Journal of Namibian Studies, 33 S2(2023): 4596–4606 ISSN: 2197-5523 (online)

Legislative Controls Securing Electronic Payment Systems

Dr. Chikh Nassima[1], Dr. Ahmad Mahmoud Masadeh[2]

[1]Lecturer "A" at the faculty of Law, Belhadj Bouchaib University -Ain Temouchent, Algeria, Nassima.chikh@univ-temouchent.edu.dz

[2]Associate Professor of Private Law-Amman Arab University-Faculty of Law, Jordan, Amasaadeh10@gmail.com

Abstract

Generally, money is the backbone of economy, essential for stability of countries, and a token for the national Sovereignty. Historically, coinage was the process by which countries were confirming their Sovereignty that they kept protecting it and used the coins as acceptable method for transactions. In the modern age with the far-reaching technological development, the digital payment has become widely acceptable and commonly used thereby the sort of security required has alo changed. Many countries enacted new laws to enhance security of the electronic payments, particularly with the increased risks of cyber attacks on the national economies in addition to recent pandemic and military tensions witnessed by the world.

Therefore, securing the electronic payment is a matter of national economy due to its influence on the Citizenery's trust in the electronic transactions and the government is responsible to make it secure through the central bank. Considering this perceived importance, the authors addressed in the current study the legal mechanisms to secure the electronic payment systems.

Keywords: Electronic Payment, National Sovereignty, National Economy, Central Bank, Electronic Authentication, Money.

Introduction

The massive use of the electronic transactions has resulted in development of intricate relationships between the public community and the electronic commerce virtual community in unprecedented ways. This new reality necessitated invention technical and law modalities to tackle with any arising problems. One of the major mechanisms is to fulfil the obligations arising from the electronic transactions.

The interaction with the electronic environment and for prompt response to finalise the electronic transactions, electronic payment and money transfer methods have evolved until became the basis of making

payments against obligations arising from such transactions. Legislations in different countries were alert to regulate such methods like the Algerian and Jordanian legislations that enacted independent regulations on the electronic payment and electronic transfer of funds .

As the electronic payment still developing from the technical and law aspects, the electronic financial transactions continues a desirable target for the cyber attacks and electronic criminals due to wealthy gains in the same time such attacks for serious threat of the national economy and the national security as.

The foregoing discussion highlights the significance of demonstrating the mechanisms applied to secure the electronic payments due to association with both the national economy and national security, taking into account that misuse of the electronic payment compromise trust in stability and security of a country.

Since this topic is multidimensional, our study will address only the legal means to secure the electronic payment as part of the banking law, and the military and security dimensions will be disregarded.

So, the problem addressed by the current study can phrased in the following questions: “What are the most prominent legal mechanisms to secure the electronic payment systems as novel payment methods in the electronic commerce, and how effective are they?”.

To answer this question, this study was of two parts. Part one discussed the transition from coinage process as a token of the national sovereign to safe electronic payment in securing the national security. Part two discussed the legal mechanisms related to securing the electronic payment systems.

Part One: Transition from Coinage Process as a Token of National sovereignty to Safe Electronic Payment in Securing the National Security

Money considered the backbone of the economy and a token for the country’s sovereignty because through its institution it make and manage the coins.

The government takes careful measures to protect methods used in moving and storage of the coins. In this modern age that characterized with the electronic payment, the dealing in coins and banknotes has been minimized.

Section One: The Need for Secure Dealing in Currency

Transition of currency requires sufficient protection measures, especially that currency represent a form of national sovereignty token.

First Subsection: Coinage as a Token of the National Sovereignty

Almost all countries in the world practice coinage for their own currency to express their national sovereignty . The coins and banknotes

take their value from the trust in the issuing state. The currency is a means of exchange and measure of value and method of fulfilling debts. It is the responsibility of the state to protect the currency by criminalizing the act of stealing money or forgery and securing the process of moving money from one person to another or from an account to another.

