RANSOMWARE: CYBERCRIME AND CYBERSECURITY

Joaquim Ramalho, University Fernando Pessoa, Portugal

ABSTRACT

Cybercrime is increasingly a threat to national and international security. Ransomware, which designates a type of malware that the agent installs on victims' computers without their consent, with the aim of demanding a consequent ransom, so that the data is provided again, is currently one of the forms of cybercrime that has the greatest impact on companies. This article seeks to reflect on the criminal imputation of ransomware crime and the importance of implementing strategic actions to support cybersecurity.

Keywords: Ransomware, Cybercrime, Cybersecurity, Illegal Access, Extortion.

INTRODUCTION

The technological outbreak and large-scale globalization bring enormous benefits, encouraging new forms of contact between people and new relational contexts, through which called cyberspace has been gaining preponderance, which corresponds an existing space in the universe of communication (de Oliveira et al., 2020), through which physical presence is not necessary to establish relational communication, and can function as a space for sharing information and contact people from all over the world.

Reflecting about the dynamic and transnational nature of cyberspace, its criminal framework does not have international uniformity, giving rise to a natural controversy due to the difficulties in effectively regulating the use of new digital technologies and the activities that may occur within them.

Although the creation of the internet was done with the aim of amplifying and promoting dialogue between people, new criminal practices (for example, blackmail, economic advantage or illicit enrichment), have potentially been developed with a focus on cyberspace, the covered in possible anonymity and consequent impunity.

Therefore, there is a pressing need to operationalize protection mechanisms in the face of new criminal practices in cyberspace and the offense against new legal assets, whether through cybersecurity systems or through international legislative diplomas aimed at protecting legal assets that have been being systematically threatened. Consequently, it is essential that the Law, respecting even its actualist principle, is updated according to the evolution of societies, which can occur through the creation of new incriminating types but also with the adaptation of those that are already defined in legal provisions (Simoiu et al., 2019).

CYBERCRIME

New technologies have enormous relevance in the citizens lives. Normally, these are used for the benefit of the users themselves, allowing them to access information from anywhere in the world in a few seconds (Ramalho & Almeida, 2024). However, objectively,

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

new technologies not only bring advantages, but they also constitute a resounding form of proliferation of certain types of crime, particularly computer crime[1].

The applicability of Positive Law to the information society has always raised several problems in terms of territorial competence, lack of legal provision for its technologies, new goods and services that are difficult to fit into existing legal institutes[2]. All these factors increase the effects of information technologies as factors that facilitate the practice of illegal acts.

Cybercrime is increasingly a threat to national and international security, corresponding, nowadays, to one of the main threats to respect for the Human Fundamental Rights, and may even be, for various reasons, a threat to national and international security.

Providing a brief conceptual framework, the EUROPEAN COMMISSION[3] (2007) considers that cybercrime corresponds to criminal acts carried out using or against electronic communication networks and information systems (Candido et al., 2023).

Trying to explain it better, adding that cybercrime ends in the designation given to cybercrimes that involve any type of activity or illicit practice on the network, such as the dissemination of viruses, computer fraud, system intrusions, violation of personal data or access to confidential information.

The cybercrime systematization can be understood from two different perspectives: (a) *stricto sensu* - in which the computer element is framed as an integral element of the legal type or as a legal asset to be protected; (b) *lato sensu* - that in which not only those whose legal interest is protected is the access or functionality of the information society, but also all those in whom information technology is a necessary part of their typical elements, that is, in which the IT element is just a means that facilitates the commission of a certain crime.

The prevalence of cybercrime, in its different facets (Prosecutor General of the Portuguese Republic, 2023), has increased significantly in a recent year[4], noting that reports of cybercrime have been increasing consistently since 2016. However, after 2020, reports almost doubled, certainly not unrelated to the confinement of people because of the situation experienced pandemic (Dias, 2022).

Considering the nature and configuration of the crime, it must be admitted that the criminal prevalence of the events that occurred may still be much higher than the number of complaints. It is therefore urgent to create effective legal institutes that fit into existing ones, since the applicability of positive law to new technologies has always raised several problems of territorial competence and the lack of legal provision for the protection of new legal assets.

Portugal, in 2009, transposed into domestic law a Framework Decision of the Council of Europe, relating to attacks against information systems, known as *Cybercrime Law*[5]. Its fundamental objective is to create mechanisms designed to protect society against cybercrime, namely through the adoption of appropriate legislation that encourages international cooperation.

