International Journal of Economic Studies and Management (IJESM)
ISSN 2789-049X
Int. J. Econ. Stud. Manag. 4, No.6 (DECEMBER-2024)

The impact of artificial intelligence on the legal validity of electronic signatures

JAZOULI Yasmine
ESSOR Laboratory
Faculty of Legal, Economic and Social Sciences FES
Sidi Mohamed Ben Abdellah University - FES - Morocco

JOUIDI Driss
ESSOR Laboratory
Faculty of Legal, Economic and Social Sciences FES
Sidi Mohamed Ben Abdellah University - FES – Morocco

Abstract : The advent of Artificial Intelligence has caused a great change in many legal arenas, but the consequences for the legal status of electronic signatures seem to be the most interesting. In this paper, an attempt is made to establish a conceptual framework for understanding how AI interacts with the authentication and veracity of an electronic signature, by undertaking an in-depth examination of associated legal challenges. The result of this effort will follow from a methodological framework that combines a documentary analysis of regulatory texts with the examination of case studies about AI applications regarding the verification of electronic signatures. First, it involves the reliability of an artificial intelligence system regarding authenticity and validity of electronic signature as against regulatory requirements like eIDAS regulation in Europe and the ESIGN Act in the United States. he preliminary results show that AI is equipping voices to strengthen the security of electronic signatures, while generating new questions relating to liability and compliance. This article concludes with a series of recommendations and guidelines for the conflict-free integration of AI into legal proceedings, and the need to demand regulation to guarantee the evidence of electronic signatures in the digital age. The aim is therefore to share an analysis that sheds light on the prospects of AI with legal systems dealing with electronic signatures to make law a discursive and secure place of practice in the future.

Keywords : Artificial Intelligence, electronic signatures, legal validity, security.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**14598483**

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Introduction

AI and e-signatures are revolutionizing legal and business engagements on all continents. AI refers to a group of technologies designed to perform tasks that require intelligence similar to those of human beings, such as the ability to recognize patterns or learn from experience (***Russell & Norvig, 2021***). Electronic signature, on the other hand, is a digital scheme that verifies the identity of the signer and ensures that the integrity of the document is not tampered with (***eIDAS, 2014***).

It would, therefore, be correct to trace the emergence of electronic signatures from the late 1990s, simultaneous with legislation that was designed to recognize their validity. In particular, the 2016 European Union's regulation known as eIDAS (***Electronic Identification and Trust Services***) marks another milestone in the legal framework underlying electronic transactions, establishing unified standards for authentication (***European Commission, 2016***). Nevertheless, rapid development in related technologies for artificial intelligence has spurred questions about what the consequences are for the legal validity of these signatures.

Surely, while AI might eventually improve the security and efficiency of verification methodologies, it also introduces liability issues and regulatory challenges in equal measure. In particular, the practical and theoretical issues arising from the integration of AI into electronic signature verification are overwhelming. On one hand, AI technologies can speed up and make the signature-verification process more accurate to better secure transactions. On the other hand, they present certain drawbacks on algorithmic bias concerning AI implementation and data security and privacy (***Crawford & Paglen, 2021***).

The core issue that this article deals with is summed up in the following question: *to what extent does artificial intelligence affect the legal validity of an electronic signature, and which regulations can ensure its authenticity and integrity in the ever-changing digital landscape?*

The aim of this paper is to assess the impact of artificial intelligence on the legal validity of electronic signatures by reviewing the present legal framework, discussing the new emerging technologies, listing the challenges involved, and drafting recommendations toward a legal approach that embraces these developments. The paper will seek to help the legal professionals and the policymaker become aware of the impacts that Artificial Intelligence has within this domain, while at the same time encourage consideration towards possible further developments of electronic signature within a fully digital ecosystem.

1 : Legal Framework on Electronic Signatures

The legal framework concerning electronic signatures is very important in relation to their validity and recognition within digital transactions. It contains national and international regulations that provide conditions under which an electronic signature can be regarded as equivalent to a hand-written signature. First, the eIDAS created by the European Union in 2016 occupies the central part to establish the same requirements for electronic signatures with respect to all member countries. These include three tiers of electronic signature, distinguished by the level of security and authenticity assured: the simple, the advanced, and the qualified, in that order. National laws supplement this framework, such as in the USA, the ESIGN Act, which recognizes electronic signature in commercial transactions. These indeed are advances, but the big gaps remain, especially on how systems will interoperate or how regulations will be followed to the letter. The rapid evolution of AI technologies has thrown up challenges that make the issue even more complicated, raising essential questions as to the legal liability and reliability of AI-based authentication systems within electronic signatures. Therefore, developing an in-depth understanding of this legal framework for navigating the modern electronic transaction environment is needed.

