Centro Sur Vol. 5 No. 3 - July - September – Revista Centro Sur - eISSN: 2600-5743

http://centrosureditorial.com/index.php/revista

Application and implications of digital signatures and certificates within the framework of law 27269 - Peru

Aplicación e implicancias de la firma y certificados digitales en el marco de la ley 27269 - Perú

Gaby Jessica Nieto Fernández
Magister in Public Management, Ministry of Energy and Mines, Lawyer, Universidad San Martín de Porres, gjnieto@gmail.com , https://orcid.org/0000-0003-0303-9915

Abstract

This research seeks to identify the befits of the application and implications in Peru of Law No. 27269 "Law on Digital Signatures and Certificates", modified by Law No. 27310 and how its application has contributed to the progress of its optimization in the public and private sphere within the framework of the establishment of electronic government in Peru and more than 19 years after its entry into force, the Regulation of Law No. 27269, approved by Supreme Decree No. 052-2008-PCM, seeks to regulate the use of digital signatures and the regime of the official infrastructure of the electronic signature, looking for different levels of guarantee and security in order to give the same legal effectiveness and validity that is given to the same legal effectiveness and validity that is given to the official infrastructure of the electronic signature. 052-2008-PCM, seeks to regulate the use of digital signatures and the regime of the official infrastructure of the electronic signature, looking for different levels of guarantee and

https://doi.org/10.37955/cs.v5i3.165
Received November 12, 2020 / Approved April, 03 2021 Pages: 122-133
eISSN: 2600-5743

security in order to give the same legal effectiveness and validity that is given to the handwritten or other similar signature, however there have been problems for its application, which we will analyze in order to propose possible alternatives for a better control and safety mechanism.

Resumen

La presente investigación, busca identificar los beneficios de la aplicación e implicancias en el Perú de la Ley N° 27269 "Ley de Firmas y Certificados Digitales", modificada por Ley N° 27310 y de qué forma su aplicación ha contribuido en los avances de su optimización en el ámbito público y privado dentro del marco de instauración del gobierno electrónico en el Perú y a más de 19 años de su entrada en vigencia, el Reglamento de la Ley N° 27269, aprobado por Decreto Supremo N°052-2008-PCM, busca regular la utilización de las firmas digitales y el régimen de la infraestructura oficial de la firma electrónica, buscando diversos niveles de garantía y seguridad a fin de dar la misma eficacia jurídica y validez que se da a la firma manuscrita u otra análoga, sin embargo se han presentado inconvenientes para su aplicación, las mismas que analizaremos a fin de plantear posibles alternativas para un mejor control y mecanismo de seguridad.

Palabras clave/ Keywords

Electronic signature, Digital signatures, Digital Certificates, Electronic Government, security levels

Firma electrónica, Firmas digitales, Certificados Digitales, Gobierno Electrónico, niveles de seguridad

Introduction

In a globalized world like the one we live in today, where all commercial operations are being carried out through electronic mechanisms, where from the comfort of home or work through a cell phone or computer, you can make purchases, payments and all kinds of commercial operations, a situation that makes Latin American countries are concerned about reducing the existing digital gap between private companies and governments, so that within their policies they promote the advancement of their digital agenda, in order to put technology at the service of the citizen (Porrúa, 2019).

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

Telecommunications have grown exponentially by technology, giving greater ease to perform daily activities, both in companies and at home (Torres and Oviedo, 2020; Govin, 2019, p. 4). ICT is an essential part of the organization, it generates and achieves productivity and sustainability effects that improve the organization Duche, Galvez, Marallano (2019). Currently, it is in constant change thanks to technology and globalization, therefore ICTs have an important role intervening in all sectors of society (Villao, 2016, p 43).

However, according to a study published by the Inter-American Development Bank in Latin America, less than 30% of procedures can be carried out entirely online and only 7% of citizens carried out their last procedure online, with the paper or certificate policy persisting. The march towards a government is still underway, requiring the commitment and investment of countries committed to making the benefits of technology available to citizens in order to meet their needs (Porrúa, 2019).

Peru has been no stranger to the implementation of digital government policies, for which, among others, it enacted Law No. 27269 "Law on Digital Signatures and Certificates", amended by Law No. 27310, a rule that seeks to incorporate into the Peruvian legal system certain legal figures to ensure the safeguarding of information and its transmission through electronic elements through the use of cryptographic techniques. When it comes to public policies, it implies "State in action" through the regulations of the political system for the resolution of public problems (Olivar, 2019). For Salvador (2001), the digital signature is presented as a necessity by the private and public sector, providing a solution for network security policies (p.52).