The Cybercrime Law sought, with the provision of substantive and adjective criminal norms, to harmonize the various legislations of the signatory countries, thus promoting a more effective fight against cybercrime, by covering a set of computer-legal concepts, criminal offenses, procedural measures aimed at regulating the way in which evidence is obtained in a digital environment and international cooperation mechanisms.

RANSOMWARE

One of the main forms of cybercrime is a malware that commonly encrypts all files and requests for a payment in bitcoin to give the victim the decryption key, known worldwide

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

as ransomware, which has relevant implications regarding the protection of individuals and security of legal persons.

Ransomware is currently seen as one of the worst attacks that can be carried out on a company, whatever the size of that company, shaking the entire business structure, both financial and social (Wendt, 2021), denigrating and disqualifying the seriousness and commitment of the company with exposed customer data[6].

The term ransomware has a generic characterization to designate a type of malware that the criminal agent installs on the victims' computer without their consent, with the aim of demanding a consequent ransom (European Commission, 2007), so that the data is provided again. Better explained, with increasingly advanced technology, ransomware gives criminals the possibility of blocking access to a computer and then the agent seeks to extort the victim, demanding a large amount of money, normally using the virtual currency Bitcoin, to make identification of the agent difficult.

Ransomware agents have companies as a major target, creating mechanisms with the aim of stealing data and, consequently, using extortion and threats against those who refuse to pay the ransom, which may correspond to financially exorbitant amounts.

Since, in general, companies have confidential data, this framework ends up increasing their silence in the face of extortion, not presenting any type of complaint or seeking help from the competent authorities, ending up becoming hostages of these criminal agents.

According to COHEN[7], the first occurrence of ransomware was verified in 1986, being called *Brain*, using a floppy disk, which corresponded to an external device used at the time to identify possible inappropriate medical software for measuring heartbeats, however, explorers at the time, they quickly acquired devices that allowed them to repel malware and transfigure the encryption of damaged files.

In 2007, an unprecedented ransomware was created, which instead of encrypting files, obstructed users' entry and prevented them from accessing their computers. Furthermore, this ransomware contracted the computer's screen and demanded a sum of money for the screen to become operational.

Ransomware attacks have evolved in sophistication and complexity, but also in prevalence, especially in the last 10 years (Simoiu et al., 2019). Currently, it is estimated that around 3% of the world's population suffers attacks of this type[8].

However, analyzing the prevalence indicators, it is important, from now on, to take into account that those reported are, without a doubt, scarce when compared to the real indicators, since the cases that they experience and report them to the competent authorities are not large, for fear of retaliation.

In some countries, ransomware attacks are markedly random, where the targets of these attacks can be both citizens and companies, which indicates that they are somewhat disorganized. However, in other countries, ransomware attacks are absolutely directed at citizens and companies, with these targets being specific and duly identified, which indicates the practice of organized crime[9].

The increase in the prevalence of cases and the most recent research have contributed to an improvement in the situation through standardized methods of assessing and managing ransomware risks, seeking to protect absolute legal assets such as, among others, individual rights and the privacy and privacy of private life (Rodrigues, 2020).

Ransomware highlighted nomenclature that, until its appearance, did not have much expression, such as data kidnapping, which corresponds to the act of blocking, disabling or

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

making access to data unfeasible, and digital extortion, which concerns the act of requesting an illicit financial advantage.

CRIMINAL IMPUTATION OF RAMSOMWARE

Normally, the tipical action qualification of ransomware has 3 stages: (1) illegitimate access to all or part of a computer system, by obtaining access to the system, which occurs through the owner's deception, but we will start with cases without induction into error, that is, through exclusively technical means (articles 1 and 2 of the Cybercrime Law); (2) subsequently, interference with computer systems by blocking computer data through encryption (Alshaikh et al., 2020), making the same data inaccessible to the user. (article 5 of the Cybercrime Law), by inserting code into the system, which encrypts data, based on an asymmetric key mechanism, and generates a personalized identification of that system; (3) finally, the ransom request stage, for extortion, demanding the payment of an amount in cryptocurrencies so that the data becomes accessible to its owner again (Ramalho, 2022). Once payment is made, the victim receives a personalized key that allows them to recover the data.

The illegal access corresponds to a crime of danger and has two objective elements of the legal type[10]: a) the agent acts without being legitimated to do so; (b) perform an act of accessing a computer system or part of it.

