THE COMPARATIVE ANALYSIS OF LEGAL REGULATIONS PERTAINING TO DIGITAL AUTHENTICATION EU

Mohammad AL ANIMAT[*]

ABSTRACT: *The electronic signature is a matter of trust in the ownership of the signature for the owner, and it may be difficult for the other contracting party to verify its authenticity, hence the importance of dealing with and organizing the digital signature, and the aim of this study is to; we need to compare the legislation between EU and Jordan in the legislation governing the responsibility of the authentication service provider for the electronic signature, to find out whether there is a lack of organization legislation with regard to the work of the electronic signature service providers, and the article examines the adequacy of general regulations in supervising and supervising the duties of electronic service providers in Jordanian law, emphasizing the importance of establishing specific regulations, and the need to establish special rules in this particular responsibility, especially with regard to the development of specific rules in line with the uncitral model law on electronic signatures. As well as the EU directives on electronic signatures and many international legislations.*

KEYWORDS: *electronic banking; security; digital; certificate; authentication*.
JEL Code: *K22, K34.*

1. INTRODUCTION

The countries are increasingly interested in preparing and issuing legislation that ensures the creation of the legal infrastructure for e-commerce and the removal of obstacles to its prosperity in a manner that ensures the enhancement of confidence in transactions that take place over the internet by ensuring safe methods for verifying the identity of the contractors, as well as ensuring the security of information transmission, in a virtual world surrounded by a set of considerations related to the security and safety of electronic transactions, the need to provide the greatest degree of confidence in these transactions arose, this is represented in particular by the need to verify the validity of these contracts and their issuance by whom they are attributed, for this reason, writing and electronic signature have emerged as tools that are consistent with the nature of electronic transactions, the electronic signature has formed one of the most prominent components of electronic commerce, many forms of this signature have emerged, such as the electronic pen signature and biometric signature[1], but resort to signature it goes beyond the problems

[*] PhD - Candidate, University of Debrecen, Géza Marton" Doctoral School of Legal Studies, HUNGARY.

[1] For a review of the concept and effects of a digital signature and a certificate of authenticity, see Musaed A., *Digital Signature and Certificate of Authenticity: Concept and Legal Implications*, "Al-Manara Journal - Al al-

that would have been caused by the use of ordinary writing the electronic one raises the issue of confidence in the attribution of this signature to its owner, and thus in the electronic transaction in general, as it may be difficult for the other contracting party to verify the authenticity of this signature and to attribute it to its owner. This highlights the need for a neutral and trusted party to be the link in this field between the sender and the addressee. Hence the importance of dealing with the digital signature and the existence of a system[2], is to verify the authenticity of the digital signature and attribute it to its owner, electronic authentication is the system in which the electronic authentication service provider issues an electronic certificate that includes elements and data specified in the law that ensures the validity of the digital signature and guarantees its attribution to its owner, through which the authentication authority verifies the integrity and validity of the data contained in this certificate in a manner that gives third parties confidence in the integrity of the transaction that he submits.

This task was undertaken by the electronic authentication service providers, who play the role of mediator between the parties and are subject to a special legal system whose provisions are regulated by special rules in electronic commerce's electronic transaction laws in many countries such as Britain and France. Furthermore, the Jordanian electronic transactions law did not explain how to grant the electronic certificate In a clear, precise and detailed law, this justifies the importance of this study, as it comes in an attempt to shed light on the shortcoming contained in the Jordanian electronic transactions law and to try to find appropriate solutions, to this problem, by using the texts of comparative legislation that had previously organized the topic accurately, the complexity involved in proving the traditional conditions of liability prompted the legislators of many states to have to regulate them with special provisions, The study is one of the recent studies that have not been written about previously. I researched the writings and articles that scholars have discussed in the past. This topic was not discussed, especially in Jordan, the development of the law in the legal legislation, and this is one of the difficulties and challenges that I faced, so I relied on comparison with international legislation, analyzing it, and obtaining a clear picture of the subsequent needs, and the EU legislator was alerted to the need to intervene to regulate the electronic authentication process and the responsibility resulting from it, given the role this process plays in facilitating and flourishing electronic commerce[3], then the French legislator came to be in harmony with the EU directive, and regulate this process with the trust law[4], which established a special

Bayt University". Vol. 11, No. 4, p. 249, 2005, and see also online for more information on. pp 66-58, 2004, London, well Max and Sweet *» Regulations and the Law: Electronic Signatures*., & Brazell L., Rice P., *Electronic Evidence Development and Evidence*, "American Bar Association publication". 2008.pp11.

