ARTICLE :

Revising the Saudi Electronic Transactions Law on E-Signatures

By Oways Kinsara

Introduction

Electronic signatures ('e-signatures') are often acknowledged for saving time, reducing cost and even for being friendly to the environment. However, when legislation on the matter was first introduced in Europe 20 years ago, preceding Saudi Arabia, e-signatures were an exception to the norm, centred around cross-border transactions and the public service. Even with the increasing interest in e-commerce and technological developments over the past decade, the lack of education and knowledge by the legal profession regarding e-signatures, has meant that the profession understood little about e-signatures until, arguably, the effect of the Coronavirus pandemic was felt. This is when lay people and small and medium-sized enterprises (SMEs) had to use the internet more frequently to conduct business. As a result, lawyers faced increasing demand from their clientele to understand the legal requirements and validity of e-signatures.

Given the increasing significance of e-commerce,[1] this article revisits the 2007 Electronic Transactions Law (ETL) of Saudi Arabia[2] and its implementing regulation[3]. In doing so, it compares the ETL to the evolution of the European regime on e-signatures, from the 1999 Directive (the 'Directive')[4] to the 2014 eIDAS Regulation (the 'Regulation').[5] However, in instances where the EU regimes are silent, the provisions of the UNCITRAL Model Law[6] are utilised to discuss the Saudi ETL.[7] The EU analysis is succinct and limited to the most important legislative alterations between the Directive and the Regulation.

The analysis is conducted in five parts. First, it overviews the ways in which legislatures can approach the electronic transformation of signatures. Second, it considers the definition of the e-signature. Third, it considers the question of legal effect and scope of protection for various categories of e-signature. Fourth, it turns to the provisions on signatories and their responsibilities. Lastly, it analyses the duties of the parties that rely on e-signatures. This article

[1] United Nations Conference on Trade and Development (UNCTAD), 'UNCTAD B2C E-COMMERCE INDEX 2019' (2019), https://unctad.org/system/files/official-document/tn_unctad_ict4d14_en.pdf . United Nations Conference on Trade and Development (UNCTAD), 'UNCTAD B2C E-COMMERCE INDEX 2020' (2020), https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf .

[2] Saudi Electronic Transactions Law, Royal Decree No M/8 dated 8/3/1428 AH (26 March 2007), https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx .

[3] Implementing Regulations of the Electronic Transactions Law, issued by the Minister of Telegraph, Post and Telephone (currently the Ministry of Communications and Information Technology) Decision No 2 dated 10/3/1429 AH (18 March 2008), https://www.mcit.gov.sa/sites/default/files/llyh_ltnfydhy_lnzm_ltmlt_llktrwny.pdf .

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures, OJ L13, 19.01.2000, p.12.

[5] European Union 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, OJ L257, 28.8.2014, p. 73–114.

[6] United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment (with additional article 5 bis as adopted in 1998).

[7] The article only utilises the Model Law in part 4 on signatories and their responsibilities.

is not comprehensive, in that it does not discuss every aspect of e-signature legislation, including the status of certification service providers.

Regulatory approaches to electronic signatures

Common law and civil law approaches

While the modern approach to e-signatures is often based on functional equivalence, it can also accompany an element of form depending on the extent to which the latter has significance in the respective jurisdiction. As illustrated by Reed, signatures in common law jurisdictions merely play an evidential function; in civil law, on the other hand, they hold a formal significance (i.e. the tangible action), which cannot be translated electronically.[8] Hence, common law jurisdictions have not struggled in regulating e-signatures, whereas civil law jurisdictions had to introduce the new category of a qualified e-signature, combining a digital signature with an issued certificate, thus mimicking the characteristics of both function and form. It is noteworthy, however, that the solution comes at the additional expense and effort of signatories.[9]

Electronic signatures from the perspective of Sharia law

Regarding Islamic law jurisdictions, Professor Al-Nasser, citing Imam Ibn al-Qayyim and others, explains that the means of proof in Sharia are not limited to an exclusive list of forms.[10] He notes that, insofar as the signature's function underlies its relationship to the signatory and the latter's knowledge of the content of the document, 'this is achieved in the electronic signature as it is in the traditional signature, if not further'.[11] Al-Nasser also illustrates that no particular form is ever required by Sharia since, in the time of the Prophet Mohammed, tree, stone, leather and other media were used alongside paper; thus, he educes that it is valid to sign through electronic mathematical equations that are linked to the signatory.[12] While Al-Nasser's analogy clearly neglects the intrinsic distinction of forms based on their nature (physical versus intangible, rather than tree versus paper), his primary argument remains valid, that is, Sharia principles do not preclude the use of e-signatures as far as they achieve the minimum functions of identity and intent. Therefore, in this respect, Islamic law leans closer to the common law world; Islamic countries, at least in principle, thus enjoy the flexibility to regulate e-signatures through a functional lens.