This crime is typified in article 6 of the Cybercrime Law, under which anyone who, without legal permission or without being authorized to do so by the owner, by another holder of the right to the system or part of it, in any way accesses a computer system, is punished with a prison sentence of up to 1 year or with fine penalty of up to 120 days (Dias, 2023). The norm provides that the penalty is imprisonment of up to 2 years or a fine of up to 240 days if the actions described in the previous number are intended to access to obtain data registered, incorporated or relating to a payment card or any other device, corporeal or intangible, that allows access to a payment system or means.

The penalization is imprisonment of up to 3 years or a fine if access is achieved through violation of security rules or through access, the agent obtains data recorded, incorporated into or relating to a payment card or any other device, corporeal or intangible, that allows access to a payment system or means. This imprisonment from 1 to 5 years when, through access, the agent has become aware of commercial or industrial secrets or confidential data, protected by law or the benefit or financial advantage obtained is of considerably high value (Gouveia, 2021). In general, the attempt is punishable, except in the cases provided.

Anyone who illegitimately produces, sells, distributes or otherwise disseminates or introduces into one or more computer systems devices, programs, an executable set of instructions, code or other computer data intended to produce the unauthorized actions described in number previous.

The illegal access, to all or to a part of a computer system, arises through obtaining access to the system, it all starts with the agent sending the victim an email with the aim of obtaining access credentials to the system. The email may consist of downloading a file, requesting to open a certain file or clicking or opening a link, which will allow the installation of a malicious program which will give access to the system.

This email, simulating the legitimization of the sending entity, seeks to promote the installation of malware, so that it can access the intended data. The request to install the

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

program constitutes the commission of the crime of computer forgery (article 3 of the Cybercrime Law).

The core of the crime of illegitimate access is since the perpetrator – a person endowed with the necessary technical knowledge to do so – penetrates a specific third-party computer system, without legal authorization or that of the respective owner or, if such authorization exists, violating the limits of the same (Ramalho, 2024). It is a conduct that is also characterized by facilitating or being able to facilitate the commission of other crimes, such as, for example, crimes involving damage to programs or other computer data, computer sabotage, illegitimate interception or computer and communications fraud.

The criminalization of the conduct described by the legislator was carried out with the aim of protecting the integrity of the injured computer system (Cohen, 1987), substantiated by the lack of authorization to access a computer system or network or intercept communications taking place on a network or computer system.

Regarding the protected legal asset, essentially, the aim is to protect, first and foremost, the security of computer systems (Liska et al., 2017), but also the need to manage, operate and control computer systems in a free and peaceful manner. This incrimination protects the security of computer systems, without prejudice to also protecting other legal assets such as privacy, property, competition and freedom of trade.

This crime has two objective elements of the legal type, the agent acting without being legitimated to do so and carrying out an act of accessing a computer system or part of it.

Regarding the protected legal asset, essentially, the aim is to protect, first and foremost, the security of computer systems, but also the need to manage, operate and control computer systems in a free and peaceful manner. This incrimination protects the security of computer systems, without prejudice to also protecting other legal assets such as privacy, property, competition and freedom of trade[11].

The interference in computer systems through blocking computer data by encryption (Rodrigues, 2018), which can be classified as the crime of computer forgery, which appears as a type of preparatory act for the commission of the crime of illegitimate access[12].

This type of crime involves the manipulation of data entered a computer system or its processing, which will result in the creation of false documents or data, damaging the security and reliability of documents in legal trafficking of an evidentiary nature.

The crime of computer forgery has the following objective legal elements: (a) the agent carries out the action of introducing, modifying, erasing or suppressing data or computer programs or, (Kiru et al., 2019) in any other way, interfering in the computer processing of data; (b) the effect of producing non-genuine data or documents, which is consummated with the production of an electronic data or document capable of having probative value[17]. Is a crime of danger and not a crime of damage, as it is not required that the damage or false document be used. Therefore, it does not require that the damage be effective resulting from the probative value of the falsehood.

Its subjective elements of the legal type are two forms of specific intent: (a) the intention to cause deception in legal relationships; (b) the intention that non-genuine data or documents be considered or used for legally relevant purposes as if they were. Regarding the protected legal interest (Santos & Ramalho, 2023), there are two currents with different normative interpretations[18]: for part of the doctrine and jurisprudence, it is considered that the protected legal interest is security in banking transactions; another party considers that the protected legal interest concerns the integrity of computer systems, with the legislator

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

intending to prevent the practice of acts that undermine the confidentiality, integrity and availability of computer systems, as well as the fraudulent use of them.