[2] Hassan L., *Electronic Documentation and the Responsibility of the Competent Authorities*, Dar Al-Raya for Publishing and Distribution, Amman, 2009, p. 101. & Al-Jammal S., *Contracting through Modern Communication Techniques*, Dar Al-Nahda Al-Arabiya, Cairo, 2006, pg. 321. & Al-Sabaheen S., *electronic* signature and its authority in proof, unpublished PhD thesis, Amman Arab University for Graduate Studies, Jordan, 2005, p. 156.& BRUN M., *Nature et impacts juridiques de la certification dans le commerce électronique sur Internet, Mars* 2000, more information see, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf (accessed 25 January 2023).

[3] Caprioli E, *La directive européenne n 1999/93/ 13 décembre 1999 sur un cadre communautaire pour les signature électronique*, Gaz. Pal, October 2000. https://www.caprioli-ts.com/migration/pdf/signature_confiance_signelec.pdf (accessed 27 January 2023).

[4] Le Tourneau P, *Contrats du numérique 2022/23 12ed - Informatiques et électroniques Relié* – Livre grand format, 2022.pp39.

responsibility for electronic authentication service providers in the official economy for the year 2004, inspired by its provisions from the texts of the EU directive.

In this regard, it must be emphasized that the issue of electronic authentication services raises many legal problems that can be resolved by special texts. For example, the legal nature of the liability of electronic authentication service providers, its legal basis, and the cases of its establishment are still subject to jurisprudential controversy. In addition to the scope of this liability and the issue of determining the extent of compensation that can be imposed in the event of damages to the customer or third parties, because the Jordanian legislator did not set up Specific a legal system for the responsibility of the electronic authentication provider to explained all the ambiguities, the importance of this study emerged in an attempt to demonstrate the adequacy of the general provisions on liability to cover the liability cases of the electronic authentication provider, and whether there is a need for the Jordanian legislator to adopt rules for the liability of electronic authentication service providers.

2. METHODOLOGY AND DATA USED

This article is built on the comparative-analytical approach that aims to facilitate access to facts as it was used to analyze the principles of digital signature related to the topic of research, by discussing the methods currently used in electronic financial operations and some examples of judicial rulings from the EU court of justice and responsibility towards electronic banks and recommendations of the EU directive in this regard, and the regulations and instructions of Jordanian transaction law about the principles of electronic digital signature and methods of cyber adaptation and some important conclusions in the uncitral model law on electronic commerce and related laws issued by UN.

In this article, the definition of the scope of responsibility and the issue of determining the extent of compensation that can be imposed in the event of damages to the customer or to third parties appear, because the Jordanian legislator did not set a specific legal system for the responsibility of the third party. Electronic authentication provider to explain all the ambiguities, the importance of this study emerged in an attempt to prove the adequacy of the general provisions of liability to cover liability issues for the electronic authentication provider, and whether there is a need for the Jordanian legislator to adopt rules for the liability of electronic authentication service providers, all of these areas will be dealt with through the following;

THE LEGAL FRAMEWORK FOR THE RESPONSIBILITY OF THE ELECTRONIC DOCUMENTATION SERVICE PROVIDER

The Jordanian legislation in the electronic transactions law did not address the civil liability of documentation service providers, because the Jordanian legislator did not regulate the subject with special texts[5]. Rather, the regulations were limited to electronic systems and imposed financial penalties and fines for providing false data, as a result, it was necessary to resort to general rules to determine the legal liability of the electronic documentation service provider.

[5] Article 25, of the Jordanian Transactions Law No. (15) of 2015.