The idea of a state as an independent entity has originally emerged from the human need for protection, security and stability. The state, as a result, shall protect individuals from any assault or breach in return that they have the right to levy taxes and enforce law. Also, coinage process is viewed within this field as the state makes coinage of the currency used and protect transactions and dealings in terms of stability. The national currency has the power of discharge, and serve as storage of value because all are trust in such currency because it is issued by the state and acceptable in the transactions and levy taxes. The state also provide protection to moneys for forgery and infringement. In addition, there is another form of protection offered by the state related to monopoly of practicing the banking activities thereby monopolizing an important function i.e. providing for payment methods and management.

The wide use of the electronic transactions and electronic payment refers to its perceived advantages that eliminated the need to carry material money and quick implantation of the electronic transactions. Studies indicate that using the electronic coins has positive benefits on the national economy and improved performance of banks , so the intervention by the legislator was necessary with a number of mechanisms to provide for secure electronic payment.

Second Subsection: Significance of Securing the Electronic Transactions and electronic Payments

The current reality reveals that the electronic transactions, including the electronic payment has become prone to novel kinds of crimes that accompanied the emergence of the technological advances. So, the personal life of individual became exposed to danger. For instance, there is assault on the privacy of individuals including privacy of content stored on personal computers and mobiles in order to steal their personal photos and professional information to achieve different intentions like blackmail, defame one’s reputation, or resell their personal data. These acts form a basis of infringement of the personal privacy and freedom; hence they threaten one’s dignity and personal life and increase instability, distrust and insecurity.

If we considered the state’s role, one can see that it is the responsibility of the state to create security for its citizenry. On this basis, the state exerts great efforts to provide security for its citizens from any infringes or assaults might occur virtually.

There are many types of crimes that tremendously hazardous on both the individual citizens and the community as a whole and also affect the stability of the state. These crimes become more risky if associated with the electronic payment processes. If the assault occurred in one process to an individual this crime will form violation of right of a person and so intervention is easy, but the reality reveals that the attacks on the electronic payment systems usually are launched by organized groups of "pirates" aiming at big loot, whether in form of gaining huge money amounts or break down the system itself, which forms threat of the national economy.

Second Section: Relationship of National Security with Electronic Terrorism

The cyber-attacks no matter what form it takes has become seen a threat to national security and maybe classified among electronic terrorist acts.

First Subsection: National Security

Historically, countries have long protected its geographical borders from a foreign invasion, and tackled threats to internal security using classical measures to preserve its existence and stability. Another way to preserve the national security was by making international allies and bilateral agreements to protect against dangers. For instance, the European countries on the Mediterranean consider protection of its security as extending to the coast countries and start dealing with offshore threats even in the African countries in order to make sure the threats, if any, not reaching its territories.

One can say that the national security has many dimensions including the political, economic, military and social dimensions , but today the concept of national security has greatly developed especially in its economic dimension due to association with the electronic financial transaction, particularly electronic payment.

Second Subsection: Concept of Electronic Terrorism

The concept of electronic terrorism is relatively new that there is no commonly agreed upon definition of it. It forms a new form of warfare that uses none classical weapons in terms of exploitation of any informatics gap in the civil or military structures that threatens the national and global security. The result of such acts is violence, destruction and spread of fear among public users causing confusion and distrust and gives lip service to some political, social or intellectual agenda . The research considers the threats related to informatics and cyber security as the highest challenge of today .

Terrorism was defined in 2002 by the EU as "acts committed for purpose of making people terror, or force a government or international organization to do or not to do an act, or destroy essential political,

constitutional, economic, or social structures of a state or international organization or having it destabilised" .

Part Two: Legal Mechanisms for Securing Electronic Payment

Recently, many novel statutes have been introduced on the national, regional and international levels , all of which aim at securing the electronic payment systems. For instance, the Algerian and Tunisian legislations were introduced to organize the electronic transactions as well as the Jordanian legislation . However, the national efforts inadequate alone to secure the electronic payment systems and the international collaboration in this field is paramount because dealing with digital coins which has become widely spread is highly risky.

First Section: Legal Framework for Electronic Payment

In light of the earlier discussion of the statutes and regulations related to electronic payments, we need to highlight the concept of electronic payment before addressing the legal modalities for safeguarding (First Item) some of which are related to texts and rules related to securing electronic payment (second Item) and some others are related to the role of the banking system in securing electronic payment (Third Item).

