Цифровое право, 2022, №3, С. 8-19 https://doi.org/10.38044/2686-9136-2022-3-3-8-19
Опубликована: Сен. 30, 2022

Cryptography and law: The case of Brazil

Cardoso O.V.
Ph.D. in Law, Judge of Federal Regional Court of the 4th Region, Professor, School of Federal Judges of Rio Grande do Sul

Аннотация

In a digitalised environment under conditions of reduced limits and boundaries between physical and virtual worlds, people's daily activities increasingly migrate to cyberspace. For this reason, legal issues relating to encryption, deciphering and codebreaking become increasingly topical. Due to the increased vulnerability of a wide range of people to exploitation, digitalisation implies an urgent need to develop measures for preserving privacy in digital life. Increasing vulnerabilities experienced in the social environment due to the Internet and network interactions can be attributed to the erasure of boundaries between people, which is facilitated by access to their data. In terms of providing general protection to online users, digital contracts, routine bank transfers and communications serve as an example. Cryptography, which allows the encoding of a message in an unintelligible format for those who do not have the appropriate key, represents one of the safest techniques for securely transmitting information online. In order to examine the relations between law and cryptology, the present work analyses Brazilian legal acts governing cryptography. Here, as well as defining cryptography, the main objective is to determine its main aspects and key features in order to examine the main legal issues and pecularities of legal regulation. It concludes that cryptography, as a mean to protect privacy on the Internet, does not exclude the necessity of law, but, on the contrary, legal regulation is essential to provide legal certainty to the cryptographic techniques.

Ключевые слова: cryptology, information security, digital law, cryptocurrency, digital signature, cryptography

INTRODUCTION

Cryptography is usually associated with methods for hiding and securely transmitting information. However, it can also be used to guarantee the veracity and authenticity of information by preventing its modification (or exposing any alterations). Therefore, the proper and safe application of cryptography depends on its regulation: the law delimits and limits the uses of cryptography, by defining what is — and what is not — lawful. For instance, digital payments in electronic commerce, the general functioning of the financial system (debit and credit cards, financial transactions in ATMs, applications, etc.) and even the sending of messages by e-mail could not be conducted in a reliable and safe way in the absence of regulation by law.

In addition to being a crucial tool in information security, encryption can also be used for purposes such as authenticating a digital signature or determining the validity of a contract.

In this connection, the currently insufficient regulation of cryptography applications causes legal certainty creates a need for legal bases for its standardisation, including in contracts.

The present work analyses conceptual and historical aspects of cryptology, cryptography and cryptanalysis in the Brazilian legal context, evaluating coherence and identifying gaps by examining practical acts and cases (digital signature, privacy protection on the Internet, data protection and cryptocurrencies).

CRYPTOLOGY: CONCEPTUAL ASPECTS

In essence, cryptology is the study of methods for hiding, storing, communicating and revealing information. In etymological terms, the expression has Greek origins (kryptós lógos) and means “hidden word”. The main objective of cryptology is to secure (and potentially ensure the secrecy of) communication between more than one person (i.e., a sender and receiver). While preserving the secrecy of information is relevant to cryptology, it is not inherent to it. Its primary value, therefore, is to use cryptological techniques to ensure the security of information transmitted in messages (Dizon & Upson, 2021).

When used to prevent information from being accessed by an unauthorised person or system, cryptology has three components: confidentiality, integrity and availability (CIA triad).

Cryptology can also be used to ensure:

a) ensuring that the receiver of the message is able to verify the integrity of a message, i.e., if it has modified in any way;

b) authentication of messages, i.e., allowing the receiver to know with certainty who is the sender;

c) non-repudiation, i.e., the sender of the message cannot deny its sending and authorship.

Thus, whether information is confidential or not, including with restricted or limited access or other classification, the need for its storage, transmission or other form of secure use or communication, results in the application of cryptological techniques, both in terms of concealing and providing access to information.

For such purposes, cryptology covers the fundamentals, definitions and techniques of concealing information (by the sender) and its adequate uncovering (by the receiver). While encoding forms one aspect of concealment, the scope of cryptology is not limited to encoding information and/or messages. Broadly speaking, cryptology covers any form of concealment (with or without encoding), the instruments or the logic used for this purpose.