However, the EU legislation affected by the EU directive on electronic signatures has adopted a system of responsibility for electronic authentication providers[6], and this prompts us to study the most important features of this system in an attempt to push the Jordanian legislator to consider this legislation and follow his approach in developing special texts to regulate the legal liability of authentication service providers in Jordan, It also raises the question about the nature of the responsibility arising from the electronic authentication process and its legal basis in terms of including it within the framework of contractual responsibility based on the provider's breach of the electronic authentication contract that binds it to the customer who obtained the certificate or including it within the scope of the default nature of that responsibility based on the provider's breach of the imposed legal obligations, according to the legislation that regulated the electronic authentication process. Therefore, we address the question of the legal nature of the liability of the electronic documentation service provider, what can be said here is that the specificity of the electronic authentication process and the complexity of the relationships resulting from the issuance of the electronic certificate justify the possibility of envisioning several assumptions of responsibility arising from electronic authentication services, so that the contractual responsibility of the responsible party of the provider towards the certificate holder and the hypothetical responsibility of the provider towards others can be imagined.[7]

There is a relationship between the provider of electronic authentication services and the holder of the certificate regulated by the electronic authentication contract. There is also a relationship between the provider and third parties who rely on the electronic authentication certificate to conclude some actions[8]. There is the relationship between the holder of the certificate and others, which is centred on a contract that they wish to conclude, and which is the subject of providing specific goods or services[9]. This raises the question of responsibility arising from all of these for the damages that result from a defect in the electronic documentation process, is the provider responsible, or is it possible to imagine the liability of the client holding the certificate and is it possible to envisage exempting the provider from liability or limiting it.

3. THE CONTRACTUAL FRAMEWORK FOR THE SERVICE PROVIDER

It is understood that contractual liability arises from the occurrence of damage resulting from the debtor's breach of an obligation resulting from the availed contract this breach is either the debtor's failure to perform his obligations or an existing and valid contract, so the client who owns the certificate of authenticity may suffer defective implementation or even delay fully or partially in implementation, and the application of damages as a result

[6] Directive 93/13/EEC protects consumers in the EU from unfair terms and is amended by Directive (EU) 2019/2161

[7] Sarhan A., Khater N., *Sources Of Personal Rights*. "Dar Al Thaqafa For Publishing And Distribution".2021, pp. 302.

[8] Mell, p& dray j., & shook, j, *smart contract federated identity management without third party authentication services*, Bonn, pp15, 2019.

[9] Lim, SY, Fotsing, PT, Almasri, A, Musa, O, Kiah, MLM, Ang, TF & Ismail, R, *'Blockchain technology the identity management and authentication service disruptor: A survey'*, "International Journal on Advanced Science, Engineering and Information Technology". Malaysia, 2018, vol. 8, no. 4-2, pp. 1735-1745.

of a breach by the authentication services provider of one of his obligations under the authentication contract concluded between them or under the text of the law,[10] where the authentication provider and the client holding the certificate have the right to set what is required if a provider breaches, they want reciprocal terms and obligations according to the principle of contractual freedom and the authority if the provider of documentation services[11], or the client, undertakes one of these obligations, their contractual responsibility is held by issuing an inaccurate to this client[12]. And at the same time, contractual responsibility arises, as the electronic authentication contract imposes mutual obligations on both parties, and any breach by the provider or the certificate holder of the obligations incumbent on each of them assesses his contractual responsibility. It is often mentioned in this contract that the provider is obligated to confirm the validity of the data contained in the certificate and verify with the contracting parties, if it is attributed to the owner of the electronic signature, even if it is not determined by a special provision in the law, this is because this commitment constitutes the core and basis of the electronic documentation process. It is the form formula of the agreement the nature of the obligation and whether it is a commitment to a result or just an obligation to exercise care.[13]

In the absence of a legal text that establishes this obligation, there is nothing to prevent the parties from including any clause in the electronic authentication contract that stipulates the obligation of the provider to save the personal data of the client who holds the certificate and that it may not be used, processed, or given to others without the client's consent. The provider may be obligated under this condition not to modify, or delete any data related to the customer without The consent of the person concerned. Accordingly, the provider is contractually liable for any breach of the obligation to create, use or trade this data without the consent of the customer. As for the obligation to suspend or cancel the electronic authentication certificate, it was regulated by the Jordanian electronic transactions law and imposed penal penalties for breaching it, but if the parties agree on the provider's obligation to suspend or cancel the certificate upon the customer's request, or if there are reasons for its suspension or cancellation, the provider's contractual liability must be based on any damage resulting from the provider's breach of this obligation.[14]

This can be applied to any breach of another obligation contained in the electronic authentication contract, where the provider's contractual liability arises for breach thereof, it is also possible to envisage the supplier's contractual liability towards third parties if the latter was linked to a direct contractual relationship, and the breach of the implementation of this contract resulted in damages where it may count with the third party electronic authentication provider, the certificate he viewed because of a contract he concluded with the provider, then it becomes clear that this certificate was invalid, revoked, or suspended without the authentication services provider notifying that caused damages to him because

---

[10] For the nature of the contractual relationship between the certification service provider and the signature holder, see Plotkin, M., *E-Commerce law and business*, "Aspen Publisher". USA, 2003.

