Revue Internationale du Chercheur
ISSN : 2726-5889
Volume 1 : Numéro 2

E-Banking: Legal Overview

E-Banking Aspect législatif

EL HILA Rachid
Enseignant chercheur
Ecole Supérieure de Technologie
Université Mohamed Premier - Oujda
Laboratoire de recherche en développement et management des entreprises et des organisations
Maroc
rac-elh@hotmail.fr

AZIZI Rachid
Doctorant
Ecole Supérieure de Technologie
Université Mohamed Premier - Oujda
Laboratoire de recherche en développement et management des entreprises et des organisations
Maroc
rachidazizi@gmail.com

Date de soumission : 11/04/2020

Date d'acceptation : 24/05/2020

Pour citer cet article :

EL HILA R. & AZIZI. R (2020) « E-Banking: Legal Overview », Revue Internationale du Chercheur « Volume 1 : Numéro 2» pp : 194 - 205

Digital Object Identifier : https://doi.org/10.5281/zenodo.3866376

Abstract

E-commerce involves not only banks and their customers, but also many third parties. The personal information detained by banks related to customers and their transactions change hands several times in the course of an electronic financial transaction. This information has to be protected by not only an institutional regulation but through an elaborated government law. The key challenge for e-banking is how to ensure proper legal protections for electronic financial transactions for both in local market and for cross-boarder transactions. The reliance on technology for the delivery channel of providing different electronic banking services is a considerable concern faced by regulators and e-banking supervisors. Indeed, the risks of data leakage and distortion are sufficiently high to warrant adequate legal and technical protection. An adequate Internet infrastructure as well as a legal and regulatory framework needs to be put in place by legal authorities in order to achieve an adequate sensitive information protection. This article attempts to highlight the importance of the legal aspect in electronic banking and to explore legal framework in force internationally and in Morocco particularly.

Keywords:

Electronic banking ; e-commerce ; e-contract ; legal aspects ; security.

Résumé

Le commerce électronique implique non seulement les banques et leurs clients, mais également de nombreux tiers. Les informations détenues par les banques par rapport aux clients, leurs transactions, changent de mains à plusieurs reprises. Il est impossible pour les banques de conserver des informations uniquement au sein de leurs propres réseaux informatiques, sans parler d'une juridiction unique. Le principal défi pour les services bancaires en ligne est d'assurer une protection juridique adéquate pour les transactions financières électroniques que ce soit sur le marché local ou pour les transactions international. Le recours à la technologie pour les différents services bancaires électroniques est une préoccupation considérable pour les autorités compétente les superviseurs des services bancaires électroniques. Les risques liés aux fuites, à la falsification ou au blocage des données sont suffisamment élevés pour justifier une protection juridique et technique adéquate. Mais pour en faire un succès, il faut plus qu'une infrastructure Internet adéquate. Un cadre juridique et réglementaire adéquat doit être mis en place. Cet article tente de souligner l'importance de l'aspect juridique dans les services bancaires électroniques et d'explorer les recours judiciaires possibles, en tenant compte du cadre juridique en vigueur à l'international et au Maroc en particulier.

Mots-clés:

Banque électronique, commerce électronique, contrat électronique ; aspects juridiques ; sécurité.

Introduction

Over the past two decades, the banking sector has invested heavily in the use of information technology. Growing global networks and rising incomes have pushed the banking sector to use new technologies to secure and maintain its strategic advantage. Electronic banking is one of the new ways used to perform financial activities using electronic technology. E-banking offers financial institutions the ability to meet different needs for customers in different locations. In recent years, due to the increasing use of information technologies and the Internet, banks and financial institutions started to elaborate more advanced and diverse services to their clients. Since the emergence of e-banking, serious problems started to come up that has to be addressed. Challenges facing the online banking system include financial and legal issues, culture and organizational process issues, infrastructure and information systems. One of the challenges facing the development of e-banking in Morocco is the legal ambiguity; that is, whether the general rules of contracts provide sufficient guarantees as to the validity of the electronic contracts. In fact, in the costumer point of view, risks are very high in the case of an electronic transfer and the Internet is a virtual world that opens wide doors to potential criminal acts. Risks in all its types (financial risk, security risk, performance risk, social risk, and legal risk) have to be addressed in order to maintain a trust relationship between the e-banking system and costumers. This paper will focus on one of the risks, which is the legal risk related to electronic transitions. It tries to provide a literature review of the legal challenges faced by the electronic banking system. Some of the questions that will be addressed are: what are the legal concerns for e-banking costumers? What are the legal arsenals available for costumers in case of a financial prejudice related to an electronic transaction?

