ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 7 N. 3 (2018), 5-14
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ201873514

Ransomware - Kidnapping personal data for ransom and the information as hostage

Márcio Ferreira[a] and Cynthia Kawakami[b]

[a]PhD Candidate in Criminal Law from University of Salamanca (Spain). Master's Degree in Criminal Law from University of Coimbra - Faculty of Law (Portugal); Post-Graduation in Criminal Law and Criminology from University of Buenos Aires (Argentina) E-mail: f.marcior@usal.es
[b]Master's Degree in Criminal Law from University of Coimbra - Faculty of Law (Portugal); Post-Graduation from University of Coimbra - Criminal Economic Law Institute - IDPEE (Portugal); Post-Graduation in Risk of Fraud Management and Corporate Compliance from FIA Business School (Brazil); Lawyer at Houthoff (Netherlands) E-mail: cynthia_kawakami@hotmail.com

KEYWORD

Privacy; Personal Data Protection; Kidnapping For Ransom; Kidnapping; Cyberspace

ABSTRACT

The mankind faces a new overview to legally handle with the hyper-connected society, in which personal data and privacy are closely related. This globalization affected directly the criminality, both in its extension and in its structure and occurrence, entailing the occurrence of new criminal conduct, such as the ransomware. The problem is that, the few existent legislations do not successfully encompass the kidnap of personal data for ransom. In this regard, this paper proposes an analysis on the vulnerability of personal data in the New Information Technologies and the Communication, the scope is to analyze the conduct and propose new solutions, aiming to bring more legal certainty to this issue. This new criminological reality deserves reflection, therefore, the present paper will adopt the comparative-deductive method to examine what the existent doctrine and jurisprudence state, in order to assess the necessity (or not) of the creation of a specific criminal legislation for privacy and personal data security of the Internet's user. The main result found is the necessity of the creation of an autonomous field of Criminal Cyber Law to handle with the offensive conducts against information and the legislative evolution demanded to offer specific solutions to RANSOMWARE, which is a new conduct, extremely different from the extortion and kidnapping that society is used to, typical in this new reality where the Information Society *lives.*

1. Introduction

The current society is deeply restructured with the advent of new information technologies and the communication, and with that, the criminality, which suffered highly complex alterations. That was how the delinquency of twenty-first century went through exorbitant variations, since the harmful potentiality and the social disapproval of determined conducts on internet, for instance, turned up slightly burdensome, and can reach an undetermined generality of people. In this context, specific problems about this new branch of the criminal-juridical emerges,

with new conducts, different from the traditionals, that, gradually, create conflicts with significant complexity to the agencies of control and the Criminal Policy.

For this reason, the ultimate recognition of Cyber Criminal Law is searched here, giving more efficient and adequate responses for this new concern generated by the modernization process, with the scope to bring the legal certainty necessary for new offenses with complementary guarantees for the ones already constitutionally defined. Therefore, it is analyzed here the criminal protection of information and the pure cyber offenses, not the traditional crimes using as a "mean" of new information technologies and the communication, but the ones with specific characteristics, that can only be executed through the trinomial ***new technologies – internet – system and computer data***. In this scenario, it is found the innovating conduct to kidnap data and computer systems through hinder and extortion. Thus, at a first sight, the paper aims to analyze in an accurate fashion the RANSOMWARE, or, the kidnapping of personal data for ransom. It will give in detail the execution manner and the peril that this cyber conduct represents to the digital economy, for the State and the society as a whole. From there, it starts the evaluation of the *iter criminis* related to the data kidnapping, based on the Budapest Convention and the other signatories countries in parallel.

Lastly, the paper analyzes the problem caused by the RANSOMWARE to the global digital economy, that, as it can be found here, already coasted billions of dollars in damages to industries in which invested a lot in the modernization process, the so-called *Internet of Things*. In a way that, there are not few inquiries that permeate the technological universe of data treatment. But given this new social demand, there are some preponderant issues to be discussed.