The main species of cryptology are cryptography and cryptanalysis will be analyzed in the following. We will also consider steganography, which is considered as a kind of cryptography.

CRYPTOGRAPHY: CONCEPTUAL ASPECTS

Cryptography comprises a method of encoding a message in an unintelligible format for anyone who does not have the proper key to decrypt it (Paar & Pelzl, 2010; Mollin, 2007). The word has Greek origins (kryptós gráphein) and means “hidden writing”. Therefore, cryptography has been described as “the science of keeping secrets secret” (Delfs & Knebl, 2007). Thus, encryption is used as a cryptographic technique for hiding a message.

Encryption uses codes and ciphers to convert data into a format that is incomprehensible to anyone who does not have a key for decoding it, i.e., converting the encoded data back into its original format. Therefore, the main concepts in cryptography are code and cipher, which refer to different actions[1].

1. Simmons, G. (n.d.) Cryptology. Encyclopedia Britannica. Retrieved January 11, 2022, from https://www.britannica.com/topic/cryptology

A code comprises a rule that replaces part of the information with another object of the same type or another. For example, when encrypting a message, the code can change the order of the letters of the alphabet, or replace letters with numbers or symbols etc.

One of the best-known encryption codes is the Morse code, created in 1835 by Samuel Finley Breese Morse, which replaces alphanumeric characters (letters and numbers) and punctuation marks with graphic signs (dots, dashes, and spaces). Although not recognised as such by its many users, the American Standard Code for Information Interchange (ASCII) is perhaps the most universally used code. This code, which is used on all personal computers and other devices, replaces alphanumeric (letters and numbers) and special characters with seven-bit binary numbers (that is, those formed by the numbers 0 and 1).

A cipher, which comprises a key or algorithm used for the encryption and decryption of a message, has the same purpose of the code, i.e., to replace the information with another object of the same type or another. While a code and a cipher are both used to hide a message by replacing its information with another object, the main difference between a code and a cipher consists in the cipher using a key to achieve this purpose.

A plaintext is the original message prior to any changes. By encrypting a plaintext, a ciphertext is produced. Thus, an encryption algorithm performs the function of converting a plaintext into a ciphertext, while a decryption algorithm converts the ciphertext back into a plaintext.

Thus, the process of transforming a plaintext into ciphertext is called encryption or enciphering, the encrypted message is called a cryptogram, while the reverse process of transforming ciphertext into plaintext is called decryption or deciphering (Mollin, 2007). Therefore, the sender of an encrypted message uses an encryption algorithm, while its receiver uses a decryption algorithm.

Classifications

There are two main approaches for classifying cryptography:

a) based on the technique used to conceal the message;

b) based on the key used to encrypt the information.

The use of encryption methods is mainly based on two techniques:

i. transposition cipher, which reorders the characters of a message according to a predetermined logic. Some examples of transposition ciphers are rail fence techniques, in which the message is written in diagonal lines, and rectangular, when the message is written horizontally in a particular number of columns;

ii. substitution cipher, which changes the characters of a message. An example of a substitution cipher is the Caesar cipher (or exchange cipher), which modifies a letter of the alphabet by substituting it with another located in a certain fixed position.

While in a substitution cipher, the characters maintain their position in the sentence but change their identity (that is, the position and number of characters in each word do not change, but their representation changes), in a transposition cipher the characters change their position in the sentence but maintain their identity (the representation of the character does not change, but its position and amount in each word changes).

The second classification of cryptography divides it into symmetric (private or secret key) and asymmetric (public key) (Paar & Pelzl, 2010):

iii. symmetric cryptography (private or secret key) uses the same key to encrypt and decrypt the message; that is, the encryption and decryption of information occurs inside the message, which must be kept secret by the sender and receiver. This ensures a rapid response to encryption and encryption since the sender and receiver of the message use the same (private) key.