This paper presents tree main points. It starts by providing an overview of the legal protection available for electronic banking which is a prerequisite for protected and secured electronic financial transactions. In the second point, a literature review of legal aspect at an international level is presented and enumerates treaties and cross-boarders bylaws available. The third and last point is an overview of the actual legal tools available in Morocco to secure the e-banking industry and then enhance trust between banks and their costumer.

1. E-banking and legal concerns

Financial institutions are in unprecedented race in order to conquer new sectors and customers using Internet in their trading for goods and services. Electronic commerce has created a genuine global market, which is developing with unquestionable potential. Aware of its power relations and its challenges on the digital economy, the legislator had no choice but to ensure the proper implementation of laws and regulations so as to maintain a solid relationship between all parties based on trust and mutual engagement.

In the same vein, the international community under the auspices of the United Nations has elaborated a directive on e-commerce. The main propose of this directive is give to the international market the proper assurance of online services offers, while respecting the country of origin's laws (G. D. ABI-RIZK, 2006).

In fact, financial institutions have the same legal obligations whether on traditional or electronic financial services. In addition, virtual financial transactions have an international connotation, which calls into question the lawsuit of e-banking which maybe poorly adapted to the traditional litigation resolution at the local level of each country. Thus, in order to have a win/win relation between the banking system and the Internet, it is for their best common interest in the emergence of new means of solving technical/legal problems.

The legislator should make e-banking consumers protection one of its priorities. In order to achieve that, a legal revolution is to be done to allow the dematerialization of contracts while preserving the same guarantees already granted to traditional contracts. A third party authority authorized by the legislator should manage the data exchange between parties related to electronic contracts. In this way, financial institutions will be able to demonstrate their good faith with the legislator and Internet customers by offering a reliable protection (G. D. ABI-RIZK, 2006).

The implementation of bylaws by legal authorities both at a local and international stage will definitely give the banking system a short and long term view in terms of security investment for their electronic banking systems. According to S. Chan (2011), "the level of security investment may depend on how government authorities regulate. If the law is more favorable to a bank when fraudulent transactions are disputed, the bank has less incentive to invest in

security. Vise versa, if the law is less favorable, the bank has stronger incentive." Government authorities have to give a transparent and viable legal arsenal to protect the e-banking system for all sorts of security issues.

2. Literature review: E-banking and Legal aspect at an international level

E-commerce has revolutionized the relationship between the economy and citizens rights. For a standard e-banking transaction, it is essential to enforce laws and regulations related to system rules and data processing and its storage in the banking system. Due to the absence of state laws, system rules must be defined by normative documents of the system owner and executed by all operators in the e-banking ecosystem. It has to specify the responsibilities of all parties, as well as the different types and levels of sanctions in case of rules violation.

Among the problems that slow the online banking development is the lack of a clear and efficient legislation to protect and secure an electronic commerce transactions. Any reliable security system will not work properly without a solid legal environment. Indeed, legal uncertainty is one of the biggest obstacles to e-banking.