Likewise, the aforementioned regulation seeks to establish the regulatory framework for the use of electronic signatures, which is granted the same validity and legal effectiveness as that enjoyed by handwritten or analogous signatures, by means of which people seek to unquestionably manifest a certain will.

However, digital signatures and digital certification have not yet been effectively implemented in Peru in public companies due to the lack of implementation of ICTs and digital technical infrastructure, such as software and hardware. In private entities, the lack of implementation of control and security mechanisms has not made the implementation of electronic signature and certification feasible.

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

According to Law No. 27269, we must bear in mind that the electronic media is insecure by nature, in order to achieve an adequate level of security for the persons involved in electronic transactions, it is necessary to use a series of technical, legal and organizational tools that make the process of exchange of goods and services in the electronic world viable, a space where it is essential to properly identify the parties involved in the various transactions and operations that occur in this area.

On this matter following Espinoza (2018) we can point out that:

> "In this context, Peru cannot be a stranger to a reality whose legal problems must be solved from computer law, (...) with a computer vision, where law and technology come together to facilitate electronic operations in globalized and interconnected environments. Thus, the Peruvian legal system has adapted to the new demands of modern times. In accordance with the advances of computer law, it has regulated in various regulatory bodies both electronic signatures and digital signatures". (p.242)

In this regard it should be noted, following the parameters established by Espinoza (2018), that:

> "Computer Law provides us with a series of institutions that [facilitate] the development of prevention mechanisms for all those undesired situations for the users of the New Information Technologies, in such a way that when certain circumstances of affectation arise, there are new legal institutions that generate confidence to the persons [such as public and private entities] that carry out operations by electronic means (...). (p. 293).

In this sense, Flores (2014), (Gamboa et al., 2019), defines Computer Law as a branch of law "(...) of a multidisciplinary nature, consisting of the set of legal rules that aim to regulate relationships and legal acts arising around information technology and the use of computer media (...)." (p. xvi), in this regard we must take into account that the definition proposed needs to be complemented with aspects related to doctrine, jurisprudence and legal research.

It is important to highlight that Computer Law is the new branch of Law that allows to give adequate solution to the problems generated by the use of Information and Communication Technologies -ICTs, therefore, it is the one called to study, analyze and seek answers to the

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

growing problems related to the level of use of Electronic Signatures in general and Digital Signatures in particular.

Several technical tools must be taken into account, highlighting those that can be configured both at hardware and software level. Regarding the first aspect, a server that supports digital certificates and the key pair (public key and private key) is required; in addition, these elements must be configured to the level that allows the web interaction with the certification and registry entities.

At the hardware level it is also essential to use cryptographic USB tokens with their respective connectors and USB ports, which allow the storage of electronic certificates, the key system or keys, all directed to be applied by the users of the system. The aforementioned devices must have a certain memory capacity, must support the operating systems required by the parties, and must have some level of coating that allows their isolation, guaranteeing possible contingencies that may arise. It is always required to analyze the legal aspects of the hardware, in view that at all times, to interact with digital signatures and certificates must interact in both the physical market and the digital market.

As for the software, it is first necessary that it is accredited by INDECOPI, as the entity that regulates and verifies the systems of Digital Signatures and Certificates. The immaterial element must have its respective software use license, which allows users to be lawful, thus avoiding possible sanctions for software piracy, with the legal consequences of such facts.

In any electronic transaction it is of vital importance to determine the identity of the holder of the digital signature. In this context, it is essential the provisions of Article 4 of Law 27269, which states that "The holder of the digital signature is the person to whom a digital certificate containing a digital signature is exclusively attributed, objectively identifying him/her in relation to the data message.

In the electronic medium it is essential to determine the identity of the person to whom the digital certificate will be assigned, the latter being understood as that electronic document that presents all the necessary elements to fully identify the holder of the digital signature system.

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

The verification or registration entities play a very important role, since they are the ones called to fully comply with these functions, and if they do not perform their identification work properly, serious problems can be generated to the system of digital signatures and certificates, especially at the level of loss of confidence, which would correspond to a negative externality for the development of electronic transactions.

In this sense, the digital certificate is signed by the certification entity, and binds the signatory to each electronic transaction that he/she signs.

The responsibility for the signing of electronic transactions, it is essential to take into account that Article 5 of Law 27269, expressly states the obligations of the holder of the digital signature, in this regard states that "The holder of the digital signature has the obligation to provide to the certification entities and third parties with whom it is related through the use of the digital signature, accurate and complete material statements or manifestations".

Digital signatures and digital certification are developed in a very sensitive context, where personal data, information of obligations and contracts, etc., circulate, then, due to the insecurity of the electronic medium itself, it is a fundamental obligation of the holder of the digital signature to provide completely accurate statements or manifestations of will, to avoid any violation to the digital signature system, and thus avoid any kind of insecurity to electronic transactions in general in which the parties involved in such context trust (Ovidio, 2006).