[11] Hegazy A., *Electronic Commerce*, university thought house. Alexandria, 2003, p. 443, - and Caprioli, *Régime juridique du prestataire*, disponible sur le site site https://www.caprioli-avocats.com/ (accessed 2 December 2022).

[12] Trudel P., Abran F., Benyekhelf K., Hein S., *Droit du cyberspace, Mon- treal*, editions THEMIS, 1997, p.3.

[13] Mell P., Dray J., Shook J., *Smart Contract Federated Identity Management withoutThird-Partyy Authentication Services, Bonn*, 2019, pp7.

[14] Article 25 of the Jordanian Transactions Law of 2015, previous reference.

he entered into contracts with the client who had the certificate based on the trust he had obtained from the electronic certificate[15]; talking about a doctrinal relationship between the provider and the third party requires searching for the adaptation of the relationship between them in the light of how to obtain the certificate, is this done directly through the provider or in another way[16], in practice from the holder of the certificate or the authentication provider[17], third parties may obtain the authentication certificate and the public key. But if the third party obtained the authentication certificate and the public key directly from the certificate holder, then we are facing a contractual relationship between the provider and third parties, and therefore it is not possible to imagine the contractual responsibility of the provider rather, it is a tort the third party may obtain the authentication certificate and the public key from the provider as a result of a contract[18], which leads to the possibility of conceiving the existence of a contractual relationship between them, with which the third party was associated with the provider of authentication services and thus the possibility of raising the rules of contractual liability if the third party who relies on this certificate incurs any damages.[19]

The possibility of conceiving contractual liability for damages incurred by third parties, who also see reliance on the certificate vis-à-vis the provider based on the stipulation theory for the benefit of others. All damages may be inflicted on third parties because they rely on the electronic authentication certificate and its reliance[20]. In fact, the contractual responsibility of the electronic authentication service provider raises several questions that the general provisions may fall short of answering, which raises some difficulties during implementation, such as the need to prove the error of the electronic authentication provider, which is often difficult to prove. The existence of a contractual relationship between them must also be the proprietor of the contract to arise. This is difficult to imagine in practice, as there is no contractual relationship between them in most cases. The multiplicity of relationships arising from it, in addition to the technical and modern nature of the various techniques of electronic signature and authentication certificates, the issue of determining the nature of the provider's commitment and whether it constitutes an obligation to take care or achieve a result; which makes the burden of proof difficult[21].

---

[15] Qassem A., *Some legal aspects of the signature Electronic*, "Journal of Law and Economics". 2002, No. 72. pp32.

[16] To learn about the concept of a general key in electronic documentation and how it works from a technical point of view, see Masa'a A., *Digital Signature and Certificate of Authenticity: Concept and Legal Effects*", "Al-Manara Journal-University Aal al-Bayt." 2005, Volume 11, Issue 4, p. 249; See also UNCITRAL, Promoting confidence in electronic commerce: legal issues of international use of electronic authentication and signature methods, United Nations publications, 2009. Available at http://www.uncitral.org/uncitral/en/ publications/publications.html.

[17] Yaqoub A., *The Civil Responsibility of the Provider of Digital Signature Certification Services towards Third Parties*, "Bahrain Law Journal". Volume Three, Issue One, 2006, p. 304.

[18] Yaqoub A., *Civil Liability of the Certification Service Provider*, previous reference, p. 313.

[19] The public key: is the symbol assigned or approved by the electronic authentication authorities to a user Electronic authentication certificate in order to verify the validity of the electronic signature; according article 2, Electronic transactions Law No. (15) of 2015.

[20] Abu al-layl I., *documenting electronic transactions, and burn, nature et impact juridique*, 2018.& BRUN M., *Nature et impacts juridiques de la certification dans le commerce électronique* sur Internet, Mars 2000, more information see, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf

[21] Sarhan A., Khater N., *Sources Of Personal Rights*, Dar Al Thaqafa For Publishing And Distribution,2021,pp. 302.

