VALUE OF ONLINE IDENTIFICATION IN COMPARISON WITH ELECTRONIC SIGNATURES

1. Introduction

With the emergence of information and communication technologies, Internet has become a crucial part of the digital relations which allowed individuals to make contact with each other without any physical interaction. Under these circumstances, the nature of the transactions had changed and transferred into the electronic world which gave rise to new business methods like e-commerce and other Internet services.

In the physical world, majority of the transactions does not require a proper identification process of the parties.[1] When the need arises, identity and any alteration made in the document can be ensured through manuscript signatures, stamp or seal.[2] However, when it comes to the Internet based transactions, it is more likely to desire to find the answer of who you are really dealing with which makes crucial to identify the counterpart. In this respect, as manuscript signatures are not suitable with the digital world, electronic signatures and relevant technologies which we call digital signatures had been developed for electronic documents. Both national and international legislations came into force to create an equivalent legal effect with the traditional signature. Notwithstanding, a great deal of issues occur in the context of identification function of the electronic signatures.

This paper will explore the importance of online identification and the underlying reasons of why online identification is more important than electronic signatures. This essay consists of three sections. The first part of the paper will examine the definition of online identification in the digital context and the purpose of the electronic signature along with the legal effect. Secondly, it will discuss the importance of the online identification in terms of providing security in the commercial transactions associated with electronic signatures. Last part will present the attribution of liability and allocation of risk as a result of electronic signature use.

2. What is Online Identification via Electronic Signature?

As digital relations are emerging between businesses, or between businesses and consumers, the significance of holding a true identity of the counterpart is increasing. Commonly, “genuine identity” refers to all the characteristics such as name, address, e-mail, etc. which are mostly unique to a person.[3] However, Internet enables individuals to have a digital identity different from the real world identity. In the electronic world, anyone could pretend to be like someone else in several ways such as setting up an e-mail account with false details. On the Internet, individuals present characteristics dissimilar to the ones in the physical world, because interaction with each of the website visited is different which leads

[1] Reed C, *Internet Law: Text and Materials* (2nd edn, Cambridge University Press, 2004) 143.
[2] Ibid, 141.
[3] Rafael Martínez-Peláez, Francisco J. Rico-Novella and Luis A. Zarza-López, 'DIGITAL PSEUDONYM IDENTITY FOR E-COMMERCE' <https://www.researchgate.net/publication/221436435_Digital_Pseudonym_Identity_for_E-Commerce> accessed 3 December 2019.

into having various profiles of who you really are[4]. This is simply related to as “partial identities” which is named as “a persona”, since none of them has a power to construct the exact identity.[5] In consequence, it is quite complicated to determine identity.

According to Chris Reed, majority of the online transactions require consumers to click on the purchase button and share the payment details. However, this approach would not fit with the transactions include contracts with larger values, since there is a necessity for the parties to identify each other and be sure that the terms of the contract has been adopted.[6] This is why as the new digital services are emerging, many organizations or Internet users are considering the ways of dealing with the concerns related to: (a) identification of the counterpart, and (b) providing secure and legally binding digital business transactions. Aforesaid demand emerged the need of understanding the electronic signatures more deeply and create trustworthy ways to ensure a reliable e-commerce environment.

An electronic signature can provide evidence of: (a) the identity of the signatory, (b) his intention to sign, and (c) his intention to adopt the contents of the document as his own.[7] Nicholas Bohm and Stephen Mason define the purpose of an electronic signature is to provide the authenticity of the individual using it, constitute identity relationships and specify the liability in the digital economy.[8] An electronic signature could be a name typed under an electronic document, an electronic sound, or digital signature. However, not all the electronic signatures provide equal and sufficient evidence for authenticity of the signatory. A name written under an email cannot be expected to provide further trust than an encryption technology.

There is no doubt that electronic signatures technology is almost the best product of maintaining the e-commerce business in a trustworthy environment. Nevertheless, as it is stated above this structure has faced some problems in practice related with authentication problems which this essay will discuss below.