Approaches to functional equivalence

It is obvious but necessary to note that technical varieties of e-signatures may achieve the primary functions of a signature, based on which technology is used.[13] Since such technicalities are not within this article's scope,[14] for the present purposes, the variety of e-signatures can be divided in two essential categories: (1) simple e-signatures, which include the majority of what laypeople and SMEs use on a daily basis, such as clickwrap (i.e. the online 'I

---

[8] Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement', (2010) 18 *International Journal of Law and Information Technology* 248, 252.

[9] Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement', (2010) 18 *International Journal of Law and Information Technology* 248, 252.

[10] Abdullah Ibrahim Al-Nasser, 'Al-Uqoud Al-Electeroneiah: Derash Fiqheyah Moqarenah [Electronic Contracts: Comparative Study on Islamic Jurisprudence]' (in Arabic) (2007) 19 Majallat Albehuth alfiqheyah Almua'aserah, 268.

[11] Abdullah Ibrahim Al-Nasser, 'Al-Uqoud Al-Electeroneiah: Derash Fiqheyah Moqarenah' (my own translation from Arabic) 268.

[12] Abdullah Ibrahim Al-Nasser, 'Al-Uqoud Al-Electeroneiah: Derash Fiqheyah Moqarenah' (my own translation from Arabic) 268.

[13] Chris Reed identified three primary functions of a signature: (i) the signatory identity, (ii) the intention to sign the document and (iii) the adoption of the contents therein: Chris Reed, 'What Is a Signature?' [2000] Journal of Information, Law and Technology at 3.1.3, https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ ; while suggesting similar primary functions, Mason considers authentication of identity to be a secondary function: Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), 7.11-7.19.

[14] For a thorough discussion of different forms of e-signature, see Chris Reed, 'What Is a Signature?' [2000] Journal of Information, Law and Technology and Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), open source at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures .

agree' button), a name in an email and scanned manuscript signatures, and (2) digital signatures, a variation of which is referred to as advanced e-signatures (AES). The latter type usually meets higher technical and authenticity standards by way of encryption technology. While legislation varies in how requirements for e-signatures are categorised and defined, they nonetheless resonate with the above broadly defined categorisation.

Likewise, the recognition of e-signatures through functional equivalence can vary between legislative regimes, which could reflect the cautiousness towards online transformation. Three distinct regulatory approaches currently exist: (1) the prescriptive approach, (2) the minimalist approach and (3) the two-tiered approach.[15] These will be briefly discussed before considering the position in Saudi Arabia.

The prescriptive approach

This approach only accepts a particular technology for e-signatures, often with an encryption mechanism, 'to the exclusion of all forms of electronic signature', [16] an approach which has been criticised. For instance, it has been argued that it is 'burdensome and overly restrictive' because it forces signatories to use the most secure and expensive technology, when simpler means are 'better suited to a particular type of transaction'.[17] Highlighting the reason behind adopting such an approach, Mason argues, 'Many politicians have been misled into the false promise that only digital signatures can be the legal equivalent of a manuscript signature, mainly because of the incorrect assurances that digital signatures are secure and safe from interference'.[18] Mason further criticises the prescriptive manner among policymakers: 'This approach is ambiguous, because it neither provides for legal certainty nor for the further development of e-commerce, as claimed in the recitals of some legislation'.[19]

The minimalist approach

Unlike the prescriptive approach, the *minimalist* approach allows signatories to use any technology that they reasonably believe to be suitable for their purposes. The focus of the jurisdiction adopting such an approach is on 'whether the intent is manifest, and the method is appropriate to the particular transaction'.[20] In other words, a typed name in the email footer would be equally effective in many circumstances as a sophisticated digital signature with a certificate. This approach is not, however, free of criticism. Blythe, for instance, argues that adopters of the minimalist trend 'over-compensate' for technological exclusivity and fail to take into consideration that particular technologies are better than others.[21] Mason, on the other hand, rightly argues that it is somewhat inappropriate for legislatures 'to impose specific technical requirements (such as the use of a digital signature) in the internet age especially as such detailed technical requirements were not imposed in the age of the telegram'.[22]

The hybrid approach

This approach recognises all e-signatures as legally valid but grants digital signatures greater evidentiary presumptions of reliability, authenticity and integrity.[23] As in the prescriptive approach, digital signatures are treated as equal to manuscript signatures in terms of legal weight. In practice it can be unclear whether a particular form of

---

[15] Stephen Blythe, *E-Commerce Law Around the World* (Xlibris Corporation, 2011), 17; Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.7-3.21.