Ransomware has been described as the new form of extortion. In extortion, the protected legal interest is the freedom to dispose of their assets by the victim, forced to act to avoid a greater harm, to themselves or to third parties. The action corresponding to ransomware attacks would give rise to an ideal set of crimes, if it began with illegitimate access, or an error induced by computer fraud, as assets are always at stake, including exclusive control of computer systems. However, we will have a real competition if a false document has been produced (computer forgery), with business confidence being the protected legal asset (Hansen, 2020), as well as when encryption causes prolonged unavailability of the computer system resulting in damage that exceeds what is necessary for completion. extortion or affect life in society (interference in systems, especially in qualified form).

The article 223 of Portuguese Criminal Law, referring to the crime of extortion, classifies as a crime anyone who, with the intention of obtaining illegitimate enrichment for themselves or for a third party, constrains another person, through violence or threat of serious harm, into a patrimonial disposition that entails, for herself or for others, harm.

It is characterized as a hybrid crime with a multi-offensive meaning, as it simultaneously protects distinct legal assets, namely property and freedom. The typical action corresponds to conduct that embarrasses another person, through the threat of an important harm, which has as its object an act of asset disposal.

Due to the ease and enormous scope and speed of disseminating content, computer fraud and extortion become a conventional method used by offenders, in general, who act in the context of cybercrime (Rodrigues, 2019).

The crime of extortion falls into the category of crimes against property in general, being a multi-offensive crime, since it protects various legal assets, such as heritage and freedom. Directly aimed at protecting freedom of asset disposition, freedom of decision and action, the damage to which is connatural to extortion, in this sense, as a form of protection of freedom of personal decision.

The objective and subjective elements of the crime of extortion include the intention to achieve illegitimate enrichment, through violence or the threat of significant harm, forcing the owners to dispose of assets that resulted in the identified losses.

The crime of extortion is close to a variety of crimes, however the closest proximity is to the crime of coercion, given that all the elements that make up the typical factual nature of this crime are also part of the crime of extortion, with the latter specializing in relation to the former. Simply due to the requirement that the coerced conduct results in unfair harm to the taxpayer and illegitimate enrichment for the agent or third party. Therefore, the crime of extortion constitutes a *lex specialis* compared to the crime of coercion.

The crime of extortion is distinguished from the crime of fraud, that is, in extortion, there is violence or a threat of serious harm, or blackmail, with the immediate objective of obtaining a financial advantage at the expense of a loss to the extorted party. On the other hand, in the crime of fraud, an error or mistake occurs.

CONCLUSION

As a final reflection, as highlighted previously, ransomware has specific characteristics that make its attribution difficult, namely its cross-border nature and its

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

apparent anonymity, which create difficulties in identifying the perpetrator of the crime and the consequent criminal attribution.

Furthermore, the lack of a certain international legislative uniformity also does not allow for the establishment of coherent sanctioning measures that allow for an effective fight against this type of crimes.

Associated with this fact, there are still problems in crime prevalence data, as there is strong evidence that many more cases are not reported to criminal police bodies. This aspect can become an indicator of widespread impunity, as it appears that justice is not effective.

The awareness of society and governments so that there is an effective mobilization in the fight and control of ransomware is imperative, in addition to the need to implement greater social participation in security and cybersecurity activities, which makes it essential to increase in investing in data security, so that, at least, constant invasion methods can be mitigated.

END NOTES

[1]For example, the universal use of electronic mail or social networks, constitutes a form of access to the practice of traditional crimes, using technologies,
[2]Citation Information: Dias VENÂNCIO. (2022). *Lições de Direito do Cibercrime. E da tutela penal dos pessoais.*
[3]Citation Information: EUROPEAN COMISSION. (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy to combat cybercrime.
[4]Citation Information: Prosecutor General of the Portuguese Republic. (2023). In https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_2023_primeiro_semestre.pdf.
[5]Law number 109/2009 of September 15.
[6]Citation Information: WENDT; JORGE. (2021). Crimes cibernéticos: Ameaças e procedimentos de investigação.
[7]Citation Information: COHEN. (1987). Computer viroses: Theory and experiments. Computers & Security.
[8]Citation Information: SIMOIU et al. (2019). I was told to buy a software or lose my computer. I ignored it. A study of ransomware.
[9]These are two great examples of the reality that countries are currently experiencing, and which constitute a real threat to fundamental rights.
[10]Citation Information: DIAS VENÂNCIO. (2023). Lei do Cibercrime: anotada e comentada.
[11]Citation Information: RODRIGUES NUNES. (2020). Os crimes previstos na lei do cibercrime.
[12]Citation Information: RODRIGUES NUNES. (2019). O fenómeno do ransomware e o seu enquadramento jurídico-penal.