1.1 Current frameworks and their scope

The legal framework of e-signatures differs considerably between countries with regard to context, including legal, cultural, and technological contexts. Against such a background, the paper is looking into the main regulations in force in Europe, the USA, and Morocco, trying to find out the existing gaps and challenges arising because of them.

The European Union enacted the eIDAS (Electronic Identification and Trust Services regulation), in 2014, which has been in effect since 2016. This regulation creates a harmonized legal framework for electronic signatures within the EU. It recognizes three types of electronic signature: the simple electronic signature, which lays down no particular measures for security; the advanced electronic signature, being uniquely linked to its signatory and capable of identifying the latter; and the qualified electronic signature, with the highest level of security, by requiring a certificate issued by a trust service provider. The scope of the eIDAS regulation is huge, considering that the electronic signature is mutually recognizable between the member states, making cross-border transactions easier. However, there are certain criticisms concerning interoperability between different signature systems and frequent updates relating to technology. In the United States, ESIGN-the Electronic Signatures in Global and National Commerce Act-granted electronic signatures legal status in 2000. According to this law, an electronic signature shall be legally valid if the requirements of intent and authenticity are met. However, the legal framework is still fragmented, with each state able to adopt its own regulations, which may cause inconsistencies.

This law considers an electronic signature as equivalent to a handwritten signature if it is linked to the signatory in such a way allowing verifying his identity. It is important to note a few shortcomings of the Moroccan framework. Legal provisions are still very limited in the public sector, where general digitization is also slow. Also, certification service providers lack specific legal guidelines, raising many question marks with regard to the reliability of the provided certificates.

Cases like the 2019 Casablanca controversial waste concession contract, with several electronic documents whose signature was contested, showed some of these legal weaknesses.

Such comparison of the regulatory frameworks across different countries shows that, behind the considerable advances achieved in some countries, relevant gaps still exist. Electronic signatures are in jeopardy without a harmonized approach with their validity differing depending on jurisdiction. Present regulations do not address any challenge posed by AI to the process of electronic signatures. As a matter of fact, AI-based technologies often fall under insufficient regulation, which can easily lead to security risks and fraud and breaches in data protection.

In the case of Morocco, although the law for e-signatures was adopted, lack of a clear enforcement mechanism, regulation concerning trustworthy service providers creates a virtual legal void that may raise serious questions relating to electronic transactions' security. Low take-up of the technologies that are digital increases problems in particular where prevailing sectors occur.

Therefore, this comparative study reveals that even while there is a sound legal framework being pursued, the gaps are still huge. Every country needs not only to recognize the importance of electronic signatures but also to ensure proactive and adaptable regulation that can respond to the legal and technological challenges thrown up by AI. International cooperation and sharing of best practices could also help boost the effectiveness of e-signature systems and user confidence.

1.2 : Limitations of the current legal framework in the face of technological advancements

Technological strides, especially in areas like artificial intelligence (AI) and blockchain, have largely changed the dimensions of e-transactions. There is some concern about the suitability of the current legislative framework that regulates e-signatures. Despite legislative attempts at clarity, some gray areas exist, leaving many legislative frameworks wanting as new digital realities emerge.

Second in terms of larger obstacles is the rapid rate at which new technologies are adopted, at a speed perhaps too rapid for the formulation of adequate legislation. It is symptomatic that such a concept as advanced and qualified e-signatures provided for in the eIDAS regulation does not completely take into account the offer of blockchain technology. Blockchain-based transactions may even guarantee the integrity and authenticity of data without the intervention of a trusted third party, therefore challenging traditional mechanisms for validating electronic signatures. What's more, these decentralized systems complicate the determination of liability in case of a dispute—an aspect not sufficiently addressed by the current regulations.