Today, these legal standards have contributed to the development of a global and open market through the harmonization of laws governing relationships between all operators and the simplification of rules and procedures related to the e-banking sector. Never the less, there are still significant contradictions between the laws in different countries which represent a major obstacle to a seamless functioning of the online economy. In fact, the legal regulations for electronic commerce must combine the use of traditional basic legal norms and standards (such as the civil and criminal code) and the new dedicated legal procedures.
Some of the most important legal issues to be addressed by the international community include:

- Taxation of electronic transactions including rates;
- Prerequisites required for an electronic transaction;
- Standardization of cryptography;
- Authentication rules;
- Data protection;
- Protection of online consumer rights.

To build a relationship of trust between operators in the electronic banking system, appropriate solutions have to be elaborated for quarrelsome issues that may arise during financial transactions. Therefore, when developing a system for financial operations protection, an arbitration protocol must be put in place. Other elements have to be ensured such as professional arbitrators having access to protocols, rules and the legal status.
In most cases, it is not easy to win a legal dispute involving the legality and validity of an e-business financial document. This often gives rise to significant disagreements at the legal level. In particular, the provisions of such e-documents are often not legally binding during the trial, as the local laws of many countries give the parties the right to challenge the validity of the transaction due to the lack of a written document or a certified one by an authentic handwritten signature of the parties. That is, the success of e-commerce often finds obstacles because of the local legal specificities of each country.

Additionally, it is a challenge to effectively regulate the rights, duties and responsibilities of participants in "electronic transactions", especially third parties such as application service providers, Internet network services, and data warehouse services, etc.

To ensure an effective relationship between e-commerce companies in different countries, it is necessary to create by-laws models or "codes of conduct" for all operators in the digital economy. Therefore, countries where the legal system is based on case law (a court decision) have a greater capacity for self-regulation of e-commerce compared to countries that rely only on normative legal acts. Online businesses are often unable to overcome the legal obstacles due to the authority of national laws, that will requires significant effort and time to evolve because of change resistance.

To overcome these local jurisdictions inconsistencies, the United Nations Commission on International Trade Law has elaborated in 1996 an international legal tool for electronic commerce called by its name UNCITRAL Model Law. It is like a standard model with which a country can solve its major problems related to e-commerce legal issues in term of electronic contracts, signatures, originals/copies, data warehouses, and e-data recognition as legal proof. Indeed, this model stipulates what must be included in state legislation, procedures provided by the model law in case of electronic data transmission. The legislator

must create a neutral legal environment, without any advantage to any type of media used whether it is paper or electronic based.

The second international legal tool elaborated for regulating the electronic transactions is a directive of the European Parliament and the Council of 13 December 1999 on the European Union's policy on electronic signatures (UNCITRAL Model Law) [1]. This document creates the legal framework for using electronic signature (ES) in the European Union. The priority is to provide an ES with a viable legal value. According to Article 5 of the directive, European States that are part of an electronic transaction are required by law to recognize the authenticity of the electronic signature as evidence in a judicial proceeding. The directive also provides legal protection for electronic transactions. In particular, the contract cannot be invalidated solely on the grounds that it has been concluded via the Internet.

All these documents constitute the legal framework. They indicate guidelines for developing legal support, restrictions of legal instruction, but do not prescribe specific rules to be applied. The main purpose of these documents is to help each country's legislative institution to develop national legislation taking into account its comprehensive guidelines (R. J. Banerjee, 2018).

3. Legal aspect: Moroccan context

In Morocco, consumers are more and more using the electronic channel for their shopping. Economic actors had no choice but to prepare the digital tools necessary to have an exiting and safe environment for e-commerce experience. The government could not stay idle and let the digital wave goes by without taking any actions to modernization its administration by creating the program "e-gov" or e-government, which is the application of information and communication technologies (ICT) to all public administration procedures with the aim of increasing the efficiency, transparency and enhancing the participation of citizens to the public actions.

A climate of trust should thus be established between e-commerce users and economic operators to continue to use e-commerce, without having to worry about threats that could

[1] The Model Law on Electronic Commerce (MLEC),

compromise their personal data, or affect their online transaction, which should be considered as a legal act protected by a law.