REFERENCES

Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware prevention and mitigation techniques. *Int J Comput Appl*, 177(40), 31-39.

Candido, J. W., Florian, F., & Borges, J. H. G. (2023). Segurança da informação com foco na propagação iminente de ransomware nas corporações. *REVISTA FOCO*, 16(5), e1766-e1766.

Cohen, F. (1987). Computer viruses: theory and experiments. *Computers & security*, 6(1), 22-35.

de Oliveira Fornasier, M., Spinato, T. P., & Ribeiro, F. L. (2020). Ransomware e cibersegurança: a informação ameaçada por ataques a dados. *Revista Thesis Juris*, 9(1), 208-236.

Dias Venâncio, P. (2022). *Lições de Direito do Cibercrime, E da tutela penal dos dados pessoais*, Coimbra, Editora D´Ideias.

DIAS VENÂNCIO, P. (2023). *Lei do Cibercrime: anotada e comentada*. Coimbra: Editora D´Ideias.

European Comission. (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy to combat cybercrime.

Citation Information: Ramalho J., (2024). Ransomware: cybercrime and cybersecurity. *Journal of Legal, Ethical and Regulatory Issues*, 27(5), 1-8.

Gouveia, J. B. (2021). Direito do ciberespaço e segurança cibernética. *Revista Jurídica Portucalense*, 59-77.

Hansen, L. P. (2020). The spy who never has to go out into the cold: Cyber espionage. *In Encyclopedia of Criminal Activities and the Deep Web* (pp. 258-270). IGI Global.

Kiru, M. U., & Jantan, A. B. (2019). The age of ransomware: Understanding ransomware and its countermeasures. *In Artificial Intelligence and Security Challenges in Emerging Networks* (pp. 1-37). IGI Global.

Liska, A.; GALLO, T. (2017). *Ransomware.* Sebastopol: O'Reilly Media

Prosecutor General of the Portuguese Republic. (2023). *Cibercrime: denúncias recebidas*. Lisboa, Public Ministry of Portugal.

Ramalho, J. (2022). Prova Digital: Articulação entre o Código de Processo Penal Português e a Lei do Cibercrime. *Revista Eletrônica de Direito Penal e Política Criminal*, 10(2), 7-18.

Ramalho, J. (2024). Recolha de prova em suporte eletrónico: os regimes do Código de Processo Penal e da Lei do Cibercrime. *J2 Jornal Jurídico, 7(1),* pp. 1-9.

Ramalho, J., & ALMEIDA, F. (2024). Apreensão de Correio Eletrónico: Os Regimes do Código de Processo Penal e da Lei do Cibercrime. *Revista Jurídica Portucalense,* 261-276.

Rodrigues Nunes, D. (2018). *Os meios de obtenção de prova previstos na lei do cibercrime*. Lisboa: Editora Gestlegal.

Rodrigues Nunes, D. (2019). O fenómeno do ransomware e o seu enquadramento jurídico-penl. *Revista Cyberlaw*, *8*, pp. 1-42.

Rodrigues Nunes, D. (2020). Os crimes previstos na lei do cibercrime. *Lisboa: Editora Gestlegal*.

Santos, C. F.; Ramalho, J. (2023). Ransomware Empresarial: cibercrime e omissão de relato às autoridades. *Emergência(s) na pesquisa sobre a violência e o crime*. pp. 161-172. Belo Horizonte: Conhecimento Editora.

Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). " I was told to buy a software or lose my computer. I ignored it": A study of ransomware. *In Fifteenth symposium on usable privacy and security (SOUPS 2019)* (pp. 155-174).

Wendt, E.; Jorge, H. N. (2021). *Crimes cibernéticos: Ameaças e procedimentos de investigação*. 2ª edição. Rio de Janeiro: Editora Brasport.

Received: 25-Jun-2024 Manuscript No. JLERI-24-14962; **Editor assigned:** 26-Jum-2024 Pre QC No. JLERI-24-14962(PQ); **Reviewed:** 10-Jul-2024 QC No. JLERI-24-14962; **Revised:** 15-Jul-2024 Manuscript No. JLERI-24-14962(R); **Published:** 22-Jul-2024