base de la BDL no. 9668 du 9 aout 2007 (circulaire 109).
- Décision de base de la BDL no. 7818 du 18 mai 2001 (circulaire 83).
- Circulaire no. 222 du 18 aout 2000, recommandations générales de la Commission de Contrôle des Banques concernant les règles de base en matière de sécurité du système d'information.

- Décision de base de la BDL no. 9668 du 9 aout 2007 (circulaire 109).
- Décision Intermédiaire de la BDL du 2 novembre 2010 (circulaire 233).
- Décision de base de la BDL no. 10965 du 5 avril 2012.
- Décision Intermédiaire de la BDL no. 11445 du 6 juin 2013 (circulaire 325).
- Décision Intermédiaire de la BDL no 11707 du 28 février 2014 (circulaire 355).
- Décision Intermédiaire de la BDL no. 11935 du 26 janvier 2015 (circulaire 385).
- Décisions du Ministère des finances no. 449/1 du 17 mai 2016 et no. 883/1 du 12 aout 2013, et no. 15/1 du 14 janvier 2016.
- Décision de base no. 12725 du 28 novembre 2017 (Circulaire 144) relative à la prévention des actes criminels électroniques.
- Décision de base de la BDL no. 9668 du 9 aout 2007 (circulaire 109).
- Décision de base no. 12872 du 13 septembre 2018 (Circulaire 146) relatif aux procédures de conformité avec le Règlement Européen de la protection des données personnelles.

Droit français

- Code monétaire et financier
- Code civil
- Code de commerce
- Code de la consommation
- La loi Godfrain du 5 janvier 1988, ou Loi no 88-19 du 5 janvier 1988 relative à la fraude informatique,
- Loi 96-597 du 2 juillet 1996 de modernisation des activités financières.
- La loi 2000-719 du premier août 2000, transposant la Directive 2000/31/CE du parlement européen, relative au commerce électronique en droit interne français.
- Loi n° 2003-706, 1er août 2003 relative à la sécurité financière
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)
- Ordonnance qui a transposé la directive 2007/64/CE du 13 nov. 2007 sur les services de paiement.
- Loi n°2010-1249 du 22 octobre 2010

- Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite loi LOPPSI II, JORF n°0062 du 15 mars 2011
- Loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité - JORF n°0075 du 28 mars 2012 p 5604.
- La loi n°2014-344 du 17 mars 2014, dite « Loi Hamon ».
- Décision n° 99-07 du 15 septembre 1999 relative « aux prescriptions et recommandations pour les prestataires de services d'investissement offrant un service de réception-transmission ou d'exécution d'ordres de bourse comportant une réception des ordres via Internet.
- Décision n°2012-652 du 22 mars 2012 du Conseil constitutionnel.

Droit Européen

- Directive n°93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.
- Directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.
- Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).
- Directive 2005/60/ce du Parlement Européen du 26 octobre 2005.
- Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.
- Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les

transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE sur les signatures électroniques.

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) en vigueur mai 2018.
- Résolution du Parlement européen sur la communication de la Commission « plan d'action sur l'accès des consommateurs à la justice et le règlement des litiges (1996).
- Communication de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation (1998).
- Recommandation de la Commission concernant les principes applicables aux organes responsables pour la résolution extrajudiciaire des litiges de consommation (30 mars 1998).
- Recommandation n°98-05 relative à la diffusion sur Internet d'informations financières par les sociétés dont les titres sont admis aux négociations sur un marché réglementé, Bulletin mensuel n° 334- avril 1999.Recommandation n°99-02 relative à la promotion ou la vente de produits de placement collectif ou de services de gestion sous mandat via internet, bulletin mensuel n° 337- juillet/août 1999. Décision générale n° 99-07 relative aux prescriptions et recommandations pour les prestataires de services d'investissement offrant un service de réception-transmission ou d'exécution d'ordres de bourse comportant une réception des ordres via internet, septembre 1999.
- Recommandation n°2000-02 relative à la diffusion d'informations financières sur les forums de discussion et les sites internet dédiés à l'information ou au conseil financier, novembre 2000.
- Recommandation de la Commission du 4 avril 2001 relative aux principes applicables aux organes extrajudiciaires chargés de la résolution consensuelle des litiges de consommation.
- Règlement Général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Droit International

- Accord Bâle II (2008)
- Convention de Bruxelles du 27 septembre 1968
- Convention CNUDCI sur les le commerce électronique
- Convention de Rome 19 Juin 1980
- Foreign Account Tax Compliance Act (FATCA) 18 mars 2010.
- Principes UNIDROIT