[16] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.3.

[17] Stephen Blythe, *E-Commerce Law Around the World* (Xlibris Corporation, 2011), 17.

[18] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.3.

[19] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.3.

[20] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.10.

[21] Stephen Blythe, *E-Commerce Law Around the World* (Xlibris Corporation, 2011), 18.

[22] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 3.10.

[23] Stephen Blythe, *E-Commerce Law Around the World* (Xlibris Corporation, 2011), 18.

legislation is prescriptive or hybrid, especially when it does not explicitly provide for the level of effectiveness or evidentiary presumption to be given to simple e-signatures.

Definitions of e-signature

The European Union

The concept of the e-signature in the Regulation[24] is largely similar to the Directive[25] with the same hierarchy: simple electronic signatures, AES and QES. Simple electronic signatures are defined almost identically to their previous definition in the Directive, except for the last indent of the definition in which a conceptual confusion has been removed: the e-signature is no longer defined as a mechanism of authentication but is read as 'used by the signatory to sign'. The characteristics of AES have been slightly changed to mitigate the criticism of the Directive's provision. Instead of requiring the use of means that must be maintainable 'under the sole control' of the signatory, paragraph (c) of the Regulation provides that AES are 'created using electronic signature creation data that the signatory can, *with a high level of confidence*, use under his sole control' (my emphasis).[26] While this is seen as more realistic, it still faces many criticisms similar to those of the Directive, especially in light of the lack of 'guidance to the citizen as to how they determine the level of confidence'.[27] Finally, there is no evolution for the QES category, albeit some different wording. That is to say, an AES becomes QES when it is associated with a qualified certificate. As the definition in article 3(14) stipulates, the certificate functions as an 'attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person'. Furthermore, for the certificate to be 'qualified' in accordance with article 3(15), it must comply with and provide the details outlined in Annex I and must be issued by a qualified trust service provider.

The Saudi ETL

The Saudi ETL does not prescribe a variety of e-signatures; rather, it only uses the term 'electronic signature', which is defined in article 1(14) as 'electronic data included in, attached to or logically associated with an electronic transaction used to verify the identity and approval of the person signing it and to detect any change to said transaction after signature'.[28] Although, upon first inspection, this definition seems rather general, a careful analysis suggests that, by adding a signature function (i.e. 'to detect any change to said transaction after signature'), the Saudi definition has taken a prescriptive approach that appears not to provide for simple forms of electronic signature. This feature can only be achieved by encryption technology.[29] The legislature further restricts the concept of e-signatures according to the conditions and specifications required to be provided, which article 14(2) of the ETL delegates to the implementing regulation. Article 14(2) states:

> 'Any person generating an electronic signature shall do so in accordance with the provisions of this Law and the conditions, requirements and specifications set by the Regulations, and shall take into consideration the following ….'

---

[24] 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 [2014] OJ L257/73, OJ L 257, 28.8.2014, p. 73–114.

[25] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures, OJ L13, 19.01.2000, p.12.

[26] Accepting the criticism: Stephen Mason, Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation', *SCRIPTed*, Volume 9, Issue 1, April 2012, 64 – 85, https://script-ed.org/article/informal-debate-on-the-issues-relating-to-terminology-and-clarification-of-concept-in-respect-of-the-eu-e-signature-legislation/ .

[27] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 4.32.

[28] Translation taken from the Official translation of the Bureau of Experts of the Council of Ministers of the Kingdom of Saudi Arabia, https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx .

[29] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 4.33.

These technical conditions, according to the provisions of article 10 of the implementing regulation, are highly similar to the AES characteristics in the EU regime; the only difference is the mandatory linkage with a digital certificate, which is to be issued by an authorised provider, meaning that any signatures other than QES are implicitly excluded by the definition of the ETL.