1. RANSOMWARE – *Kidnapping personal data for ransom*

"Each individual have in its nature something that, if it comes out in public, it would arouse disapproval."
GOETHE

The constant and the vertiginous technological evolution are conducting the humanity towards a new world, different and much more complex than expected. These transformations are results of the technical-scientific knowledge experienced after the Cold War, summarized on Technological Revolution. In this aspect, the author supplements: "*Virus*, *spyware, worms, hackers, mailbombing, spam…,* new revealing expressions not only as a way of culture and to see the world, especially, new types of offenses to traditional legal interests, and perhaps even new legal interests that emerge from this new informatic world"[1]. In the same perspective (SAIN, 2012, p. 7): "With the global network expansion in a new millennium, types of traditional crimes adopted new modalities through the usage of emerging technologies".

We are now living in a time of change, times in which old realities are even more questioned by technical phenomenon. Several traditional crimes are suffering profound mutations when they appear with a new vision based on the use of new technologies. "The globalization affected the criminality, both as in its extension as well as in its structure and the form of apparition" (BORJA GIMÉNEZ, 2009, p. 141). It is a new threat that united in a combined manner, the global and the local, where it arises the crimes of high technology. "The TIC's[2], together with internet, maximized the effects of traditional delinquency[3]". The combination of these factors made the potentiality of certain virtual conducts become slightly serious in cyberspace, defined as a new space for criminal opportunities.

At this point, specific problems of this new area of legal knowledge rise, which gradually brought conflicts derived by the relation law/computer with significant complexity. The inquiry is totally justifiable, because the new criminal action in cyberspace has a sophisticated *modus operandi* and with high difficulties for the

1 Macedo, ***algumas considerações acerca dos crimes informáticos em Portugal*** *in.* Costa Andrade & Castanheira Neves**,** 2009, p. 221.

2 *New Technologies Communication and the Information.*

3 Barranco, 2016, p. 679.

ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 7 N. 3 (2018), 5-14
eISSN: 2255-2863 - http://adcaij.usal.es
Ediciones Universidad de Salamanca - CC BY NC DC

Criminal Law and for the control agencies throughout the world. On the sidelines of these radical changes in criminality, that is the moment when it emerges one of the most creative action and threatening of the virtual space, named as ***RANSOMWARE***, or, ***virtual kidnapping of personal data for ransom***[4]. It is a new way of kidnapping, very different from the one already created, but this time, what it is kept in captivity is not a person, but the personal data. The performance of these offenders is creative and diverse, they invade the privacy of victims blocking completely their devices (computer, smartphones, tablets and etc.), obstructing, then, the access of personal information, such as: images, important contacts, private conversations, personal archives and etc. One of the top leaders of global campaigns of *ACRONIS*, consider the RANSOMWARE the most daunting threat security of IT in the entire the history[5].

It consists basically in a virus, which in general conceals in other desirable file in the view of the most vulnerable and curious users. They are files attached in emails, videos from untrustworthy sites, including systems and programs updates that in principle are realible, as Windows and Adobe Flash. "Nowadays it does not occur only the destruction of information, but also the halt of its dissemination, which obviously suppose the functional neutralization of related services" (LLINARES, 2012, p.58).

Once the invasion of the victim's computer is done, a malware activates and block all the operative system, releasing a caveat with an emotion threat/blackmail and the amount to be paid for the ransom. According to the felon's instruction, the victim will make the payment of ransom in order to recover its information within the first three days, otherwise, the amount to be paid will increase. It is important to mention that in some occasions the cyber criminals invade the webcam of the victim to record embarrassing scenes.

Basically, the kidnappers block the victims' computer and ask for money – or Bitcoin[6] – in exchange of a key that promise to unblock the devices. According to specialists, the spread of RANSOMWARE[7] is due to the simplification of monetization and impunity. According to a Portuguese website - In this criminal ecosystem, it is reckoned that the hacker will fulfill the agreement and will give back the files as soon as the payment is done. Huge mistake![8] In the same view, Zampolyansky, chief of SBM Marketing at Kaspersky Lab states that when you are dealing with Ransomware, paying the ransom is not a guarantee that the data will be restored without problems[9]. Even if in some remote cases the virtual criminals give back the bloked files, they keep a virus installed in the victims' server, in order to facilitate future invations.

There is also the police *RANSOMWARE*, in which, after blocking the victims' computer, it simulates a message on the computer's screen of the user, allegedly sent by authorities of public security. In this case, it pops up the caveat that, from that computer, an illegal activity related to child pornography was executed. According to the message, in order to get back the normal access of the device, the alleged "felon", in this case victim, must pay a fine imposed by police authority.