3. Security of the Transactions

Increase of the global trade volume in parallel with the emergence of the digital technologies had effectively removed some of the barriers take place in the commercial transactions. Rather than being in presence physically, majority of the businesses and consumers are now choosing to enter into contracts by affixing electronic signatures on the document because of

[4] 'Understanding Your Online Identity An Overview Of Identity' (Internetsociety.org) <https://www.internetsociety.org/wp-content/uploads/2017/11/Understanding-your-Online-Identity-An-Overview-of-Identity.pdf> accessed 3 December 2019.
[5] Ibid.
[6] Christopher Reed, ‘Legally Binding Electronic Documents: Digital Signatures and Authentication’ (2001) 35 Int’l L 89.
[7] Reed C, 'What is a Signature?', 2000 (3) The Journal of Information, Law and Technology (JILT). <http://elj.warwick.ac.uk/jilt/00-3/reed.html/>. New citation as at 1/1/04: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/>
[8] Nicholas Bohm and Stephen Mason, 'Identity And Its Verification' (2010) 26 Computer Law & Security Review.

its marginal cost, utility and ease of use.[9] Contribution of digitalization will foster the economic prosperity and sustainability of the development of the businesses.[10]

On the other side, preserving the process of an online transaction and ensuring the identity of the parties have become the main issue because of the security concerns. One of the main purpose of an electronic signature is to identify the person who owns it. However, not all the electronic signatures are providing same level of identification function[11]. For instance, a digital signature technology serves a better guarantee than a scanned image of a manuscript signature in the means of identifying the counterpart[12]. This is because a digital signature is accompanied with a certificate and accreditation scheme, while a person who sends his scanned signature relinquishes the control over it[13]. Also, there are a lot of ways to be sure of the identity of the transaction holder, depending on the method of electronic signature. It could be a simple password for the use of a credit card or it may amount to a digital signature. In each way content of the data is send to the recipient who will check whether the identity of the sender matches with the signature. As a result, security level and proofing the link to the signatory presented by each signature model in the online context differentiates.

On of the main challenges that electronic signatures face in the way of promising security is Internet, since it is not secure enough to maintain such transactions.[14] For instance, in the daily basis, majority of the companies are satisfied while conducting transactions by sending emails without any need of further authentication other than typing names or adding address. Since communication through emails are send via satellite transmissions and saved in the servers database, an unauthorized individual can gain access and pursue or alter the content easily.[15] Fraudsters may go beyond and act as a lawful trader by composing false websites[16]. In the case named *Bassano v Toft*[17]*,* clicking on the "*I accept*" button to approve the consent of entering into an agreement in the course of purchasing an online good or service has became another way of authentication. It is concluded that the word "*I*" appears to be the mark referred to the signatory. The problem with such a signature is that the creditor has only clue about someone clicked on the button, but no trace related with who actually performed it. "*The nexus between the action of clicking the icon and the identity of the person who purported to order the items may be difficult to resolve, bearing in mind the security risks associated with using the internet*."[18] In conclusion, since there is no physical document to adduce or no information about the identity of the counterpart, the nature of the online

[9] Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods. New York, United Nations.
[10] (Itu.int, 2020) <https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf> accessed 10 December 2019.
[11] Andrew Murray, Information Technology Law: The Law And Society (3rd edn, Oxford University Press 2016) 510.
[12] Ibid, 511.
[13] Stephen Mason, Electronic Signatures In Law (School of Advanced Study, University of London 2016), 152.
[14] Paul Todd, E-Commerce Law (Routledge-Cavendish 2005), 103.
[15] Yaman Akdeniz, 'UK Government Policy On Encryption' [1997] SSRN Electronic Journal.
[16] Ibid (n 14) 105.
[17] Bassano v Toft & Ors [2014] EWHC 377 (QB)
[18] Ibid (n 13) 208.

communications face with more infringement on the process and invasion into the transaction.