Therefore, unlike the EU regimes, the definition and characteristics set out in the Saudi ETL and its implementing regulation are not permissive in the sense that they do not accommodate the wide nature of what may constitute a signature. This, as Al-Ajaji rightly argues, may limit the methods of e-signatures and the technology that can be used, which is in contradiction to the principle of technological neutrality.[30]

Legal effect and scope of protection

The EU Regulation

Article 25(2) of the EU Regulation stipulates: 'A qualified electronic signature shall have the equivalent legal effect of a handwritten signature'. Despite the different wording between the Regulation and the Directive, the effect is identical: the legal value equivalent of a handwritten signature obviously implies admissibility. As such, the value of QES can be classified as conclusive evidence in the sense that it 'must, as a matter of law, be taken to establish some fact in issue'.[31] The absence of case law on the matter could explain the clarity attributed to this legal effect. For less secure e-signatures (i.e. AES and simple electronic signatures), which do not meet the law requirements for QES, the Directive included a non-discriminatory clause in article 2.

Although interoperability and legal certainty are priority objectives of the Regulation,[32] national courts have a discretion (for which see Recital 49) to determine the extent to which probative value may be given to simple electronic signatures and AES, which represent the most commonly used forms among the general public. Although Recital 48 notes, 'In specific cases ... electronic signatures with a lower security assurance should also be accepted'.

As noted earlier,[33] common law jurisdictions have not struggled in legally recognising e-signatures regardless of their security sophistication or form. England and Wales, for instance, did so before any legislative framework arose, with the Industrial Tribunal (as it then was) finding that a first name at the end of the email sufficed to constitute a signature, thereby altering the terms of an employment contract upon email exchanges.[34]

In examining the legal effect of an AES, the EU legislature does not differentiate between the types. Professor Murray notes that AES are given 'a different but no greater evidentiary value' than simple electronic signatures because 'their role is within public services'.[35] Nevertheless, since the difference between conclusive evidence and mere admissibility lies in the extent to which the proof needs further support, it may be argued that, in practice, AES enjoy greater probative value than simple electronic signatures when considering the technical standards to which they adhere. This does not mean they cannot be repudiated,[36] although the Council of Europe encourages all states to grant greater legal presumption to all e-signatures by stating: 'The reliability of the electronic data should be

---

[30] Abdulrahman Abdullah Alajaji, 'An Evaluation of E-Commerce Legislation in GCC States: Lessons and Principles from the International Best Practices (EU, UK, UNCITRAL)' (PhD thesis, Lancaster University 2016) 226, https://eprints.lancs.ac.uk/id/eprint/83401/1/2016Abdulrahmanphd.pdf .

[31] Jonathan Law, editor, *A Dictionary of Law* (9th edn, Oxford University Press, 2018), see 'conclusive evidence'.

[32] See, among other things, Recitals 4 and 44 of the Regulation.

[33] Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 International Journal of Law and Information Technology 248. See footnotes (8-9) of this article and the accompanying text.

[34] *Hall v Cognos Limited* (Hull Industrial Tribunal, 1997) Case No 1803325/97. For a longer list of cases, see Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), 7.114 – 7.153.

[35] Andrew Murray, *Information Technology Law: The Law and Society* (4th edn, Oxford University Press, 2019), 427.

[36] For an important discussion of non-repudiation, see Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), 7.286-7.301.

presumed, provided that the identity of the signatory can be validated and the integrity of the data secured, unless and until there are reasonable doubts to the contrary'.[37]

The Saudi ETL

E-signatures that comply with the ETL, which are QES in effect, are given full legal effect, in accordance with the provisions of article 5(1), which reads:

> 'Electronic transactions, records and signatures shall have full effect and their validity and enforceability may not be contested, nor may the execution thereof be stayed on the ground that they were wholly or partially conducted by electronic means; provided that such electronic transactions, records or signatures are carried out in compliance with the conditions provided for in this Law'.

Article 14(1) further stipulates that where a signature is required by law, an electronic signature has the same effect as a manuscript signature. This is reinforced by article 9(1) which repeats that, if electronic records satisfy the provided requirements (among which a qualified certificate is mandatory), 'the electronic transaction or electronic signature shall be accepted as evidence'.

Article 14(3) goes one step further by clearly outlining the legal presumptions for compliant e-signatures:

> 'If an electronic signature is provided in any legal procedure, the following shall be deemed valid, unless proven otherwise or the concerned parties agree to the contrary:
>
> a) The electronic signature is the signature of the person identified in the relevant digital certificate.
>
> b) The electronic signature was provided by the person identified in the relevant digital certificate for the purpose specified therein.
>
> c) The electronic transaction has not been altered since the electronic signature was affixed thereto'.