There is no doubt that the parties can avoid these difficulties through the terms agreed upon in the electronic authentication contract. Therefore, the parties should be vigilant and careful when drafting the terms of this contract, especially those related to the terms of the exemption and mitigation of liability, especially since many of these terms may be considered a kind of arbitrary terms that are subject to deletion or modification. In particular, the EU directive on unfair conditions provisions of 5 April 1993 can be applied to the relationship between customers and suppliers.[22]

The electronic transactions law in 2001 was devoid of any text specifying the conditions for in cases where the documentation provided is responsible and its legal system is clarified, the legislator is satisfied with including texts that decide a criminal penalty for issuing an inaccurate, suspended, or revoked certificate of authenticity. In light of the absence of a special text; deciding the responsibility of the electronic documentation service provider in the Jordanian legislation it was necessary to resort to the rules the public in civil liability, whether contractual or tortuous countries are interested in preparing legislation to ensure the enactment of the law provides confidence in these transactions; for this reason, the electronic signature has emerged as a tool in line with the nature of electronic transactions. The validity of these contracts must be mentioned because electronic signature is the most important means of electronic commerce.[23]

When taking an extensive look at the legal and financial rules and principles of the uncitral law regarding ratifications of service providers and the most important regulatory reference points in this regard, we will address the EU directive in this regard international use of electronic authentication and signature methods may also benefit from the adoption of those uncitral standards, the use of electronic signature methods in international contracts may benefit from the adoption of uncitral standards for electronic and paper-based digital signature systems[24]. The criteria for functional equivalence between electronic signatures and paper ones may provide an international common framework for allowing electronic authentication and signature methods to meet foreign form signature requirements. Some problems may persist, however, in connection with the international use of such methods that require the involvement of a trusted third party in the authentication or signature process[25].

4. PLACE OF ORIGIN RECIPROCITY AND LOCAL VALIDATION

One of the most important obligations of a local certification service provider, certification authority or regulatory authority is to have country-specific signatures and certificates for some form of verification; based on reciprocity, signatures and certificates are legally issued from one country to another. Many recognition systems are likely to

[22] Directive 93/13/EEC protects consumers in the EU from unfair terms and conditions which might be included in a standard contract for goods and services they purchase. It introduces the notion of 'good faith' to avoid any significant imbalance in mutual rights and obligations, as part of the New Deal for Consumers, Directive 93/13/EEC has been amended by Directive (EU) 2019/2161, which aims to modernise EU consumer law and improve its enforcement.

[23] The Jordanian electronic transactions law no. (85) in 2001.

[24] Trudel P., Abran F., Benyekhelf K., Hein S., *droit du cyberspace*, "Faculté de droit de l'Université de Montréal, Centre de recherche en droit public". editions themis, 1997.

[25] UNCITRAL TRADE LAW Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, UNITED NATIONS Vienna, 2009.

have some discriminatory effect when not intended; for example, if you are incorporated in a non-EU country, you have three options for certification recognition if you are in the EU; certification service providers must meet the requirements of the EU electronic signatures directive and have accreditation under a system set up in a member state.[26] The directive effectively requires foreign certification service providers to comply with both their home country and EU union regulations, which is a higher standard than would be required of certification service providers accredited in a member state. In addition, the EU union directive on electronic signatures has been implemented with some deviations. Ireland and Malta, for example, recognize foreign digital signatures (creditable certificates in EU terminology) as equivalent to domestic signatures provided other legal requirements are met. Requirements are met. On the other hand, recognition is subject to local verification (Austria, Luxembourg) or a decision by a local authority (Czech Republic, Estonia, Poland) and this tendency to insist on some form of local verification, usually justified by legitimate concerns, regarding the reliability of foreign certificates, leads in practice to a system of distinguishing foreign certificates according to their geographical origin.The EU directive on electronic signatures requires foreign certification service providers to comply with both their original data and the EU system, a higher standard than accredited certification service providers in an EU member state. [27]