On the other hand, the sending of a private key to the receiver must occur in a secure manner to prevent unauthorised people from accessing it and the decrypted message. Therefore, sharing the private key is difficult to use this type of encryption. The main algorithms used for the private key are the block symmetric key (which divides the message into blocks of equal size in terms of bits) and flow (which affects the message bit by bit);

iv. asymmetric cryptography (public key) uses different keys (one public and one private) to encrypt and decrypt the message. Thus, either data encrypted with a public key can only be decrypted with the corresponding private key, or data encrypted with a private key can only be decrypted with the corresponding public key.

Encryption keys can also be used to ensure the integrity of information by ensuring that information signed by a private key is not modified and can be accessed by a public key. The main examples of this use of cryptography are digital signatures and time stamps.

STEGANOGRAPHY: CONCEPTUAL ASPECTS

Steganography is a technique used to conceal a message in a non-secret object (hidden writing). Despite being a different type, it is usually considered as a form of cryptography, which can be divided

into true secret writing (cryptography in a strict sense) and covert secret writing (steganography) (Mollin, 2007). The word also has Greek origins (steganós gráphein means “covered writing”).

Steganography is especially used to hide text messages in different files (with image, video, audio, text etc.) in order to allow the circulation of confidential content, which can be accessed by anyone who knows how to access the message.

Digital files facilitate the use of steganography due to consisting of ordered sequences of bits (binary digits) stored in a file, as occurs, for example, in image pixels.

While cryptography and steganography are both used to ensure information confidentiality so that information is not accessed by unauthorised persons or systems, they do not ensure its integrity — that is, that the message will reach the receiver without any change in the information.

CRYPTANALYSIS: CONCEPTUAL ASPECTS

The main objective of cryptanalysis, which is also an expression of Greek origin (kryptós analýein means “open word” or “enlightened word”), is to discover or recover information encrypted or concealed despite lacking possession of the key or the form of concealment. Therefore, it is also known as the “art of breaking” cryptographic systems (Paar, 2010)[2].

To achieve its objective, cryptanalysis accomplishes in three stages:

a) identification: checks the existence of a hidden message and which code or system was used for this purpose;

b) cracking: testing of codes or other ways to identify the hidden content of the message;

c) configuration: stage of identifying the hidden content of the message.

LEGAL REGULATION OF CRYPTOGRAPHY IN BRAZIL

The use of cryptology and its distinct types (especially cryptography) depends on its legal regulation (Liguori, 2022)[3]. The

2. Simmons, G. (n.d.) Cryptology. Encyclopedia Britannica. Retrieved January 11, 2022, from https://www.britannica.com/topic/cryptology

3. On the advantages and disadvantages of legal regulation of cryptography, see chapters 5.2.1.1 and 5.2.1.2 of the book.

law itself can be the object of cryptography, in the so-called “cryptographic law” or “smart regulation”, which proposes the use of a self-executable code as a new mean of legal regulation, which replaces a person’s (that is, the legislator’s) ability to predict the future with lines of code protected by cryptography (Deakin & Markou, 2020).

Considering the need for balance and updates in this relationship between law and technology, we proceed to an analysis of the main legal acts in Brazil (Salvador et al., 2019).

DIGITAL SIGNATURE

The first legal Act in Brazil to regulate the application of encryption techniques is the Medida Provisoria (MP) no. 2.200-2/2001 (hereinafter — MP 2.200-2/2001), which established the Brazilian Public Key Infrastructure (ICP-Brasil) consisting of a hierarchical chain of trust validation to digital certificates for digital identification[4]. ICP-Brasil’s main objective is to guarantee the authenticity, integrity and legal validity of electronic documents, support applications and applications enabled with digital certificates — and, consequently, secure electronic transactions (article 1 of the MP 2.200-2/2001)[5]. Thus, Brazil has a public digital certification infrastructure, which is maintained and audited by the National Institute of Information Technology, a federal agency that plays the role of the Root Certification Authority.

Cryptography is also mentioned in article 6 of MP 2.200-2/2001[6]: each digital certificate can be issued by an accredited Certification Authority (CA), with the creation of a pair of cryptographic keys by the holder — that is, a public key and a private key.

A digital certificate, as regulated by MP 2.200-2/2001, uses asymmetric cryptography (or public keys) to ensure the integrity, authentication and non-repudiation of a digital signature. In this way, a person can use a private key to digitally sign a document, which can be accessed by anyone using the public key. With such a digital certificate it is possible to verify who actually digitally signed the document (authentication), preventing changes to it (integrity) and preventing the signer from denying authorship (non-repudiation).

4. Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.
5. Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.
6. Medida Provisoria No. 2.200-2, de 24 de agosto de 2001, Establishes the Brazilian Public Key Infrastructure (ICP-Brazil), Diário Oficial da União [D.O.U.] de 27.8.2001.

This does not necessarily involve the protection of confidentiality, since a digital certificate can be used specifically for the purpose of publicizing the document and its public verification (as occurs, for example, in judicial decisions, in contracts and other acts).

In addition, a digital certificate can be used to verify the integrity and authenticity, or even the content of a digital or scanned document.

For example, sending a letter with receipt of confirmation can only contain the description of the object, but not its integral content (such as an extrajudicial notification). In turn, the digital sending (by email, message application or other way) of a document signed electronically (with cryptography) allows the verification of the content of the document, as well as its sender and overall integrity.

To permit these acts, it is necessary to regulate the legal form of electronically signing a document and the valid ways of sending or verifying that document, which is facilitated in Brazil by MP 2.200-2/2001.

In addition, the Electronic Signatures in Global and National Commerce Act[7], approved in 2000 in the United States, was the first Act in the world that regulate the certification digital and innovated by conferring to the digital signature the same legal validity of a written signature, i.e, one written on a physical substrate such as paper.

PRIVACY PROTECTION ONLINE

Although the Brazilian Internet Act (Act no. 12.965/2014) does not mention cryptography, it supports its use by assuring the rights and guarantees of Internet users, in article 7, I, II and III, including the inviolability of the privacy and the private life, the inviolability and secrecy of communication flow on the Internet (transmitted) and the inviolability and the secrecy of stored private communications (static)[8].

For example, SSL (Secure Sockets Layer) and TLS (Transport Layer Security) digital certificates on websites comprise security protocols that create an encrypted link between the server and the browser. This attests to the authenticity of a page and protects the confidentiality of the transmitted data and information. Although these certificates have long been used, for example, by banks and

7. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. 7001-7031 (2000).

8. Act No. 12.965, de 23 de abril de 2014, Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, Diário Oficial da União [D.O.U.] de 24.4.2014.

digital commerce, their use has been expanded to become a security guarantee for websites through their integration with the protocol for hypertext transfer. Thus, in addition to the standard HTTP (HyperText Transfer Protocol,), the HTTPS (HyperText Transfer Protocol Secure) protocol is integrated with SSL or TLS in order to use encryption in the communication between the user and the application on the Internet.

Article 13, IV, of the Brazilian Internet Act provides for encryption as one of the techniques used to guarantee the inviolability of data on the Internet, in record management solutions for safekeeping, storage and other data processing activities[9].

In another example, the end-to-end encryption is used in message applications, with data encrypted only in the sender's device, or in the receiver's device. This method of encryption excludes the key from the service providers; that is, in order to prevent third parties from accessing data while being transferred from one device to another, it is provided only to the sender and receiver of the message. Therefore, no third party can access the message content (including the application developer him- or herself) because it is unintelligible to anyone who does not have the proper key for decrypting it.

In Brazil, the Supreme Court started to decide the ADPF 403 and the ADI 5527, in which the suspension and blocking of messaging services by court decisions are discussed, considering that messages are protected by encryption and not stored on the servers of the service, but only on users' devices[10].

PROTECTION OF PERSONAL DATA

The Brazilian General Personal Data Protection Act (Act no. 13.709/2018 — LGPD)[11] does not contain any direct reference to encryption (Althabhawi et al, 2022). However, encryption can be applied based on several LGPD rules. Firstly, it is related to the concepts of anonymised data (article 5, III) and anonymisation (article 5, IX). While anonymised data does not contain or does not allow the identification of its subject, anonymisation is an activity of processing personal data in such a

9. Act No. 12.965, de 23 de abril de 2014, Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil, Diário Oficial da União [D.O.U.] de 24.4.2014.