In the same context, the Moroccan legislator has put in place a whole legal arsenal to establish a climate of trust in electronic financial transactions. It adopted the law n 07-03 promulgated by the dahir n 1-03-197 of 11 nov 2003 which complements the penal code by regulating the offenses relating to the data processing systems. To combat systems and data hacking, the legislators introduced the law No. 2-00 on copyright amended by Law No. 34-05.

Law no. 07-03 introduced sanctions against any crimes relating to electronic financial data processing. This law stipulates that the fact of gaining access fraudulently to an automated data processing system is punishable by six months to one year of imprisonment and from 5,000 to 20,000 dirhams of fine or only one of these two penalties.

The legislator intends to sanction all cases in which a person enters an automated data processing system. The fact is incriminated whether the access to the system is done physically or remotely, or the system is protected or not. Indeed, the mere fact of accessing without right an automated data system is considered as a crime. We are talking about a formal offense. The penalty is aggravated when access has caused system damage, such as alteration or data deletion. The penalty is thus increased to two years of imprisonment and from 50,000 to 500,000 dirhams of fine.

Article 607-4 of Law No. 07-03 stipulates that the obstructing or altering the operation of an automated data processing system shall be punishable by two to five years imprisonment and 50,000 to 1,000,000 dirhams of fine or one of these two penalties only. The term "obstructing" used refers primarily to any behavior that results in an obstruction of any automated data processing. This law also represses the act of "altering" the operation of the system by changing the system behavior in order to prevent a normal operation of an automated processing of data. Among the tools used by malicious people are "viruses" and "Trojans" which can be a normal file hiding malware that is usually used to take control of a user's computer, in order to steal or even to destroy the data and inject more malware into the victim's computer.

Another article (607-6) has strengthened the protection against "false ID and data" used to assimilates malicious data as authentic writing such as bank statements, contracts, letters, ect. This article stipulates that any kind of falsification of electronic documents, whatever their form, that are likely to cause harm to others, is punishable by imprisonment of two to ten years and a fine of 100,000 to 3,000,000 dirhams or one of these two sentences only.

With article 607-6, a traditional counterfeit is equivalent to an electronic one. Malicious users could thus be pursued for a fake in terms of electronic contracts. The same penalties are applicable for persons who use falsified data deliberately or not and they will be treated as if they were the main perpetrator of the falsifications.
The attempt to access confidential electronic data is also punishable under article 607-7 of the same penalties as the offense itself.

Concerning criminal association for electronic crimes, the legislator has introduced section 607-8 which states that anyone who has participated in an association or an agreement made for the purpose of preparation shall be punishable by the penalties provided for the offense itself. The main purpose of this section of the law is the criminalization of any act aiming at preparing for an offense such as "crackers", which are programs capable of recovering passwords or access codes in order to prepare an intrusion. Even the exchange of stolen passwords, the design of a virus intended to intrude a data base, and the delivery of bank cards to be re-encode are considered punishable offenses under this article.

As for detaining any materials that are likely to help committing a fraudulent act, article 607-10 came as a legal arsenal to help law enforcements in conducting their pursuit. In fact, any person that manufactures, acquires, holds, assigns, offers or provides equipment, instruments, computer programs or any data designed to commit the offenses provided for in this article is punished by imprisonment for two to five years and a fine of 50,000 to 2,000,000 dirhams.

The outcome of the materials used to commit these acts, article 607-11 gives the court the power to order the confiscation of materials used to commit the offenses. In addition, the guilty party may be prohibited to exercise their relative position for a period of two to ten years and the inability to perform any public function for a period of two to ten years as well as the publication of the decision of conviction may also be pronounced.