The consequences would be considerable and could be more significant when occurred with companies[10]. The internet kidnappers aim to focus their actions on companies and institutions, that, in general, do not have

4 Specialists point out that Ransomware as the biggest threat of the year in terms of security. The 2016 was the year of online kidnap for ransom. Armed with Ransomware, the cyber felons are able to threaten a normal user who calmly uses the internet at home, as well as self-employed or companies f all sizes. Small, medium or big, publics or privates, all organizations meet together at the target's position of a malware type, which is capable to invade computer equipment, code sensitive information, block the system and request payments in exchange of the re-establishment, frequently giving no time to the victims to act. Available in*:* http://www.silicon.es/a-fondo-como-ataca-ransomware-como-frenarlo-2321602#jJYGyeeXwfcwug2R.99 - *Access in: 01-03-2017*.

5 *Available in:* http://www.silicon.es/a-fondo-como-ataca-ransomware-como-frenarlo-2321602#jJYGyeeXwfcwug2R.99 - *Access in: 01-03-2017*.

6 O *Bitcoin* is a virtual money or a descentralized eletronic money created in 2009, and, in contrary of the majority of coins, it is not supported by any government, nor depends on the reliance of any central issuer.

7 Check the statistics through the map ***RANSOMWARE WAR*** in: https://www.google.com/maps/d/u/0/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=39.65096271537315%2C-94.99983505&z=4

8 Read more in the portuguese site "Dinheiro Vivo": https://www.dinheirovivo.pt/opiniao/ransomware-o-rei-do-ciber-crime/#sthash.tuhGwKCz.dpuf - *Access in: 01-03-2017.*

9 *Available in:* http://www.silicon.es/ransomware-pymes-2322591#Wdt573ov08W1sgXx.99 - Access in: 01-03-2017.

10 In recent years, the use of Smartphones and tablets exponentially increased, for this reason, the offenses against portable deviced with malware will continue. According to the company Check Point, 20& of the employees of companies will be responsible for any gap of security, putting at risk the corporate data. This will be done with awareness, since everything will be

other way to solve the problem, but paying the ransom to recover their information. "The final damage caused by an encrypted malware infection is resulted by the combination of many factors. The partial or total suspension of corporate operations (internal business proceedings, financial transactions, etc.), the loss of valuable data (financial documents and projects, client or standard data base) and the reputational risk."[11] It calculates that the infections through *RANSOMWARE* against companies doubled, with more than 50.000 infected computers[12]. In accordance with the *Europa Press* de Madrid website: *The companies pay an average of 500 euros to try to recover their data after a Ransomware attack*[13]. The FBI foresees that the Ransomware criminals accumulated approximately USD 100 millions of dollars in kidnapping for ransom in 2016, before the USD 30 millions acumulated in 2015[14]. In California, for example, a transportation company become again a victim of cyber criminals, passengers could travel for free after an attack of Ransomware, that kidnapped the computers of *San Francisco Municipal Transportation Agency* – SFMTA – which received in dawn the message "**You Hacked**", with a request of USD 70.000. The action of invasors obstructed the system performance of purchasing and selling tickets, causing an incalculable disorder for the company[15]. In line with the technical director of *Check Point* Eusebio Nieva - The ransomware is without a shadow of doubt one of the most important threatens against security that the companies are currently facing[16].

The *RANSOMWARE* was considered the most profitable virus of history[17]. In fact, it would not be excessive to affirm that new types of *RANSOMWARE,* in a near future, will have the capability to change even faster, in order to maximize its efficiency.