10. S.T.F., Arguição de Descumprimento de Preceito Fundamental No. 403, Relator: Min. Edson Fachin, Ação Direta de Inconstitucionalidade No. 5527, Relator: Min. Rosa Weber.

11. Act No. 13.709, de 14 de agosto de 2018, General Personal Data Protection Act (LGPD), Diário Oficial da União [D.O.U.] de 15.8.2018.

manner that the personal data can no longer be attributed to a specific data subject. Thus, the LGPD does not make any provision for the anonymisation of data, but one of the techniques that can be used to anonymise personal data is encryption.

Data anonymisation is a method for protecting the controller due to removing the influence of LGPD on data processing, which can be carried out through encryption. In this case, the main purpose of encryption is not to provide privacy or greater security to the processing of data, but rather to make the LGPD inapplicable to the agent procesing operations.

In addition, by regulating security measures, practical rules and governance in Chapter VII (articles 46–51), the LGPD determines the use of cryptography as a security measure for protecting personal data from unauthorised access, including accidental or unlawful situations of destruction, loss, alteration, communication or any form of inappropriate or illicit processing (article 46).

Cryptography is also legitimised by article 48, § 3º, of the LGPD, which regulates the communication of security incidents with personal data and stipulates incumbency on the part of the controller to demonstrate the adoption of "(...) appropriate technical measures that make the affected personal data unintelligible, within the scope of and within the technical limits of its services, to third parties not authorised to access them". Thus, even if there has been a security breach or unauthorised access to systems, files and other devices, the impossibility of third parties to access the encrypted data must be taken into account when evaluating the incident (and proving the absence of damage to the personal data subjects).

CRYPTOCURRENCIES

As a medium for conducting business transactions, the main functions of currency are:

a) value measurement: when used to assign a price to an object, such as products and services;

b) means of payment: a standardised form to be used in exchanges;

c) reserve method: use of currency as a reserve by its controller to manage the economy, thus explaining why not all banknotes and coins are in circulation but part of them is kept in reserve.

Currencies are classified in the ISO 4217, an international currency standard, by means of a three-letter capital code[12]. This code is used to standardise the identification of coins, some precious

metals and certain financial units (such as special drawing rights) in international trade (such as bank transfers, the purchase of international plane tickets etc.).

A digital currency (electronic money, electronic currency or electronic cash) is the digital form taken by a particular currency. Therefore, in addition to banknotes and physical coins, a country can also have a virtual format of its currency.

Conversely, a cryptoasset is any cryptography-based asset, which relies on distributed data recording technology; that is, an asset with a digital form and use. It can be classified in terms of:

a) security tokens, which represent, in a digital environment, some physical securities. These are especially common in financial markets where they may be used for raising funds for a company, a new product or project, or to represent shares in an investment fund;

b) utility tokens, which comprise assets for accessing services or the provision of goods, which can be created by an organisation (such as, for example, fan tokens created by sports clubs for their members and fans, or tokens used in electronic games to purchase in-game products). Since these are not securities or financial assets, they can be created freely and do not depend on prior regulation by a Central Bank or a Securities and Exchange Commission;

c) cryptocurrency, which is a cryptoasset that performs the functions of a payment method, especially those of a currency unit, medium of exchange, store of value and unit of account (Uhdre, 2021).

In these cases, tokens perform contract functions, with the main objective of proving custody by whoever has its custody or is designated as their owner or possessor. Security tokens and utility tokens are also digital bearer securities because they represent rights (and their holders) and are considered safe, authentic and reliable due to the use of cryptography.

More specifically, cryptocurrency is a kind of digital currency and cryptoasset, which is not regulated or managed by a country or a Central Bank due to being based on a decentralised system.

While a cryptoasset comprises any encrypted economic asset based on distributed data recording technology, a cryptocurrency is one of its types, consisting of a cryptoasset with the additional function of a payment method. As a kind of cryptoasset,

12. Group Six. (n.d.) Data Standarts. Retrieved July 26, 2022. https://www.six-group.com/en/products-services/financial-information/data-standards.html

cryptocurrency has a digital form and use; that is, it is created, used and circulated exclusively in digital media.