One of the most important was the EU directive on electronic signatures, article 6 of this directive included a legal regime for the responsibility of the French provider of electronic documentation services in confidence in the digital economy in 2004, to confirm this trend. authentication services with specific rules by the nature of the tasks performed by these providers and the role they play given the extreme dominance of the electronic authentication process in internet contracting and commercial trust. And the directive came with several rules that highlight the specificity of the rules of responsibility for services electronic documentation is distinguished from the general rules of responsibility, In the same regard the EU directive established the legal system for the liability of suppliers on several grounds, including the obligation to distinguish between an approved electronic certificate and a non-accredited certificate. It also resorted to strictness in the responsibility of the suppliers, as it is an assumed responsibility**,** (the EU directive also allowed the possibility of limiting the extent or scope of his responsibility, unless the provider proves the opposite).[28]

On November 11, 2020, the court of justice of the EU union held that the near-field communication (NFC) functionality of a bank card, also known as contactless payment, in itself is a "payment instrument" as defined in the EU payment services directive 2015/2366 PSD 2, the CJEU also clarified the meaning of "anonymous use" under PSD 2 about NFC

[26] Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ec article 25/3 legal effects of electronic signatures: a qualified electronic signature based on a qualified certificate issued in one member state shall be recognized as a qualified electronic signature in all other member states.

[27] Article 7, European Union directive on electronic signatures, Article 7, Eligibility for notification of electronic identification schemes An electronic identification scheme shall be eligible for notification pursuant to Article 9(1).

[28] Sedallian V. *Le dëveloppement du commerce électronique, les nouveaux métiers de la confiance*, www.droit-lechnologies.com. P. 5 "Capriol", La directive européenne n 1999/93M|CE du 13 décembre 1999 sur *un cadre communautaire pour les signature électronique*, Gaz. Pal, October 2000.

functionality. The court stated that a bank may not exclude its liability for unauthorized low-value transactions in its general terms and conditions by simply claiming that blocking the NFC functionality would be technically impossible but must prove impossibility in light of the objective state of available technical knowledge when a customer reports a lost or stolen bank card. Furthermore, the court ruled that if the user is a consumer general terms and conditions provide for tacit consent to possible future amendments to such terms and conditions and must comply with the standard of review set out in directive 93/13 on consumer rights protection, not with PSD2, it defines the responsibilities required of each party and defines the responsibility of the certificate authentication service provider, which defines the actions of the authorized party. The relying party bears the legal consequences of failing to do so; (i) take reasonable steps to verify the authenticity of an electronic signature, (ii) if the electronic signature is supported by a certificate, reasonable steps shall be taken; verifies that the certificate has been suspended or revoked and that any certificate restrictions are observed.[29]

5. DISCUSSION

The idea seems to be that a party intending to rely on an electronic signature should consider whether and to what extent such reliance is reasonable in light of the circumstances. It is not intended to address the issue of the validity of the electronic signature, which is addressed under article 6, and should not be dependent on the behaviour of the relying party, the question of the validity of an electronic signature should be separated from the question of whether it is reasonable for a relying party to rely on a signature that does not meet standard set out in article 6.[30] Consumer issues while article 11 may place a burden on authorized parties, particularly when such parties are consumers, it may be recalled that the model law is not intended to invalidate any rule governing consumer protection, nevertheless, the model law may play a useful role in educating all relevant equal relationships, including authorized parties, regarding the standard of reasonable conduct that must be met concerning electronic signatures. In addition, establishing a standard of behavior whereby a relying party must validate the signature through accessible means may be seen as necessary for development.[31]

Emphasizes the electronic signatures model act of 2011, which outlines the responsibilities required of each party and outlines the responsibility of the certificate authentication service provider, which outlines the procedures for the authorized party. The relying party bears the legal consequences for failing to take reasonable steps to verify the authenticity of the electronic signature, and if the electronic signature is supported by a certificate, reasonable steps must be taken; to verify that the certificate has been suspended or revoked and that any restrictions related to the certificate are observed, and article 11 comes in; the idea seems to be that a party intending to rely on an electronic

29 Case before, European Court Of Justice *Rules On Liability Of Banks For Unauthorized Low-Value Transactions Using Contactless Payment* "The Library of Congress" https://cutt.us/hqnwX .accessed Jan 02, 2023.

30 Article "6" UNCITRAL Model Law on Electronic Signatures with Guide to Enactment UNITED NATIONS, New York, 2001.

31 Article 11, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment UNITED NATIONS, New York, 2001.

signature should consider the question of whether and to what extent such reliance is reasonable in light of the circumstances. It is not intended to address the issue of the validity of an electronic signature, which is dealt with in article 6 and should not depend on the conduct of the relying party; the validity of an electronic signature should be separated from the question of whether it is reasonable for the relying party to rely on a signature that does not meet the standard set forth in article 6.