2. The *Iter Criminis* and the Comparative Law

RANSOMWARE is treated as a multi offensive conduct, because it threatens many legal interests (data and computer systems[18]) with varied conducts. In a way that, the ***iter criminis*** present in *RANSOMWARE*, start with a ***submission of a malicious software***[19]***,*** which consists of the creation and distribution of computer programs

done through malwares of their own portable devices connected to a Rogue AP and to one cyber criminal who will have access to the credentials through MITM attacks. *Available in:* http://www.redeszone.net/2016/11/01/los-dispositivos-moviles-iot-cloud-seran-los-principales-objetivos-los-cibercriminales-2017/. *Access in: 11-28-2016.*

11 Read more about this subject in the Portuguese website: https://www.dinheirovivo.pt/opiniao/ransomware-o-rei-do-cibercrime/#sthash.tuhGwKCz.dpuf - *Access in: 01-03-2017.*

12 Law in Network – *Available in:* https://derechodelared.com/2015/12/17/historia-del-ransomware-infografia/comment-page-1/ *Access in: 11-28-2016* .

13 The Ransom ware is not a trivial threaten: its increasing number confirmed its success between the felons, that found in it a source of easy and constant entry. Half of the companies (52%) pay for the ransom of data. The average cost of ransom was 495 euros, still 15% of companies pay more than 1000 euros. *Available in:* http://www.europapress.es/portaltic/sector/noticia-empresas-pagan-media-500-euros-recuperar-datos-ataque-ransomware-20161202143624.html. *Access in: 12-16-2016.*

14 *Available in:* http://www.silicon.es/a-fondo-como-ataca-ransomware-como-frenarlo-2321602#jJYGyeeXwfcwug2R.99 - *Access in: 01-03-2017*.

15 *Available in:* http://www.channelbiz.es/2016/11/29/un-ransomware-ataca-la-ciudad-de-san-francisco/ - *Access in: 12-16-2016.*

16 *Available in:* http://www.silicon.es/a-fondo-como-ataca-ransomware-como-frenarlo-2321602#jJYGyeeXwfcwug2R.99 - *Access in: 01-03-2017*.

17 **RANSOMWARE THE KING OF CYBERCRIME.** The evolution of cybercrime is constant and the threatens we already know mixes with new ones, which emerges to surprise the victims and find their weakness. See more in: https://www.dinheirovivo.pt/opiniao/ransomware-o-rei-do-cibercrime/#sthash.tuhGwKCz.dpuf.

18 According to the Budapest Convention of September 23, 201, about Cyber delinquency in it Chapter I (definitions), article 1-b: for "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*; I*n accordance with the article 1-a, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

19 Pursuant to the **Colombian legislation**, in its article 269E – Chapter One – Assaults against data and computer systems confidentiality, integrity and availability– MALICIOUS SOFTWARE USE. Anyone who, without being authorized to do so, produces, traffics, acquires, distributes, sells, sends, enters to or extracts from the country or malicious software or other computer

with harmful effects. In the criminal order, ***the abusive access to the computer system*** comes[20], because the one, in which, with no authorization, enters in a protected informatic system or stays inside it against the will of the person that has this right, commits cybercrime already defined as crime in a diverse legislation throughout the world. In continuation, the act of **ilegally hindering a system or telecommunications network with no authorization to execute it**[21], or still**,** whoever obstructs the perfomance or normal access or a computer system and the personal data contained in it.

The convention of cyber delinquency elaborated by the Council of Europe in September 23, 2011, in Strasbourg, had the participation of many countries, such as Chine, Canada and Japan. The Budapest Convention, as it was known, was the first international treaty with the scope to fight against cyber delinquency, upon the global harmonizing of laws through the cooperation between participant nations.

According to the **Budapest Convention** guidance:

> In accordance with the article 5º of the mentioned convention – OFFENSES AGAINST SYSTEM INTEGRITY - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, **when committed intentionally, the serious hindering without right of the functioning of a computer system** by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

In spite of the international guidance about the topic, most of legislations do not mention the crime of ***online kidnapping for ransom***, which basically consists of the duress on the victim to execute, not execute, or tolerate the performance of something upon the use of threat. Note that, despite the expression "data kidnapping", it does not apply to the traditional crime of extortion, since, in this crime, there is the existence of the ***violence and threat of immediate force***, which does not occur in kidnapping for ransom committed through digital instruments as Ransomware. Definitely, this conduct can be found in the catalogue of those considered complex, being therefore the result of the merger of many typical characters, taking as a example the kidnapping, which is used as a way of committing the extortion. In the case of the conduct under discussion, some countries consider the case as a type of criminal coercion added with a special scope, substantiated in the will to earn an economic advantage.