Furthermore, the problems of cybersecurity became more cogent. While electronic signature systems had been created for the very reason of guaranteeing data authenticity and their proper storage, they are not totally safe from cyber-attacks. Cases of forging an electronic signature or compromising the storage devices prove that there are risks attached to the methods. It follows, therefore, that the legal framework often has to struggle with already obsolete security models, given the constantly developing character of digital threats.

The second major concern is the absence of a clear guideline on personal data management and privacy protection. Although regulations like Europe's General Data Protection Regulation lay down strict principles on the processing of data, it is not always clear how these principles interact with e-signature systems. So, companies and end-users are always in doubt regarding the validity of an electronic signature in relation to data protection, where the authentication process entails a transfer of personal information.

The current legal framework does not address algorithmic biases that may arise in the application of AI in e-signature systems. With increased complexity in AI algorithms and their integration into verification processes, it is highly necessary that such technologies do not reproduce or amplify already existing inequalities. In this regard, regulators shall develop guidelines in the assessment of algorithm fairness, reliability, and transparency for users' rights protection.

Finally, harmonization of regulations is essential at the international front. Globalization and e-commerce have increasingly made companies operate across borders. The differences existing between various national legislations make the implementation of electronic signatures difficult, especially when documents are signed in one jurisdiction but used in another. Companies can be brought to question the validity of such signatures across different legal systems, which retard the fluidity of international transactions.

It means that the limitations imposed by the current legal framework in the face of the technological change call for proactive review of the regulations. Regulators should collaborate with experts in technologies so that the laws are adapted to new digital realities while ensuring security, fairness, and protection of users' data. Otherwise, without such evolution, there is a danger that the legal framework for e-signatures will become obsolete and thus destroy integrity and trust in e-transactions.

2 : The role of artificial intelligence in electronic signature validation

This will definitely integrate artificial intelligence into the validation of electronic signatures—a huge step toward better efficiency and security of digital transactions. On the other hand, electronic signatures have become the backbone of any electronic exchange in the world that needs to ensure the authenticity and integrity of documents. But now, with AI rising, verification and analysis methods are going through revolutionary change.

This chapter discusses how AI contributes to the validation of e-signatures, its applications and benefits, and the ethical and legal challenges involved. From this understanding of what role AI can play, one can envision a time when electronic transactions are secure, more accessible, and reliable.

2.1 Technological innovations and artificial intelligence systems in use

Technological innovations and the rise in artificial intelligence systems are greatly revolutionizing the landscape of electronic signatures. Technologies have made signature validation better by using advanced algorithms and data processing techniques, given the major concerns around security, authentication, and integrity of a transaction. In this respect, this paper reviews various AI systems and technological novelties employed in the e-signature field and compares their advantages with their disadvantages. The greatest emphasized point in e-signature analysis is machine learning. The machine learning algorithms used in signature validation are usually trained to learn patterns from data. For example, one would train a model on finding anomalous behavior of signatories and thus potentially recognizing forged signatures. Its benefits include processing in real time and continuous learning through new datasets.

However, it still has its drawbacks, such as the risk of bias in training data that may create validation errors, and high-quality large amounts of data to be used for training purposes (***Chato & Latifi, 2018***). Quantam computing, though still in the developmental stages, promises to bring huge strides in cryptography and security of electronic signatures. Because it can do complex calculations at speeds unheard of before, quantum computing may ultimately make possible the development of far more secure signature systems, making forgery extremely difficult. It brings with it better protection against computer attacks and a potential time-saving in the validation processes. However, this technology is still experimental and costly, and not ready yet for large-scale applications ***(Sharma, Gupta, & Sood, 2024).***

This blockchain technology helps to create decentralized e-signatures and thereby creates a register that is immutable. Smart contracts can be designed to validate and execute a transaction the moment a signature is verified. This will lead to advantages in terms of high security and transparency, since it is decentralized, and reduced transaction costs by the elimination of intermediaries. However, implementation complexity in existing systems and poor scalability in public blockchains remain as drawbacks (***Song & Zhu, 2021***). Integration of AI in facial recognition, voice recognition, and other biometric systems increases the authenticity level of e-signatures. For example, the software will be able to check whether the biometric belonging to the signatory corresponds with the one recorded at the time of creating the signature certificate. This will further add another layer to the validation process and easily facilitate remote authentication of transactions.