Consumer issues while article 11 may place a burden on authorized parties, particularly where such parties are consumers, it may be recalled that the model law is not intended to override any rule governing consumer protection, however, the model law may play a useful role in educating all related equal relations, including authorized parties, as to the standard of reasonable conduct that must be met in connection with electronic signatures. In addition, establishing a standard of behaviour according to which the relying party must verify the validity of the signature through accessible means may be seen as essential to the development of any public openness infrastructure system. Infrastructure system[32].

Finally, I believe that reliance on the reasonableness of reliance on the certificate of authenticity, as a condition of the service provider's civil liability is necessary to strike a balance between providing protection to third parties and moving away from imposing excessive obligations on the provider. If it is unreasonable for a third party to rely on a defective authentication certificate because of its previous dealings with the certificate holder or by the nature of the transaction, then it is not reasonable to say that the authentication service provider is responsible in this case. The provider's responsibility for the damages resulting from the electronic document may be negated if there is one of the reasons for the general rules of liability, including force majeure, the act of third parties, and the action of the injured party.

As for the decision according to force majeure as the reason for the supplier's negation of liability, the supplier's responsibility for the damage caused may be nullified if he proves that the damage had to occur due to an uncontrollable cause and is due to an unexpected event outside his control. The reason is exceptional beyond the will of the parties, such as the failure of the foreigner, it is required that it be unexpected and that the occurrence and damage of the electronic devices used in the electronic authentication processes due to the occurrence of an earthquake, volcano, wars or floods.

It is noted that these cases revolve around the non-liability of the provider due to the act of the customer holding the certificate or his decision of the general rules on liability. Thus, the provider did the act of a third party and not because of force majeure, which is for the damage that arises to others despite his suspending the work of the certificate or cancelling it with a request that is not responsible[33].

Similarly, if the certificate holder fails to keep the secret number of their electronic signature confidential or fails to inform the provider if a third party has obtained or taken control of the private key, or if any modifications have been made to the data after the certificate has been issued, the responsibility of the provider may be negated. Additionally, if it can be proven that it is not reasonable for a third party to rely on the electronic authentication certificate, such as in cases where the certificate has been suspended or

[32] Article 11, UNCITRAL Model Law, previous reference.

[33] Hegazy A., *Electronic Commerce*, university thought house. Alexandria, 2003, p.43, - and Caprioli, *Régime juridique du prestataire*, disponible sur le site site https://www.caprioli-avocats.com/

permanently revoked, and this is clearly indicated in the electronic certificate registry that the provider is required to maintain, this will be considered a valid reason for the provider not being liable for any damages resulting from unreasonable reliance on the electronic certificate.

6. CONCLUSION

The study is one of the recent studies that have not been written about previously. I researched the writings and articles that scholars have discussed in the past. This topic was not discussed, especially in Jordan, the development of the law in legal legislation, and this is one of the difficulties and challenges that I faced, so I relied on comparison with international legislation, analyzing it, and obtaining a clear picture of the subsequent needs.

Indeed, interested customers may encounter a legal void and instability related to legal liability, the conditions for its creation, and the consequences associated therewith when engaging in electronic signature activities. The Jordanian legislator did not explicitly address these points within a specific, detailed, and comprehensive legal framework of all possible developments in the accelerating world of electronic commerce, which raises questions about liability, including the liability of the provider for damages resulting from defects in the electronic authentication process, and the responsibility of the customer for violating the certificate.

The Jordanian legislator must realize the importance of developing laws, especially those working in the field of information technology and financial transfers because they need to be developed continuously to keep pace with the course of global electronic commerce, avoid legal instability, and use the European experience to be a motive for setting the exact details and required legislation and clarifying any ambiguity, as stability encourages investors in the field of electronic commerce to move forward.

In addition, the provider is obligated to refrain from deleting, adding, or modifying the personal data necessary to provide and maintain the certificate and the possibility of limiting or excluding the provider's liability remains uncertain. Thus, the provider bears contractual liability for any breach of the obligation to generate or use data without the consent of the customer.

REFERENCES

LITERATURE

Abu al-layl I., *documenting electronic transactions, and burn, nature et impact juridique,* 2018.