To overcome this problem, developing world has tried to find solutions such as encryption technology which is the product of the e-commerce transactions. Public-key infrastructure ("PKI") is a method to provide security for commercial electronic transactions.[19] Public-key certificates are held by some trusted third parties whom store the relevant information of the certificate holder and revoke or update the certificate when it is necessary.[20] However, it is obvious that companies are sharing some private datas about their commercial operations which basically results in being in the hands of the PKI service provider.[21] Even though the purpose of security relies under the ultimate aim of PKI, sharing information about the company will create a crack in the company's security wall.

Even though some commentators support that one of the best advantage of a digital signature is to have a value in proving the origin of the data and that no alteration had been made[22], this view has not been supported widely. This idea is named as non-repudiation in the digital signatures terminology. A digital signature demonstrates that a certain private key was used, rather than indicating the document was signed by the person who owns the private key.[23] Since the owner of a digital signature may not be able to preserve the sole control over it or code of the encryption system can be broken, there may be a case of forge the signature.[24] As Stephen Mason states "[*t]he difference between a digital signature and clicking an icon is a narrow one*."[25] All these possibilities indicates that unauthorized or inconvenient use[26] will be a matter of deal which lead the recipient of the key into confusion about the signatory's identity. Even though it is commonly viewed that digital signatures are the best imprint of the communications in the electronic world, they still have issues related with the identification and preserving the security transactions.

In despite of the presence of a valid electronic signature, bringing online identification function into the forefront is significant in order to minimize the risk of fraud and identity theft. According to Petr Sveda and Vaclav Matyas, this issue could be solved through implementation of a "restrictive configuration" system which means a specified computer with the private key used only by the owner of the key and for restricted purposes.[27] This could be a way to obstruct fraudulent transactions carried out by the fraudsters which may cause countless harm to a businesses such as loss of confidential information, or disruption of the company's affairs. Giving online identification prominence will provide mutual confidence among the trading parties or purchasers.

---

[19] Ibid (n 14) 516.
[20] Ibid (n 1) 145.
[21] Ibid.
[22] Francisco Jordan-Fernández, 'Electronic Signature Today: A Manufacturer'S Wiewpoint' (Static.safelayer.com, 2004) <https://static.safelayer.com/www/images/stories/pdf/up5-3jordan.pdf> accessed 10 December 2019.
[23] Lorna Brazell, Electronic Signatures And Identities (London: Sweet & Maxwell 2008), 135.
[24] Ibid (n 1) 147.
[25] Ibid (n 13) 209.
[26] Ibid (n 13) 156.
[27] Ibid (n 13) 156.

4. Attribution of Liability and Allocation of Risk

As far as online identification is concerned, one of the main issue must be dealt is liability in regard of the use of electronic signatures. In order to defeat the liability issues, majority of jurisdictions impose legal presumptions related with the electronic signatures. One of them is "*that the apparent signatory did in fact make the electronic signature*."[28] The individual who intended to create an electronic signature has also given the consent of adopting the terms of the contract which make him liable for the possible legal disputes. To acknowledge the authenticity of the identity the link between the signatory and the signature should be proved. However, as it is exemplified, electronic signatures and even digital signatures does not indicate correctly whether Alice is Alice. In such a case, attribution of liability and allocation of risk would become an issue that is difficult to solve.

According to Chris Reed, majority of the online business-to consumer ("B2C") transactions requires consumers to click on the purchase button and share the payment details.[29] There is a possibility for a third party fraud, but this is a risk that could be taken by the traders.[30] Therefore, being sure about the legally binding force of the contract is relatively enough.[31] However, this approach would not fit with business-to-business ("B2B") transactions, since larger values are a matter of the contracts which created a necessity for the parties to identify each other and be sure that the terms of the contract has been adopted.[32] Various kinds and levels of liability will be generated upon this outcome. The importance of this appears in holding promises and meeting the expectations of the contracting parties which are valuable within the context of increasing the economic welfare of the digital society.