Nonetheless, issues related to privacy and biometric data security still prevail, along with the risks of recognition errors that could compromise access (***Hossin & Sulaiman, 2015***).

A comparative analysis of the AI system and technological innovations shows obvious advantages and disadvantages. Technologies such as blockchain and AI in biometric analysis are highly secured, though they come with challenges in implementation and concerns about privacy. On the other hand, machine learning is greatly flexible and adaptive but faces issues of bias and data dependency.

The diversity of technologies and standards makes interoperability complicated. Regulators shall give uniform standards for different AI and e-signature systems to be easily integrated.

Raising awareness among users and business entities is important for new technologies and their functioning. Better understanding of innovations would lead to better acceptance of them and increased adoption. Lastly, legislation must change and adapt to take account of challenges brought in by these new technologies. The regulators are supposed to work with experts in the field of technology to come up with standards and policies that ensure the security of e-signatures while ensuring the privacy of users' lives.

Thus, integration of artificial intelligence and other technological innovations in the domain of e-signatures opens up many possibilities to enhance the security and efficiency of transactions. However, the challenges that lie ahead must be met with due care so that the benefits can be maximized, the disadvantages minimized, and a strong legal and technological framework provided for the future.

2.2 Problems of reliability and liability

Questions of electronic-signature reliability and liability are at the forefront of nearly every debate concerning a rapidly changing digital world. While electronic signatures represent an undeniable benefit in areas such as increased efficiency or lower transaction costs, some have expressed concern over both the integrity of these processes and the apportionment of liability in the context of litigation. The reliability of an electronic signature depends on quite a few parameters, including technology, key management, and the authentication processes of the signatory.

The reliability of electronic signatures therefore depends on the technology deployed in creating and authenticating them. Qualified electronic signatures, which meet the eIDAS regulation standard for Europe, offer strong assurance through the use of digital certificates issued by a trusted service provider (***Council of Europe, 2021***). The lack of internationally harmonized standards may compromise the mutual recognition of signatures in different jurisdictions. Some of the benefits of electronic signatures include enhanced security and increased user confidence in carrying out e-transactions; some of the drawbacks include complexity, costs of implementation for firms, and dependence on third-party suppliers for certificate management.

The security of an electronic signature also depends on key management. If the keys are compromised, the signature could be invalidated completely, and the parties will be exposed to fraud risks. Secure key storage, the use of security hardware (HSM), and implementation of standardized revocation processes are critical elements in ensuring signature reliability (***ISO, 2022***). One of the clear positives of this system is the greater security against forgery and usurpation, although at a high cost for all secure solutions and significant logistic challenges associated with key management and distribution.

So far as the apportionment of responsibility for electronic signatures is concerned, the topic becomes complicated when digital transactions involve more than two parties. In most cases, the responsibility for the validity of an electronic signature may not be very clear. Where a signatory challenges the authenticity of a transaction, it will be important to find out whether the signature has been authenticated in order and, if so, whether the signing process conformed to existing standards. Moreover, jurisdiction to jurisdiction, the legal framework for electronic signatures can vary, making resolution of such disputes even more challenging ***(Smedinghoff, 2008***). While a better appreciation of the role and duties of the parties can bring down disputes, there is always the risk of costly disputes due to ambiguities in contractual agreements.

The adoption of clear, internationally harmonized regulations is essential to establish precise rules on liability in the context of electronic signatures. Laws such as the Uniform Electronic Transactions Act (UETA) and the International Institute for the Unification of Private Law (UNIDROIT) Model Law on Electronic Transactions provide a basis, but much work remains to be done to address discrepancies between legal systems (***UNIDROIT, 2023***). Clear regulatory frameworks will go a long way in giving confidence to market players, increasing the uptake of e-signatures, and easing international transactions. On the other hand, slow adjustment of the regulations to rapid developments in technology is an ongoing challenge, as is the risk of dissonance between different legal systems. The reliability and accountability of e-signatures are dependent on cooperation among all parties concerned.

Conclusion

The question of how artificiel intelligence affects the legal validity of e-signatures is a rather complicated one and needs to be analyzed in detail. Although the integration of AI into signature frameworks could increase their security and efficiency, it entails major issues concerning liability, integrity, and the authenticity of the transaction. On the flip side, advanced technologies such as blockchain and machine learning could be in place to make the verification of identity more secure, increasing the reliability of e-signatures by making forgery much harder and creating traceability in transactions.