First Subsection: Concept of Electronic Payment

Article two of the Jordanian Regulations of Electronic Payment and Transfer of Funds defined the electronic payment as "a set of programs and tools prepared for make payments, settlement, and transfer of funds electronically approved by the central bank" .

In light of this definition, it becomes clear that electronic payment system is one of the electronic methods designed to settle down the financial obligations electronically using computer software programs made for this purpose in particular in order to fit with the electronic environment and the electronic commerce. This context leads us to define the electronic transfer of funds that closely associates with the electronic payment. The second article of the Regulations of Electronic Payment and Electronic Transfer of Funds provides that "transfer funds from the sender to the beneficiary via electronic means licensed or approved by the central bank". So, the electronic transfer of funds has become a system on which daily bank processes are based when dealing with customers. Based on this system, the transfer of funds process commence with a person designated as "sender" to another person designated "the beneficiary". The banks are dealing with the electronic methods to finish the electronic transfer of funds process , where the electronic transfer of funds is considered one of simplest and low cost operations of settling debts and finish transactions.

Second Subsection: Rules to Secure Electronic Payments

There are many legal texts phrased in framework of securing the electronic transactions and electronic payment, most importantly acknowledgement of cogency of the electronic signature by amending the civil law to commensurate with the digitization requirements. Thereby, the electronic signature acquired cogency of proof based on the provision of article 323 repeated and article 323 repeated of the civil law . The Algerian legislator invented special rules to secure the crimes related to IT & Communication crimes . To that end, the modernized justice statute was enacted in 2015 .

Further, the Algerian legislator enacted new laws, most importantly the statute determining general rules governing electronic signature and authentication . However, some of the prominent mechanisms were the introduction of the authentication certificate , the national authority of electronic authenticatio , the governmental authority of electronic authentication , the economic authority of electronic authentication , and electronic authentication service provider .

The statute no. 18-05 on the Electronic Commerce , the Algerian legislator provided for a number of rules as to secure electronic payment, particularly in terms of subjection to the central bank's authority as discussed below.

In Jordan, the legislator issued the Electronic Crimes Act no. 27 of 2015 which stated in its seventh article on transfer funds through a website or a information system that: "Whoever practices one of the acts specified in article (3), (4), (5) and (6) of this law, if affected an information system, website, or electronic network of transferring funds, electronic payment, settlement or any banking services provided by banks or financial institutions shall be sentenced by temporary penal labour for a period no less than five years in prison or a fine of no less than (JD5,000.00) but not more than (JD10,000.000).

In this context, it is worth to note that the Jordanian Electronic Transactions Law ensured confidentiality of the electronic commercial transactions by keeping secrecy of the electronic transaction between parties. So, it is prohibited by law to disclose customer secrets by the authenticating party or misuse the data available in hand for any other purpose that the authentication purpose. In fact, the Jordanian legislator obliged the authenticating party to strictly abide with confidentiality of information requirement. To ensure established rules of electronic commercial transactions, the Jordanian legislator obliged the authenticating party to refrain from issuing authentication certificates before making sure of the soundness of the operation procedures of the authentication system. The authenticating party is also required to promptly inform the Communications Sector Regulatory Commission and customers if the authentication system has become insecure.

Third Subsection: The Role of the Banking System in Securing Electronic Payment

The Algerian legislator provided special texts related to safeguarding electronic payment, basically the statute 05-18 addressed the electronic commerce, and its subjection to the central bank's control taking into consideration the fact that the electronic payment systems and management are monopolized by the banks.

First: Banking Monopoly of Electronic Payment Systems and Management

Generally, banks exercise their activities with a sort of monopoly in that the original banking processes including offering methods of payment to clients and management are not allowed but to banks .

The Electronic Commerce Act no. 18-05 provided that payments should be made through licensed systems, and that the electronic payment should be made through designated portals, and be created and invested exclusively by the banks or the Algerian post only.