Any form of electronic signature technology or digital signature may be unsuccessful to identify the person who signs the document which will result in the occurrence of liability issues. In some of the jurisdictions, an email address is considered to be an electronic signature.[33] However, in the case named *J Pereria Fernandes SA v. Mehta*[34], a personal guarantee was given regarding to the company's debts by sending an email, but the name of the sender was not typed under it. According to the final judgement, because only mail address was appended to the document, there was no act made by the sender which is linked that intention of signing the document could not be confirmed.[35] The from address was not considered to be sufficient enough to identify the sender of the message. In the daily basis, majority of the people have little or no doubt about the identification function of an email, especially considering that there were exchange of emails. Even though an email address is commonly considered to be an electronic signature, in this case it was held that it is not serving any identification function. Counterpart of the communication depended on the promise, but still had faced with economic loss which should be compensated. Liability perspective of this kind of a judgement is detrimental.

---

[28] Singapore Electronic Transactions Act 1998, s 18(2)(a).
[29] Ibid (n 6) 89.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] See example cases: SM Integrated Transware Pte Ltd v. Schenker Singapore (Pte) Ltd
[34] Bassano v Toft & Ors [2006] EWHC 813 (Ch)
[35] Ibid.

ID Certification schemes have been used for the purpose of identification of the signatory and developed in this perspective. However, this system is not practical, since plenty of liability issues may occur which makes it unreliable within the context of commercial transactions. Under normal conditions, information supplied by the signatory has been received by the Certification Authority ("CA") which offers different security levels of the certificates depending on the information. On the other hand this issue changes when it comes to practice. As Chris Reed explains, CA involves into an agreement with a third party called Registration Authority ("RA") which could be a corporation or trade association. The RA supplies the information to the CA regarding its employee or members to validate an electronic signature. Then the ID Certificate is issued which indicates that the identification process has been held by the RA, and not by the CA. This type of an identification method does not comply with the liability provisions stated under the electronic signature laws, since they only consider the incorrect information involved in the ID Certificate which is provided by the CA.[36] As online identification information is not supplied properly by the RA, electronic signature attached to the document would not serve any identification purpose which will result in loss of the individual who relies on the transaction that must be covered. In consequence of not having any provisions, there will be issues related with the liability of the RA.

Liability and risk issues are mostly associated with "relationship with access control to the electronic signature." [37] The owner of an electronic signature accepts to have full responsibility of maintaining the control over any form of electronic signature. The receiver of the document cannot always have an opportunity to examine whether the sender is the one who purports to be. Recipient will try to avoid investigating the position of the sender is not practical in the means of commercial life. Currently, attribution of liability and allocation of risk in regard of electronic signature use is provided by contracts and statutes.[38] Mason recommends the parties to have clear contractual terms to avoid any possibility of dispute.[39]

5. Conclusion

The emergence of the digital world had enabled users to participate into different kind of contracts which were held through Internet by electronic signatures. This paper has argued the vital aspect of the online identification and the reasons of the greater value in comparison with electronic signatures. Since there is no imprint of these transactions in the physical world, it creates many challenges which cannot be solved by any legal model.[40] As it is explained two of which was the security problems, together with, liability and risk issues associated with the use of electronic signatures. In order to increase the accountability of the Internet based transactions, it is important to adopt some measures both technically and legally. This clarifications should help the sender and receiver to be sure about the enforceability of the contracts and avoid the damages that could occur in respect of innocent parties.

[36] Ibid (n 1) 150.
[37] Nicholas Bohm, 'Watch What You Sign!' (2014) 3 Digital Evidence and Electronic Signature Law Review.
[38] Ibid (n 13) 178-179.
[39] Ibid 213-15.
[40] Ibid (n 1) 308.