AL-JAMMAL S., *contracting through modern communication techniques*, dar al-Nahda al-Arabiya, Cairo, 2006.

Al-Sarhan A., Khater N., *Sources of Personal Rights*, 2016.

Brazell L., Rice P., Law: *Electronic Evidence Development and Evidence,* American Bar Association publication »,2008.

BRUN M., *Nature et impacts juridiques de la certification dans le commerce électronique* sur Internet, Mars 2000, more information see, https://www.lex-electronica.org/files/sites/103/7-1_brun.pdf (accessed January 25 2023).

Caprioli E., *la directive européennes n 1999/93/ 13 December 1999 sur un cadre communautaire pour les signature électronique*, gaz. Pal, October 2000.

Hegazy A., *Electronic Commerce*, "university thought house". Alexandria, 2003, and Caprioli, *Régime juridique du prestataire*, disponible sur le site site https://www.caprioli-avocats.com/ (accessed December 2 2022).

Le Tourneau P., *contrats informatiques et électroniques, dalloz*, 2006,& Le Tourneau p., *droit de la responsabilité et des contrats, dalloz*, 2006-2007, n 3946. *Neveux les prestataires de service de certification*: quelle responsabilité pour quelle service, 2002.

Lim S., Fotsing P., Almasri A., Musa O., Kiah M., ang T. & Ismail R., *blockchain technology the identity management and authentication service disruptor: a survey'*, international journal on advanced science, engineering and information technology, Malaysia, 2018.

Lina H., *electronic documentation, and the responsibility of the competent authorities*, dar al-raya for publishing and distribution, Amman, 2009.

Masa'a A., *digital signature and certificate of authenticity: concept and legal effects*", al-Manara journal-university aal al-Bayt, 2005.

Mell P., Dray J., Shook J., *smart contract federated identity management without third-party authentication services*, Bonn, 2019.

Musaed A., *Digital Signature and Certificate of Authenticity: Concept and Legal Implications*", Al-Manara Journal - Al al-Bayt University, Vol. 11, No. 4, 2004.

Plotkin, M., *e-commerce law and business, the nature of the contractual relationship between the certification service provider and the signature holder*, "aspen publisher". *USA*, 2003.

Qassim A., *some legal aspects of the signature electronic, journal of law and economics*, 2002.

Sarhan A., Khater N., *Sources Of Personal Rights*, Dar Al Thaqafa For Publishing And Distribution,2021,

Sedallian V., *Le dëveloppement du commerce électronique*, les nouveaux métiers de la confiance, and caprioli, la directive européenne n 1999/93m|ce du 13 December 1999 sur un cadre communautaire pour les signature électronique, gaz. Pal, October 2000 , (accessed 3 November 2022), www.europea.EU.intal/comm/dg/fr,

Trudel P., Abran F., Benyekhelf K., Hein S., *droit du cyberspace*, "Faculté de droit de l'Université de Montréal, Centre de recherche en droit public". editions themis, 1997.

Yaqoub A., *the civil responsibility of the provider of digital signature certification services towards third parties*, Bahrain law journal, volume three, issue one, 2006.

CASE LAW

Case before, European Court Of Justice *Rules On Liability Of Banks For Unauthorized Low-Value Transactions Using Contactless Payment* "The Library of Congress" https://cutt.us/hqnwX .accessed Jan 02, 2023.

LEGAL ACTS

Article 2, Jordanian electronic transactions Law No. (15) of 2015.

Article 8, of the Jordanian electronic transactions law no. (85) in 2001.

Article 25, of the Jordanian Transactions Law No. (15) of 2015.

Article 6, article 11, UNCITRAL model law on electronic signatures with a guide to enactment united nations, New York, 2001.
Article 7, EU union directive on electronic signatures, December 1999.
Article 8, EU union directive on electronic signatures, December 1999.
Directive 93/13/EEC protects consumers in the EU from unfair terms and is amended by Directive (EU) 2019/2161.
Uncitral united nations commission on international trade law promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, united nations Vienna, 2009.

WEBSITE
https://uncitral.un.org/en , (accessed 7 November 2022).
https://www.caprioli-avocats.com/ (accessed 27 January 2023).
European Court Of *Justice Rules on the liability of banks for unauthorized low-value transactions using contactless payment*, https://cutt.us/u9iqv accessed Jan 02, 2023.