It is clear that the Saudi regime considers QES to be conclusive evidence. However, what is not clear is whether the ETL has taken a prescriptive approach or a less restrictive hybrid approach. This uncertainty is highlighted by Mason, where he labelled the ETL as a prescriptive-in-nature legislation;[38] this can be compared with the World Bank Group's assessment, which listed it as two-tiered.[39] This discrepancy in understanding comes from the cautious manner taken by the Saudi legislature towards simple electronic signatures and AES, which are considered below.

Chapter two of the ETL concerns the legal effects of e-signatures, e-records and e-transactions. Article 5 stipulates:

> 'Their validity and enforceability may not be contested ... on the ground that they were wholly or partially conducted by electronic means; provided that such ... signatures are *carried out in compliance with the conditions provided for in this Law*' (my emphasis).

In the same chapter, article 9(3) states: 'Electronic transactions, signatures and records shall be deemed reliable evidence in transactions and shall be deemed intact until proven otherwise'. This provision, contrary to the former, suggests that all e-signatures, despite non-qualified ones, may benefit from being presumed as 'reliable evidence'. However, reading it in conjunction with the provisions of article 5 and considering the entirety of the law, it appears that the drafters meant to only refer to compliant e-signatures, QES in particular.

Moreover, while it may seem, at the outset, and testament to a non-discriminatory two-tiered treatment, article 9(2) does not oblige courts to admit noncompliant e-signatures. It reads: 'Electronic transactions or signatures *may* be admissible as presumptive evidence even if their electronic records do not satisfy the requirements set forth in

---

[37] Council of Europe, 'Guidelines of the Committee of Ministers on Electronic Evidence in Civil and Administrative Proceedings' (2019), paragraph 22, https://www.coe.int/en/web/cdcj/digital-evidence .

[38] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 155.

[39] Lillyana Daza Jaller and Martin Molinuevo, 'Digital Trade in MENA: Regulatory Readiness Assessment', (2020, Policy Research Working Paper No. 9199), World Bank, Washington, DC, https://openknowledge.worldbank.org/handle/10986/33521

Article (8) of this Law'. The word 'may' here in contrast with 'shall', as in article 25(1) of the EU Regulation, reflects the ETL drafters' cautiousness towards unqualified e-signatures.

In line with this, article 14(4) excludes simple electronic signatures and AES from the presumptive values granted to e-signatures under article 14(3), as mentioned above, stating, 'If an electronic signature does not satisfy the conditions and requirements set forth in this Law and the Regulations, the presumed validity established in paragraph (3) of this Article shall not apply to said signature nor to the electronic transaction associated therewith'. Notwithstanding this observation, it is only if the court, through its discretionary power under article 9(2), decides to admit a noncompliant e-signature within the ETL meaning, be it a simple electronic signature or an AES, that a three-element test will be applied, as provided by article 9(4), as follows:

> 'When assessing the reliability of an electronic transaction the following shall be considered:
>
> a) The method of creating, storing or communicating an electronic record and the possibility of tampering therewith.
>
> b) The method of maintaining the integrity of information
>
> c) The method of identifying the originator'.

It appears that, to date, neither AES nor simple electronic signatures have been the subject of litigation, which precludes us from seeking further clarity on any approach the judiciary may take.

In sum, in differing from the EU hybrid approach, the Saudi ETL does not oblige courts to accept unqualified e-signatures. At the same time, due to its negation of any presumed validity of such signatures, it stands in stark contrast to the British minimalist regime. This serious derogation of protection has the potential to be a considerable barrier to the diffusion of electronic transactions and e-commerce.

Signatories and their responsibilities

The EU Directive and Regulation

The Directive defined a signatory in article 2(3), which suggested, though not explicitly, that signatories can only be natural persons. The Regulation avoids the problem of its preceded EU instrument by excluding legal persons from the use of e-signatures in article 3(9), which defines a signatory as 'a natural person who creates an electronic signature' and designates another subject matter to legal persons, i.e. electronic seals.[40] This means that, for legal persons (e.g. companies) to take up an e-signature, they have to do so through a human representative. There is a disparity, however, in the need to provide a link in the relationship between the natural person and the legal entity when using e-signatures. Krawczyk explains that this confusion was later acknowledged as 'a risk for the internal integrity of the data', and, consequently, attribute certificates were introduced for companies.[41] This problem could have been avoided in the definition for a signatory. Neither the Directive nor the Regulation established an explicit obligation on signatories to exercise due care in relation to their use of e-signatures. Such obligation may, nonetheless, be implied in the requirements of AES, whose creation data must be maintained by the signatory with a high level of confidence, as provided in article 26(c) of the Regulation.