It is necessary to emphasize that the holder of the digital certificate will be responsible for the use of the pair of keys, namely, a public key and a private key, both generated in the context of an asymmetric cryptography system, that is, the science of encryption that provides high levels of security to electronic transactions.

The Law on Digital Signatures and Certificates, since the year 2000, established the conceptualization of the digital certificate. In this sense, according to Article 6 of Law 27269, the digital certificate is defined as "(...) the electronic document generated and digitally signed by a certification entity, which links a pair of keys with a specific person confirming his/her identity".

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

It must be taken into account that for the generation of the digital certificate a certification entity that has reliably accredited the identity of the holder of the digital certificate participates, this process can be done directly by the certification entity when it has registration entity functions, otherwise it must delegate this function to a registration entity, institution that ultimately has the obligation to clearly determine the identity of the holder of the digital certificate, to whom the key pair will be attributed, for the purposes of the signed.

The holder of the digital certificate will be responsible for the use of the pair of keys, namely, a public key and a private key, both generated in the context of an asymmetric cryptography system, that is, the science of encryption that provides high levels of security to electronic transactions.

Within the scope of the provisions of Law 27269, it is important to take into account that digital certificates are issued by certification entities and not by registration entities; Article 7° of the aforementioned law, which informs us about the content of the digital certificate, in the following terms:

The digital certificates issued by the certification entities must contain at least:

1. Data that unmistakably identifies the subscriber.
2. Data identifying the Certification Entity.
3. The public key.
4. The methodology for verifying the subscriber's digital signature imposed on a data message.
5. Serial number of the certificate.
6. Validity of the certificate.
7. Digital signature of the Certification Entity

It is also essential to take into account the data identifying the certification entity, since the issuance of the digital certificate and the generation of the digital signature system depend on that entity, both at hardware and software level.

The Peruvian legal system requires that the public key be included in the digital certificate, and it should be understood that it refers to the validation mechanisms and the way to access it in the electronic media,

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

for the purpose of its recognition, always in a context of technical authentication.

In relation to the legal framework, legal instruments with the status of law are required to give value to such operations, and an adequate legal framework is needed to provide the legal support that will enable users of virtual environments to have the ideal frame of reference for their permanent interaction in the electronic world.

In Peru, Law No. 30096 "Computer Crimes Law" has been passed, which aims to prevent and punish unlawful conduct affecting computer systems and data and other legal assets of criminal relevance, committed through the use of information or communication technologies, in order to ensure the effective fight against cybercrime (Dávila, 2020).

In this case a legal asset is protected, such as: confidentiality, integrity and availability of information. The use of new technologies generates progress, however, when used for illicit purposes, such as accessing private information with the intention of causing harm, it only causes economic damage.

In Peru, the most common computer crimes are: fraud, hacking, malicious propagation of a virus, identity theft, terrorism, child pornography, sending e-mails to obtain pishing data (obtaining private information such as bank account passwords and e-mails), espionage to capture company information, card cloning, obtaining personal and business information, bank fraud, online extortion, theft of intellectual property data, attacks on Internet providers, among others.

In most computer crimes, the cybercriminal, is the person who has computer and systems knowledge which would allow him/her to gain unauthorized access to public or private terminals (illicit access), breaking or transgressing all security systems (Rodas and Loor, 2017).

In computer crimes, the purpose is to prevent access and make the operation of the system impossible, this is the main purpose and there must be malice (knowledge and willingness to commit the crime). In computer crimes, the damage is to be assessed and in this case the misuse of information technologies is punished (Vela, 2020).

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

Materials and Methods

This research used the inductive method, through an analytical-systematic process; observation and documentary review were used for the applicability and implications of digital signatures and certificates in the framework of Law 27269, in Peru.

The bibliographic reviews were carried out exhaustively using the inductive process, because they take as a reference the provisions of the Peruvian state with respect to the modernization of the state through the use of electronic tools in Peruvian public management, and reach the conclusions.

Results

Since the enactment of Law No. 27269 "Law on Digital Signatures and Certificates", amended by Law No. 27310, security and control policies have been implemented, which are protected by the Computer Crimes Law.

The State has been implementing policies to make significant progress in the application of digital government, with the Law of Digital Signature and Certificates, which incorporates into the Peruvian legal system legal figures to ensure the safeguarding of information and its transmission by means of electronic elements through the use of cryptographic techniques.

The digital certificate must contain all those data of the holder of the digital signature system, but the essential condition is that there is no doubt about the identity of the holder, being this the reason why the legal requirement is linked to an indubitable identification of the subscriber.