Second: Subjection of Electronic Payment to Central Bank's Control

To enhance security of the electronic payment processes, the Algerian legislator subjected electronic payment platforms created and operated by banks to the control of Bank of Algeria. The same attitude was adopted by the Jordanian legislator where the article four of the Jordanian electronic payment system provided that: "Considered part of the payment methods any electronic method approved by the central bank enabling user to perform electronic payment or transfer of funds electronically as follows:

- Prepaid Cards: issued by a bank or a licensed electronic payment service provider to customers charged by funds.

- Credit Cards: issued by a bank or a licensed electronic payment service provider to customers without s funds in the customer's account.

- Debit Cards: issued by a bank to customers on the condition of availability of funds in the customers' account.

The import is that the electronic payment instruments are subjected to instructions of the Central Bank of Jordan and comply with the confidentiality and safety of transactions requirement, and conform with the requirement related to unity of the controlling bodies and facilitation of the control process.

The subjection of electronic payment to central bank's control is reasonable due to perceived technical experience and qualified personnel that are able to lead the process, and on the other hand the central bank possesses established relations with the banks and the bourse and different governmental authorities. Ultimately, the central

bank exercises the control on behalf of the government which further strengthens trust in the banking system. However, such trust remains fragile without accomplishing positive results in order for a central bank to keep the trust of the public in its procedures .

So, enhancing the central bank's controlling role on the electronic payment processes considered paramount especially that the reality provides significant evidence that huge financial crises would not be resolved without intervention from the government and the central bank. The global financial crisis in 2008 gives an important lesson. However, there are some economists who call for complete freedom of money transfer; particularly the electronic moneys i.e. ensuring the digital moneys are subjected to no control by the government or its authorities. The proponents even considered the digital moneys as 'Monnaie privé' including 'bitcoin'which is suspicious as being used in money laundry and financing terrorism .

Fourth Subsection: Anticipated Problems

However, huge the law legislations to secure the electronic payment system and advanced technology available for continual improvement, it is difficult to create comprehensive security of the electronic payment, especially if we knew that there are continual attacks to break into the various platforms. So, careful measure should be taken because all platforms are connected to the internet, and attackers usually are technologically experts, or belong to organized groups with huge capabilities to even to countries targeting other countries .

On the other hand, there is a problem related to protect rights and freedoms. Banks, including the central bank, that collect large amount of personal data of their customers, account owners and electronic payment process are in a position of potential breach of individual's privacy, freedoms and rights. Proponents of the economic freedom consider the free electronic payment is the safest form that complies with personal freedom and justice. In this context, "Milton Fridman", 1999, predicted that digitization will become a superpower on the expense of governments . On the other hand, the opponents consider that the existence of payment system controlled by private providers unorganized by law would highly risky .

Second Suction: International Collaboration in Securing Electronic Payment

Because of the importance of securing electronic payment along with safeguarding electronic transactions and ensuring cyber security, the world countries are seeking to collaborate internationally to accomplish such goals. For example, in 2013 Tallinn Manual was written by an expert group in the international law at the invitation of the NATO for purpose of addressing the issue of how to interpret the humanitarian

international law rules in the context of cyber warfare, in addition to other bilateral and collective agreements and efforts.

Conclusion:

Despite the perceived interest in the electronic payment processes it remains relatively unsafe process considering the cyber attacks by hackers and terrorist cyber attackers. Knowing how large amount of moneys targeted by pirates or even destruction the electronic payment system itself, one can imagine the associated hazards. So, the state should take careful measures to enhance the safety of the electronic payment systems as consider it a national priority because it relates to protection of the national economy and the sovereignty of the state and national security taking into account that the first quarter of the 21st century has witnessed a global health crisis compromised the national income of giant states in addition to the impact of the Russian Ukraine war embarked in March 2022 which disclosed fragility of the world system and reaffirmed the need to depend on national capabilities.

Based on the earlier, we suggest the following:

- The Central Bank shall through the Council of Money and Loan issue regulations that comply with the requirements of security and prompt for electronic payment users.

- Banks are encouraged to develop banking products and services using electronic payment systems in order to attract more clients with greatest level of service satisfaction.

- Banks are called to diversify their methods of payment so that to commensurate with the clients' expectations.