6. Les arrêts et jugements

- Cass. Lib. Pourvoi no. 92, 11 octobre 1956, Baz 955 p.111.
- CA Rouen, 16 janvier 1979, JCP E 1981, II, 13506, no. 16.
- Cass. Com., 2 décembre 1980, no 79-11.231, Bull. Civ. IV, no. 400. Routier (R).
- Beyrouth, 15 déc. 1981 : Hatem fasc. 174 p. 504. Beyrouth, 10 nov. 1960 : Chamseddine, Droit comm.1985, p. 182.
- CA Paris, 8 oct 1981, D. 1982, IR p. 124, obs. M. Vasseur.
- CA Paris, 4 mars 1987, D.1987, p. 288, obs. Vasseur. CA Paris 13 Nov. 1992, JCP 1993, pan. 177, I, 301 obs. Gavalda et Stoufflet.
- Cass. 1e civ. 28 avril 1987, D. 1988.1 note Delebecque.TGI Paris, 25 mars 1987 : D. 1988, somm. p. 19. F
- Cass. 1re civ., 20 nov. 1990, Dame Monanges c/ Kern et autres : JCP G 1992, II, 21908, note J. Ravanas).
- CA Paris, 20 mars 1990, D. 1992, somm. P.31, obs. M. Vasseur.
- Cass. 1e civ. 24 nov. 1993, D. 1994 som. com. p. 236, obs. Paisant, Defrénois, 1994 p. 818 obs. D. Mazeaud , Cass. 1re civ. 21 fév. 1995, JCP 1995.II.22502, n. Paisant).
- Tribunal correctionnel de Privas, 3 septembre 1997, disponible sur : http://www.cyberlex.org/haas/coquine.htm, note HAAS G. et TISSOT O.
- Cour Banc. Spec. No. 103/167 du 1 déc. 1998 Mebco (en liquidation) c/ BLOM Bank, cité par Sader « Les banques, droit et jurisprudence», p. 214.
- CA. Pau., 14 oct. 1999, France Telecom, JCP E 2000, p. 873T.com. Paris, 23 mars 2000, ISA c/Omniséquence, Expertises 2000 p. 355.
- C. Appel Versailles, 14 mars 2001, Ste AOL Bertelsmann Online France, Gaz Pal. 2002, 1, somm. P.261.
- Cass. Com. 29 janvier 2002 n°260 FS-P+B Compagnie Préservatrice Foncière Assurance-Crédit Agricole.

- TGI Paris, 19 oct. 2004, Assoc. Les utilisateurs du cybercable, Comm. Com. Électr. 2005, no.9, note Luc Grynbaum.
- TGI Paris, 5 avr. 2005, UFC Que chisir c/ Tiscali.
- CA Rennes, 13 janv. 1992, d. 1993, somm. p. 54, obs. M. Vasseur ; JCP E 1993, Internet, 432, note C. Gavalda.
- CApp Lyon, 7 déc. 2001, no 1999/06589, Media Overseas c/Banque Populaire Loire et Lyonnais.
- Cass. 1ere Civ.13 février 1996, no. 09411726 et 94-12440: Bull. I, no. 84; 29 avr.1997: Bull. I, no. 132; 15 mai 2002: Bull. I, 132. 1
- Cass. 1ere Civ. 14 octobre 1997, no. 95-19609: Bull. I, no. 278.
- Cass. Com., 24 mars 1997, Brother, RJDA 1998, no.967
- TPI de Beyrouth, 13 juillet 1998 : RJL 1998, p.936.
- C. App de Paris, 10 février 1999, Estelle Hallyday c/ Valentin Lacambre : Gaz. Pal., 5-6 avril 2000, jur. P. 19 note Caron Ch.
- Tribunal Illinois, case no. 07 C 5387 – 21 Aout 2009 -: affaire Shames Yeakel vs. Citizen Financial Bank.
- CA Toulouse, 25 janvier 2001, FRS c/Société Actipole, JCP E 2001, p. 1001, note Le Tourneau (Ph).
- T. com. Paris, 5 mai 2004, Ste Peyre c/Société Silog, Expertises 2004, p. 278.
- Cass. Civ 2e, 8 avr.2004: Bull. Civ. 2004, II, n° 163.
- C. App Versailles 18 nov. 2010 Marie –Maure C. épouse A. c/SA Natixis Interépargne. Décision no. 09/06634.
- Cass. Civ. 1ere, 20 décembre 2012, no. 11-28202.
- Cass. Civ, Ch. com., arrêt du 18 janvier 2017- Crédit mutuel de Wattignies / M. X.
- Cass. Com., 20 septembre 2017, pourvoi n°16-14341
- Cass. Civ. Ch. Com. Fin. Et eco. , 28 mars 2018, pourvoi no. 16-20.018
- C. App. de Beyrouth, 19 juillet 2018, Pharaon c/ Crédit Libanais - non publié.

7. Sitographie

A

www.adil.org.lb
www.aub.edu.lb

B

www.banque-france.fr
www.bdl.gov.lb
www.botnets.fr

C

www.cnil.fr
www.courdecassation.fr
www.credoc.fr
www.cyberlex.org

D

www.droit-technologie.org

E

www.ecomleb.org
www.economie.gouv.fr
www.economy.gov.lb

F

www.fevad.com
www.finnet.jrc.it

G

www.gemalto.com

I

www.internetworldstats.com/stats.htm

L

www.lemonde.fr
www.legalis.net
www.legifrance.gouv.fr
www.lex-electronica.com
www.lexinter.net

O

www.onlinebankingreport.com

U

www.uncitral.org

V

www.volle.com

W

www.wipo.it
www.worldbank.org

Index Alphabétique

Les chiffres renvoient aux numéros de paragraphes.

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Table des matières