This research shows that with the implementation of Law 27269, significant advances are presented for the processes that require signatures and certificates, it boosts the Peruvian legal system and ensures the protection of information; as well as its transmission by means of electronic elements through the use of cryptographic techniques. Likewise, Arcetales and Gamboa (2019), state in their research that new technologies are relevant for the improvement of public management, ICTs determine a greater public value.

The use of ICTs in government achieves efficiency and effectiveness in programs, improving access and dissemination to the community,

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

businesses and organizations. Also, Fernandez (2001), in his research "La ley de firma digital Argentina", points out that the use of digital signatures is important to make procedures viable and also the application of sanctions that imply its regulation.

Conclusions

With the advancement of technology, there is also an increase in computer crime in Peru and worldwide, which brings with it economic consequences and numerous frauds committed by criminal organizations that are often not reported or whose crimes are committed abroad without often there is a penalty, is intended to give an advance in electronic government, through the implementation of the signature and Digital Certificates, the same that will allow certain procedures to be faster and more efficient.

Since this is a context of information security, it is essential that the certification entity has the appropriate mechanisms and criteria for a correct accreditation of the methodology to verify the subscriber's digital signature. The State must invest in modern technology through the acquisition of software and hardware that allow the implementation of systems with greater security, which will allow the confidence of citizens in the use of digital signatures.

References

Dávila, W. (2020). Computer crimes Peru. Blog Resultado legal [October 12, 2020]. http://resultadolegal.com/%EF%BB%BFdelitos-informaticos-peru/

Duche, A., Gálvez, P. and Marallano, P. (2019). Information and communication technology in the implementation of supply chain management strategies in business: a systematic literature review. Centro Sur social science journal. 4(2). http://www.centrosureditorial.com/index.php/revista/article/view/86/241

Espinoza, J. (2018). Between electronic signature and digital signature: approximations on its regulation in Peru. *Journal of the Institute of Legal Sciences of Puebla.* 12 (41). https://www.revistaius.com/index.php/ius/article/view/315/601

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

Flores, L. (2014). *Derecho Informático*. Grupo Editorial Patria. 1st Ed. https://editorialpatria.com.mx/mobile/pdffiles/9786074380637.pdf

Gamboa, M., Barros, L., & Barros, C. (2019). Childhood Aggressiveness, Learning and Self-Regulation in Primary Students. *Luz. Revista Electrónica Trimestral de La Universidad de Holguín*, *53*(9), 1689-1699. https://luz.uho.edu.cu/index.php/luz/article/view/743/637

Govin, P. (2019). Security trends and vulnerabilities in cloud-based systems for educational processes. *Formación docente -revista iberoamericana de educación.* 2(3). http://www.revista-iberoamericana.org/index.php/es/article/view/25

Olivar, A. (2019) Public policies, differential approach and epistemologies of colonialism: a twist in the vindication of minority groups' rights. *Centro Sur,* 3(1). http://www.centrosureditorial.com/index.php/revista/article/view/23/44.

Ovid, J. (2006). Electronic Contracting. *THĒMIS-Revista De Derecho*. (44), 253-269. http://revistas.pucp.edu.pe/index.php/themis/article/view/10075

Porrúa, M. (2019). The Digital Agenda in Latin America: A progress at different speeds. Inter-American Development Bank. [October 12, 2020]. https://blogs.iadb.org/administracion-publica/es/la-agenda-de-gobierno-digital-en-america-latina/.

Rodas, P. and Loor, E. (2017). Typification training process in the integral organic penal code for cybercrimes. *Formación docente -revista iberoamericana de educación.* 1 (1). 42-79. http://www.revista-iberoamericana.org/index.php/es/article/view/4/pdf

Salvador, I. (2001). The digital signature: a technology for intercommunication in the Society - NETWORK. *Spanish Journal of Science Education.* 24(1). http://redc.revistas.csic.es/index.php/redc/article/view/33

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743

Torres, Á. and Oviedo, B. (2020). Use of information and communication techniques and their impact on access control. *Journal of business and entrepreneurial studies,* 4 (1). http://journalbusinesses.com/index.php/revista/article/view/66/181

Vela, N. (2020). Analysis of document forgery and protection of the legal good in criminal matters. *Journal of business and entrepreneurial studies*. 4(1). http://journalbusinesses.com/index.php/revista/article/view/26/59

Villao, D. (2016) Digital tools in second language learning. Sinergias educativas, vol. 1(2), Grupo Compás, Ecuador. http://www.redalyc.org/articulo.oa?id=573563368006.

Received January 12, 2021 / Approved May, 03 2021 Pages: 122-133
eISSN: 2600-5743