Cryptocurrency is formed by the same suffix “crypto” (originating from the Greek word kryptós) also seen in the expression cryptography (secret writing). Therefore, it represents a “secret currency” or “hidden currency”. However, it is not a currency created to circulate in secret or confidentially. On the contrary, cryptography is used to secure the existence of the currency and its circulation; i.e., to support business conducted with the use of cryptocurrency via the provision of integrity, authentication and non-repudiation. For this purpose, blockchain technology is generally used to provide security for the storage and circulation of cryptocurrencies.

In Brazil, the regulation of cryptocurrencies is still incipient and has no legislative basis, but only infra-legal norms. There is legal basis in Brazil only for the creation of a digital or electronic currency. Act no. 12.865/2013 regulates payment arrangements and payment institutions that are part of the Brazilian Payment System (SPB)[13]. In this context, article 6, III, ‘g’, authorises payment institutions to convert physical money into electronic money (and electronic money into physical money) in order to manage the use of electronic money.

In addition, article 6, VI, of Act no. 12.865/2013 contains a legal definition of electronic money: “resources stored in an electronic device or system that allow the end user to carry out a payment transaction”.

Based on this Act, the Central Bank of Brazil issued the Notice no. 25.306/2014, on February 19, 2014[14], whose main objective was to highlight the risks involved in trading “virtual currencies” or “crypted currencies”.

A new alert on the risks existing in the safekeeping and trading of virtual currencies was issued by the Central Bank of Brazil in Notice no. 31.379/2017[15].

The Brazilian Securities and Exchange Commission (CVM) issued Circular Letter no. 1/2018[16] on the possibility of investing in

13. Act No. 12.865, de 9 de outubro de 2013, Diário Oficial da União [D.O.U.] de 10.10.2013.
14. Notice No. 25.306, de 19 de fevereiro de 2014, Diário Oficial da União [D.O.U.] de 20.02.2014
15. Notice No. 31.379, de 16 de novembro de 2017, Diário Oficial da União [D.O.U.] de 17.11.2017.
16. Circular Letter No. 1/2018/CVM/SIN, de 12 de janeiro de 2018, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html

cryptocurrencies by investment funds regulated by CVM Instruction no. 555/2014 (which regulates the creation and operation of investment funds in Brazil).

Based on the absence of legal regulation in Brazil and the lack of consensus on the possibility and form of standardisation, the CVM concluded that cryptocurrencies are not financial assets (according to the definition of item V of article 2 of the CVM Instruction no. 555/2014)[17]; thus, they cannot be acquired by funds.

However, in the same year, the CVM issued Circular Letter no. 11/2018[18], in which it is explained that CVM Instruction no. 555/2014 does not prevent investment funds in Brazil from investing indirectly in cryptocurrencies, through the acquisition of funds shares, derivatives and other assets abroad that invest in virtual currencies, as long as they are in a country that authorises this type of investment.

In addition, Normative Instruction no. 1.888/2019 of the Federal Revenue Service of Brazil (RFB) imposes the duty to provide information on carrying out operations with cryptoassets (that is, cryptocurrencies and other species)[19]. By regulating the duty to declare cryptoassets on the part of individuals or individuals and legal entities, the RFB indirectly recognises the legality of operations carried out with these assets, based on the constitutional principle of legality provided for in article 5, II, according to which whatever is not expressly prohibited by law is permitted ("no one shall be obliged to do or refrain from doing anything except by virtue of the law").

The article 5, I, of Normative Instruction RFB no. 1.888/2019 defines cryptoassets as "the digital representation of value denominated in its own unit of account, whose price can be expressed in local or foreign sovereign currency, electronically transacted with the use of cryptography and of distributed ledger technologies, which can be used as a form of investment, instrument for the transfer of values or access to services, and which does not constitute legal tender".

Finally, Bill no. 4401/2021, currently pending in the Brazilian National Congress, is aimed at the regulation of virtual assets and the activities of virtual assets service providers; this is in addition to

17. Instruction No. 555/CVM, de 17 de dezembro de 2014, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/instrucoes/inst555.html

18. Circular Letter No. 11/2018/CVM/SIN, de 19 de setembro de 2018, Retrieved January 11, 2022, from https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html

19. Normative Instruction No. 1.888, de 3 de maio de 2019, Diário Oficial da União [D.O.U.] de 07.5.2019.

changing the Crimes Against the National Financial System Act and Money Laundering Act[20].