- Enhance security from logistic aspects by recruiting qualified human resources; provide them with continual training and incentives to ensure retention.

- The Central Bank shall enhance transparency regarding electronic payment systems by generating data through its digital platforms on periodic basis.

- Contest application process by the clients regarding arising problems encountered with electronic payment shall be facilitated and resolve such problems as prompt as possible.

- Interrelations between the national and foreign central banks and other institutions active in the field ensuring security of electronic payment systems should be enhanced and strengthened.

Bibliography

First: References in Arabic

1. Dr. Obeidat, Ibrahim Mohammad. Electronic Commerce Legislations, Dar al-Thaqafa Publishers and Distributors, Amman-Jordan, 2021.
2. Al-Qalyubi, Samiha. Commentary of the Egyptian Law of Commerce, Dar al-Nahda al-Arabiya, Edition 3, Part 2, 2000.
3. Shaker, al-Quzweni, Lectures on Banking Economy, University Publication Diwan, 4th edition, Algeria, 2008.
4. Subhi, Tadrus; Qarisa, Ahmad Ramadan Nimatullah. Economies of Moneys and Banks, University House, Beirut, 1990.
5. Slaiha Mohammad and Shafia Hadad, Electronic Terrorism and National Security of a State: New Pattern and Different Threats, Algerian Journal of Security and Development, Journal 8, Issue 15, July 2019.
6. Lamia, Tala. Cyber Threats and Crimes and Impact on the National Security of a State and Combat Strategies, Maalem Journal of Law and Politics Studies, Journal 4, Issue 2,2020.
7. Kahina Racham, Controls by Central Bank to Regulate Electronic Payment Transactions and Reality of Banking Cards in Algeria, International Journal of Economic Performance, Journal 4, Issue 1, 2021.

Second : International References

1. Philippe Rodriguez, La révolution de la Blockchain : algorithmes ou institutions à qui donnez-vous votre confiance ? édDunod, France, 2018.
2. Gilbert BOUGI et Helmi HAMDI, La crédibilité de la banque centrale face aux défis de la monnaie électronique.

www.researchegate.net/publication/254398648.

3. Michel Aglietta et Laurence Scialom, Les défis de la monnaie électronique pour les banques centrales, revue d'Economie politique, 2002/2, N° 2014.
4. Michel Aglietta et Natacha Valla, La souveraineté de la monnaie et ses transformations historique : l'invention de la monnaie digitale de banque centrale au XXI siècle et ses conséquences géopolitiques, Revue d'Economie financière, France, N° 144 , mars 2022.

Third: Laws and Regulations

1. Statute no. 05-10 dated June 20, 2005 Amended Civil Law 9Official Gazzete, Issue 44, dated June 28, 2005).
2. Act no. 09-04 dated August 05, 2009 on the Rules Safeguarding from IT & Communications Crimes and Combat (Official Gazette, Issue 47 dated August 16, 2009).
3. Act no. 15-03 dated February 01, 2015 on Modernisation of Justice (Official Gazette no. 06 dated February 10, 2015).
4. Act no. 15-04 Determinants of General Rules of Electronic Signature and Authentication dated February 01, 2015 (Official Gazette, no. 6 dated February 01, 2015 (Official Gazette, no. 6 issued on February 10, 2015).
5. Act no. 18-05 dated May 10, 2018 on Electronic Commerce (Official Gazette no. 28, issued May 16, 2018).
6. Mandate no. 03-11 on Money and Loans dated August 26, 2003 as Amended (Official Gazette, no. 52 issued on August 27, 2003.
7. Legislative Decree no. 93-10dated May 23, 1993 on Money Transfer Bourse (Official Gazette, no. 34 issued on May 23, 1993).

8. Electronic Payment and Transfer Regulations no. 111 of 2017.
9. Electronic Crimes Act no. 27 of 2015.
10. Regulation on Licensing and Accreditation of Electronic Authentication Providers no. 11 of 2014.
11. Jordanian Electronic Transactions no. 15 of 2015.
12. Model Law of Electronic Commerce issued pursuant to UN Resolution no. 85 of 1966.