The texts of Law No. 07-03 presented in addition to the Penal Code with regard to offenses relating to automated data processing systems are a guarantee of protection for individuals and institutions, but they are not sufficient. Certainly, this legal framework is very desirable, but an international solution implementing protection tools and common laws has to be elaborated. Attacks on computer systems can be initiated from anywhere on the globe. It is for this reason that it is desirable to have common procedures to allow the investigating judge to extend the inquiry into interconnected computer systems located in several countries given the international nature of many computer networks. Moreover, it is not easy to administer a proof of an offense of intrusion since it was carried out from an open network located in another country, not to mention the difficult task to identify of the responsible person. It is clear that on the legal aspect, the work is far from done.

4. Managerial Involvement

At the managerial level, this paper shows to bank managers and government representatives the importance of the establishment of legal certainty in the e-banking systems. In fact the growth of electronic financials transactions depends on both technological advances and consumers confidence. This bank/consumers trust relationship has to be reinforced through not only a secure technological environment but also through a sound legal framework. Bank managers needs to legal aspects play an important role in e-banking evolution as far as the need to enhance costumer trust in the offered services is concerned.

Conclusion

Globalization and technological advances are imposing new challenges for legislators around the world. Among them, there is the fact that electronic commerce has become indeed new transformative force on global trade and local regulations lack harmony and suffers with many disparities in terms of legislative aspects. However, e-commerce tools put in place are able to handle almost all e-commerce issues in a secure manner and maintaining a high degree of users satisfaction.

Unfortunately, legislation of many countries is lagging behind the electronic revolution. Morocco is one of these countries. To benefit from the new global trade, it is necessary for Morocco to provide electronic banks and e-commerce users with a legal framework to become operationally and commercially viable.

It is high time for government representatives to discuss on a common ground so as to unify their legal means to address all legal uncertainties involving e-banking ecosystem both locally and internationally. Meanwhile, academic researches on the subject are highly recommended to address the potential influence of legal aspect in e-banking adoption. In other words, does legal certainty or uncertainty influence the intention of customer to adopt e-banking use in their financial transactions? Is law enforcement by legislators regarding e-banking will affect costumer relationship with e-banking?

BIBLIOGRAPHIE

Abi-Rizk, D.G. (2006). « L'Internet au service des opérations bancaires et financières », Thèse de Doctorat, Pantheon-Assas University (Paris II), 174-176

Banerjee, R. J. (2015). « Legal aspects of electronic banking services », Source: https://booksforstudy.com/16631116/bankivska_sprava/pravovi_aspekti_bankivskih_elektronnih_poslug.htm , consulted Septembre, 10th 2018

Chun S.H. (2011). "Smart Mobile Banking and Its Security Issues: From the Perspectives of the Legal Liability and Security Investment". Communications in Computer and Information Science, vol 184. Springer-Verlag.

Code Pénal, (2012). « Loi n° 2-00 relative aux droits d'auteur et droits voisins », BO, Secretariat Générale du Gouvernement, Source:

www.sgg.gov.ma/portals/0/AvantProjet/22/Avprojet_droit-auteur_Fr.pdf, consulted on April, 10th, 2019.

Code Pénal, (2004), "Infraction relatives aux systèmes de traitement automatisé des données", BO, Source: www.sgg.gov.ma/BO/Fr/2004/BO_5184_Fr.pdf, consulted April 10th 2019.

Code Pénal, (2000), BO, Secretariat Générale du Gouvernement, Source: www.egov.ma/sites/default/files/loi_ndeg07-03_code_penal.pdf, consulted on April, 10th, 2019.

OCDE, (2004), « L'OCDE demande aux gouvernements d'intensifier leur lutte contre le spam». Source : www.oecd.org/document/38/0,3343,fr_21571361_34590630_26505574_1_1_1_1,00.html, consulted April, 10th 2019.

Pierrotin, I.F. (2009). «Le Forum des droits sur l'internet », Direction de l'information légale et administrative, La documentation Française. 46-50.

NCOI, (1996), Trade Law, "The Model Law on Electronic Commerce (MLEC)", Source: www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html, consulted on April 9th, 2019.

Treaty Doc. 108-11, "Council of Europe Convention on Cybercrime", Nov 23, 2001.