This Bill, which is expected to be approved in 2022, considers virtual assets as digital representations of value that can be traded or transferred by electronic means and used for making payments or for investment purposes.

CONCLUSIONS

Cryptography is a type of cryptology, which consists of the study of techniques for concealing, storing, transmitting and revealing information. It is used to prevent information from being accessed by people without authorisation, which is associated with information confidentiality. However, cryptography is not limited to confidentiality, but also ensures compliance with the integrity (keeps information unchanged and indicates any changes made), authentication (the receiver knows who the sender is) and non-repudiation (the sender of the message cannot subsequently deny its authorship) of messages.

While cryptography is not yet regulated in Brazilian law, it is envisaged in legislation as one of the possible methods of ensuring information security, good practice and governance (among others), supporting confidentiality, integrity, authenticity and non-repudiation of data, information and related activities.

The security provided by the application of encryption in the protection of data and information, whether stored or transmitted, especially in the digital environment, prevents unwanted incidents and demonstrates compliance with legal norms.

Having various uses, cryptocurrency is a kind of digital currency and cryptoasset, which is not regulated or managed by a country or a Central Bank due to being based on a decentralised system. While the cryptoasset comprises any encrypted economic asset based on distributed data recording technology, cryptocurrency is one of its types, consisting of a cryptoasset with the functionality of a payment method. As a kind of cryptoasset, cryptocurrency has a digital form and use; that is, it is created, used and circulated exclusively in digital media.

The wide use of digital currencies around the world, and their potential for illicit purposes, requires state acts that regulate their use in a safe and lawful manner.

20. Bill No. 4401, de 8 de julho de 2015, Retrieved January 11, 2022, from https://www.camara.leg.br/propostas-legislativas/1555470

For these reasons, although there is no legal basis to authorise business transactions and the practice of other acts with cryptocurrencies in Brazil, these are authorised based on the constitutional principle of legality, according to which what is not expressly prohibited by law is allowed.

This legislative gap is expected to be addressed in Brazil with the approval of Bill No 4401/2021, which regulates virtual assets and the activities of virtual assets services providers[21].

REFERENCES

1. Althabhawi, N. M., Zainol, Z. A., & Bagheri, P. (2022). Society 5.0: A new challenge to legal norms. Sriwijaya Law Review, 6(1), 41-54.

2. Deakin, S., & Markou, C. (2020). From rule of law to legal singularity. In S. Deakin, & C. Markou (Eds.), Is law computable: Critical perspectives on law and artificial intelligence (pp. 1-29). Hart Publishing.

3. Delfs, H., & Knebl, H. (2007). Introduction to cryptography: Principles and applications. (2nd ed.). Springer.

4. Dizon, M. A. C. & Upson, P. J. (2021). Laws of encryption: An emerging legal framework. Computer Law & Security Review, 43, Article 105635. https://doi.org/10.1016/j.clsr.2021.105635

5. Liguori, C. (2022). Direito e criptografia: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia [Law and cryptography: Fundamental rights, information security and the limits of legal regulation in technology]. Saraiva Jur.

6. Mollin, R. A. (2007). An introduction to cryptography. (2nd ed.). Chapman & Hall/CRC.

7. Paar, C., & Pelzl, J. (2010). Understanding cryptography: A textbook for students and practitioners. Springer.

8. Salvador, J. P. F., Liguori, C. A. F., Santos, G. K., & Guimarães, T. B. Criptografia e Direito: Uma perspectiva comparada [Cryptography and law: A comparative perspective]. In D. Doneda, & D. Machado (Eds.), A criptografia no direito brasileiro [Cryptography in Brazilian law] (p. 107-121). Thomson Reuters, Revista dos Tribunals.

9. Uhdre, D.C. (2021). Blockchain, tokens e criptomoedas [Blockchain, tokens and cryptocurrencies]. Almedina.

21. Bill No. 4401, de 8 de julho de 2015, Retrieved January 11, 2022, from https://www.camara.leg.br/propostas-legislativas/1555470