It might be considered right to leave issues related to the conduct of the signatory to the discretion of national courts. Arguably, uncertainties could have been removed by providing how signatories should reasonably act in relation to their e-signature. Such uncertainties hinder the very objective of e-commerce promotion and e-signature acceptance, which should be achieved by establishing certain, clear and predictable legal instruments. As Brazell

[40] See article 3(25) of the Regulation. Although e-seals may ensure the origin and integrity of data, their purpose and probative value are generally different from those of a signature.

[41] Paweł Krawczyk, 'When the EU qualified electronic signature becomes an information services preventer', 7 *Digital Evidence and Electronic Signature Law Review* (2010), 17.

argues, 'guidance through future case law would of course have been a slow process with potentially years of commercial uncertainty in the interim'.[42]

The UNCITRAL Model Law

Since the EU law is silent on signatory conduct, the provisions of the two-tiered UNCITRAL Model Law on the matter are considered. Article 8(1) of the Model Law provides that 'each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data.' Thus, the due care obligation is imposed regardless of which type of e-signature is used. Sub-paragraph (b) further clarifies signatories' duties, providing that they must:

> 'Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
>
> (i) The signatory knows that the signature creation data have been compromised; or
>
> (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
>
> (c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate'.

These provisions provide for consistency, balance and certainty. In addition, paragraph 2 specifies the allocation of liability when signatories do not comply with their due care responsibility: 'A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1'.

The Saudi ETL

The ETL defines a signatory in article 1(16) as '[a] person making an electronic signature in an electronic transaction using an electronic signature system'. 'Person' is defined in article 1(8) as '[a]ny natural or corporate person whether public or private'. Thus, it was explicitly yet strangely decided that legal persons alongside human beings can sign. This is contrary to the EU regime and is problematic from both conceptual and practical perspectives. As a matter of legal concept, legal persons can only act through their natural agents, especially because 'a legal entity is an artificial construct, and being incorporeal, is not capable of being a signatory'.[43]

Practically speaking, taking the example of signatures on behalf of a company within a QES or AES, all persons authorised to represent the company in different matters (not the company itself) will need to use the company's signature, and, consequently, the private key will no longer be under the sole control of a single person, thereby hindering the claimed advantage behind the use of secure digital signatures. It is assumed that this is a mere legal fiction, as what the legislature seemingly intends by including legal persons in the definition of a signatory is that each natural person should have her own attribute certificate to sign on behalf of such entities. This is confirmed by the practice of the Saudi National Centre for Digital Certification (NCDC), which was established by articles 19 and 20 of the ETL to supervise and provide certification services; it states on its website that digital certificates for entities are 'issued to *persons* within the organization *with specific authority* such as signing special transactions'[44] (my emphasis).

Turning to responsibilities, article 14(2) of the ETL reads:

> 'Any person generating an electronic signature ... shall take into consideration the following:

---

[42] Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd edn, Sweet & Maxwell, 2008) 3, as cited in Jay Forder, 'The Inadequate Legislative Response to E-Signatures' (2010) 26 Computer Law and Security Review 418, 423.

[43] Stephen Mason, 'Revising the EU e-Signature Directive', *Communications Law*, Volume 17 Number 2, 2012, 56, 58.

[44] Saudi National Centre for Digital Certification, 'Types of Digital Certificate', https://www.ncdc.gov.sa/?page_id=3072&lang=en .

> a) Take necessary precautions to prevent unlawful use of signature generating data or the personal equipment related thereto. The Regulations shall specify such precautions.
>
> b) Notify the certification service provider of any unauthorized use of his signature in accordance with the procedures specified in the Regulations'.

Referring to the ETL's implementing regulation, article 11(1) stipulates the following mandatory precautions:

> '1) Maintaining the confidentiality of digital certificate and documents issued by the electronic signature certification service provider and not permitting any unauthorised access to them.
>
> 2) Applying appropriate techniques and safe solutions as per digital ratification procedures'.