Similarly, AI offers a way to automate the validation process, decreasing human significantly and diminishing costs linked with signature management. However, these technologies require much care in their application, as over-relying on artificial intelligence may be risky in terms of data confidentiality and manipulation, in particular, when managing consent.

The implication of artificial intelligence on the legal validety of e-signatures give rise to questions of liability where there is a challenge in court.

If an e-signature that has been generated or authenticated through an AI system is to be challenged, it may not be easy to determine the party liable : the one signing, the developer of AI, or the provider of the signature service. Current legal system, often poorly adapted to rapid changes in technology, must be updated to incorporate such modern developments.

With such a view, this paper could make some recommendations for such issues. To begin with, current regulation should be revised to cover specific provisions on the application of artificial intelligence in regard to electronic signatures. Requirements on transparency and validation for algorithms in use could offer better protection for users of the signature. What is more, clear rules must be issued that clarify the liability when AI systems employed with e-signatures fail.

In the final analysis, communication bbetween legal practitioners, technology experts, and regulatory authorities is of the essence in coming up with fair solutions that will ensure the legal validity of e-signatures ; While at the same time reaping maximum benefits of artificial intelligence. Such cooperation can help to ensure that the growing use of AI enhances, rather than undermines, the authenticity and reliability of e-signatures in our increasingly interconnected digital economy.

Artificial intelligence's impact on the validity of electronic signatures is an emerging area that demands diligence and foresight. How electronic signatures evolve is reliant on our collective ability to face these challenges with morality and diligence as we transition into more comprehensive use of these technologies while keeping trustworthiness and safety in digital payments intact.

.

REFERENCES

[1] ***Crawford, Kate & Paglen, Trevor. (2021). Excavating AI: the politics of images in machine learning training sets. AI & SOCIETY. 10.1007/s00146-021-01162-8.***

[2] ***eIDAS. (2014)*. 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. *Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2014/910/oj***

[3] ***European Commission. (2016).*** **eIDAS: The new Regulation on electronic identification and trust services.**

[4] ***Russell, S., & Norvig, P. (2021).*** **Artificial Intelligence: A Modern Approach** ***(4th ed.).***

[5] ***Loi n° 53-05 relative à l'échange électronique de données juridiques (2007).***

[6] ***Controverse sur le contrat de concession de déchets à Casablanca (2019).*** ***https://fr.le360.ma/economie/casablanca-revoit-plusieurs-clauses-du-contrat-de-gestion-deleguee-des-dechets-190394/***

[7] ***Hossin, M., & Sulaiman, M. N. (2015). A review on evaluation metrics for data classification evaluations.*** **International Journal of Data Mining & Knowledge Management Process,** ***5(2), 1–11. https://doi.org/10.5121/ijdkp.2015.5201***

[8] ***Sharma, P., Gupta, V., & Sood, S. K. (2024). Evolution of quantum cryptography in response to the computational power of quantum computers: An archival view.*** **Archives of Computational Methods in Engineering.** ***https://doi.org/10.1007/s11831-024-10122-6***

[9] ***Chato, L., & Latifi, S. (2018). Application of machine learning to biometric systems: A survey.*** **Journal of Physics: Conference Series,** ***1098, 012017. https://doi.org/10.1088/1742-6596/1098/1/012017***

[10] ***Song, Z., & Zhu, J. (2021). Blockchain for smart manufacturing systems: A survey.*** **Chinese Management Studies,** ***ahead-of-print. https://doi.org/10.1108/CMS-04-2021-0152***

[11] ***Council of the European Union. (2021).*** **ST 9471 2021 INIT.** ***https://data.consilium.europa.eu/doc/document/ST-9471-2021-INIT/en/pdf***

[12] ***International Organization for Standardization. (2022).*** **ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls** ***(3rd ed.). ISO/IEC. file:///C:/Users/YOGA/Downloads/d3d149.pdf***

[13] ***Smedinghoff, T. (2008).*** **The legal challenges of implementing electronic transactions.**

[14] ***International Institute for the Unification of Private Law. (2023).*** **UNIDROIT principles on digital assets and private law.** ***UNIDROIT. https://www.unidroit.org***