Moreover, article 11(3) of the implementing regulation, mirroring article 14(2)b of the ETL, obliges signatories to report any unauthorised use to a CSP with related documentation as soon as he or she is aware of such illegal usage.

Additionally, article 22 of the ETL, which has the heading 'Responsibilities and Obligations of Certificate Holders', provides obligations on signatories to give accurate data to CSPs and to notify them in the case of any modifications provided in the certificate, and prohibiting the reuse of any elements of any previous e-signatures with another CSP if the certificate associated with that e-signature has been suspended. These provisions, although differently worded, reflect and achieve similar outcomes as those in article 8 of the Model Law. However, they only apply to certificated e-signatures, and are not relevant for other forms of signature. They also do not specify the allocation of liability in case of negligence. Yet presumably, liability is assumed for any failure to comply in accordance with the provisions of article 27 of the ETL.

Relying parties and their responsibilities

The EU

The Directive neither defined the relying party nor explicitly provided for the duties that a recipient of an e-signature must assume before relying on the signature. However, in Annex IV, it states, 'During the signature-verification process it should be ensured with reasonable certainty ...', and thereafter lists several recommendations, including '(c) the verifier can, as necessary, reliably establish the contents of the signed data'. While it is imperative to provide for a minimum obligation on the relying party to conduct reasonable checks on e-signatures prior to reliance, Mason suggests, 'Given the complexity of this issue, ... it was probably considered right to leave this to the judges to resolve in the event of disputes'.[45] It is a complex issue, especially as what is reasonably satisfying for the relying party would significantly differ in the case of simple electronic signatures compared to AES and to e-signatures with an associated certificate. Nevertheless, it would have been desirable to provide an explicit duty of conducting reasonable verification for the relying party rather than mere recommendations. Clearly, the drafters deliberately intended not to impose any obligations, as evident in the plain language of the title 'Recommendations for secure signature verification' in Annex IV; Mason further comments: 'Had it been intended to impose such a duty on the recipient, no doubt it would have been made explicit in the Directive'.[46]

The Regulation, on the other hand, defines a relying party in article 3(6) as 'a natural or legal person that relies upon an electronic identification or a trust service' but, like the Directive, does not impose due diligence duties in explicit terms. Mason found that '[t]he only reference to the need for a relying party to assure themselves of the validity of a signature is in recital 57'.[47] The recital reads:

> 'To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation ...'.

Although implicit, the recital is more explicit than the Directive in addressing the need for relying parties to reasonably check the validation of the e-signature on which they will be relying.

---

[45] Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 134.

[46] Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 134.

[47] Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), 161.

The absence of a requirement to conduct due diligence exercises on the part of both the signatory and the relying party in relation to QES may lead to undesirable consequences, thereby hindering the promotion of the very e-signatures that are considered to have a favourable legal effect in the two-tiered approach. Particularly, it can be assumed that both parties, in order to be certain of the legal effect of their transaction signed by a QES, have to assure themselves that it matches the various technical requirements set forth within the legislation. In other words, 'a check list of 30 items which, if met, bring[s] the signature within article 5(1) [of the Directive]', granting it full effect.[48] Such an interpretation, although radical, is assumed by Professor Reed, who accordingly heavily criticises the Directive (which is worth quoting in full):

> 'To decide if a particular e-signature technology can be accepted as producing the equivalent to a hand-written signature, the relying party needs first to consult a legal specialist to identify which parts of the 30 item checklist are important and what they mean in the context of the particular transaction. Then a technical expert needs to be consulted to produce an opinion on whether those requirements of the checklist have been met. Finally, the legal expert needs to review the technical expert's opinion, to produce a further opinion as to whether a court would be convinced by the technical expert's argument. If this is certainty it is a very uncertain type of certainty'.[49]

The analysis by Mason, adopted in this article, disputes such an interpretation, given that the technical requirements for legally effective e-signatures are to be met, in essence, by CSPs. This is what the plain language of the Regulation (and the Directive) provides for.[50] Notwithstanding, had reasonable and sufficient responsibilities been explicitly placed on signatories and relying parties in their use of QES, any doubts or alternative interpretations would have been eliminated.

The Saudi ETL

Article 14(5) of the ETL obliges relying persons to 'exercise due diligence in verifying the authenticity of the signature, using relevant electronic signature verification data in accordance with the procedures set forth by the Regulations'. Referring to the implementing regulation, article 12(1) requires relying parties to ensure that (1) 'the certificate of the sender has been issued by a licensed provider of certification services … and verify its validity'; (2) the details in the attached data, including address and name thereof, match those of the signature holder based on the certificate; and (3) there is no alert indicating any defect in the signature or attached data. Moreover, article 12(2) provides, strictly, that failing to satisfy any of the verification elements will result in the e-signature being deemed voidable and unrelated to the data originator.

When it comes to relying on QES, the abovementioned provisions are effective, in that they outline with clarity the reasonable checks to be made in order to rely on a QES. It is easy to check whether the CSP is licensed through the published list of certified CSPs by the enacted supervisory body, the Saudi NCDC. The remaining elements can be checked by contemplating the certificate itself. Nonetheless, there is again an evident exclusion of other forms of e-signature, as the obligations are only relevant and implementable when there is a certificate. The provision in article 12(2), which effectively links the legal validity of e-signatures to the achievement of such obligations, makes it even clearer that the legislature had only QES in mind.

In this respect, the ETL and its implementing regulation are different from the Directive and the Regulation, neither of which outline the relying party's obligations except with an indicative yet unrestrictive provision. It is worth noting that the ETL approach is also distinct from the approaches of '[t]he other GCC Member States [which are] … more

[48] Chris Reed, 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73.6 *Modern Law Review* 903, 907.

[49] Chris Reed, 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73.6 *Modern Law Review* 903, 907.

[50] Certification Service Providers (also referred to as 'Trust Service Providers' in the Regulation) are subject to the technical requirements as well as exposed to liability provisions in both EU frameworks. See, for example, article 6 and annex II of the Directive and recital 35, article 13, article 19 and section 3 of the Regulation. This article however, as indicated in its introduction, does not explore the status of those providers.

tolerant ... [as] they do not limit recognition to advanced digital signatures associated with a certificate. Both types are accepted when addressing the issue of the conduct of the relying party'.[51]

Conclusion

This article has critically discussed the e-signature regime of the 2007 Saudi ETL, in reference to the evolution of its counterpart EU instruments, the 2014 Regulation and the repealed 1999 Directive. By analysing the regulatory approaches to e-signatures, the article notes that civil law jurisdictions tend to follow a stricter approach, which reflects the significance of form, whereas the common law world tends to follow a minimalist approach. In this respect, Islamic law jurisdictions, at least in principle, enjoy the flexibility to regulate e-signatures with a pure functional equivalence perspective, similar to common law countries. This is because Sharia law does not impose much importance on form.

Contrary to the EU regime, the Saudi ETL defines and characterises e-signatures in a discriminatory manner which does not keep pace with the wide nature of what may constitute a signature, and provides for a function that can only be met by encryption technology. In terms of legal effect, the ETL concurs with the EU regime in legally recognising QES as having the equivalent effect of handwritten signatures. However, while the EU has adopted a two-tiered approach that admits all types of e-signatures, the Saudi ETL and its implementing regulation, despite a few confusing provisions, are highly prescriptive and in favour of QES to the exclusion of simpler e-signatures. Even regarding signatories and relying parties, unlike the EU regime, which left their conduct and responsibilities to national courts, such issues are explicitly detailed and regulated in the ETL, yet formulated in such a way that only prescribes for QES, with no relevance to uncertificated e-signatures.

With its overly restrictive approach, the ETL contradicts the principle of technological neutrality and risks invalidating everyday transactions that can be demonstrably genuine, for which sophisticated security is both burdensome and irrelevant. Since Sharia rules are permissive, there is nothing to preclude the legislature from taking into account the appropriate facilitation of e-signatures regardless of technology or form insofar as the primary functions of a signature are achieved. Thus, given the quantum leap in e-commerce and its potential in Saudi Arabia, based on these findings, Saudi regulators are urged to introduce a minimalist approach to e-signatures similar to the UK framework or, at least, to a two-tiered model such as the EU regime. If the legislature deemed its approach appropriate in 2007, the increasing reliance of ordinary people and SMEs on online transactions today compels different, permissive and careful consideration.

Oways Kinsara is a Saudi Arabian legal researcher and, at the time of writing, an LLM candidate at the London School of Economics and Political Science, London

O.kinsara@gmail.com

[51] Abdulrahman Abdullah Alajaji, 'An Evaluation of E-Commerce Legislation in GCC States: Lessons and Principles from the International Best Practices (EU, UK, UNCITRAL)' (PhD thesis, Lancaster University, 2016), 231.