In respect to the Spanish Code, for example, in articles 264[22] and 264-2 of the organic law 10/1995, the kidnapping for ransom is not addressed to a specific manner, since it does not mention the online extortion. But

programs of harmful effects, will be held liable to a prison term of forty-eight (48) ninety-six (96) months and a fine of $100 to $1,000 the minimum statutory monthly wages.

20 In accordance with the **argentine legislation** – resolution 476/2001 of 11/21/2001, article 1º – ILLEGITIMATE ACCESS TO SYSTEM OR COMPUTER DATA - It will be repressed with a fine of 1.500 to 30.000 pesos anyone who illegitimate access by any way to a system of computer data, private ou public, of restricted access. The penalty will be 1 month to 2 years of imprisonment if the individual reveals, realease or commercialize he information illegally accessed.

21 Pursuant to the **Colombian legislation**, in its article 269B – Chapter One – Assaults against data and computer systems confidentiality, integrity and availability –ILLEGITIMATE OBSTRUCTION OF COMPUTING SYSTEMS OR TELECOMMUNICATIONS NETWORKS. Anyone who, without being authorized to do so, prevents from or hinders the normal operation of or access to a computer system, the data contained therein, or to a telecommunications network, will be held liable to a prison term of forty-eight (48) to ninety and six (96) months and a fine of $100 to $1,000 minimum statutory monthly wages, provided that the conduct does not constitutes an offense punishable by a higher penalty.

22 **Article 264 -** Whoever, by any means, without authorization and in a serious way, were to erase, damage, deteriorate, alter, suppress or **making computer data inaccessible**, computer programs or electronic documents pertaining to others, when the result produced is serious, shall be punished with a sentence of imprisonment of six months to three years. **2.** It will be imposed a penalty of imprisonment of two to five years and fine ranging from one to ten times the amount of damaged caused, when any of the following circumstances concur in the conduct described: **1.ª** When committed within the setting of a criminal organization; **2.ª** When special damage has been caused or it a high number of computer system has been affected; **3.ª** The offense has seriously damaged the performance of essential public service or the provision of primary legal interest. **4.ª** The offenses that have affected the computer system of a critical infrastructure or that have created a situation of serious risk for the State's security, of European Union or a member State of European Union. For these effects, it will be considered the critical infrastructure an element, system or considered that this is essential for the maintenance of vital functions of society, the health, the security, the protection and

also, because in some situations, the interpretation of the case law of the mentioned article, however, is done from a perspective that the inaccessibility of data precedes a computer damage, which creates important gaps because not all the hindering of a computer system has to be performed with destruction, alteration or make unusable the information contained there.

As it can be seem, the current Spanish legislation does not embrace the referred conduct in a appropriate manner, considering that the online extortion acquire a specific role when it comes to computer offenses, different from the usual extortion that requires threat of immediate force and violence. The extortion with Ransomware can happen, for example, due to embarassing photographs, exclusive materials, extensive work, and even, essential files for routine and maintenance of companies[23].

In any case, despite it is not a rule, the *iter criminis* of the kidnapping personal data for ransom can also occur the ***computer damage***[24] (destroy, modify, alter ou suppress computer data). In accordance with many specialists authors of the subject, nowadays, the Cyber Criminal Law is already an autonomous reality, thus, the conduct here discussed deserves a specific law. **Brazil**, for instance, does not include as a crime the conduct of kidnapping data, what most closely resembles would be the article 154-A included in the criminal law in joinder with the extortion of article 158, both included in the Brazilian Criminal Code. In addition, in the present case, there is the material requirement that the action imply an undue violation of computer mechanism. The specific intent, in this case, would be the obtention of profit or economic advantage through the hindering of data or information.

Just as in Brazil, what you have in **Portugal** is a formal joinder of offenses, like the *extortion* defined in article 233 of Criminal Code, with *computer sabotage* of article 5º and\or *computer damage* of article 4º, in addition to the *illegal access* of article 6º, all set forth in the Portuguese cybercrime law. Or else, with the *improper access of* article 44º and article 45º referring to the *destruction of violation of data* or *personal data vitiation* criminalized in law 67/98, of October, 26th, of the Lusitanian country.

In a diametrically opposite view, in regard to the kidnapping of personal data for ransom in **California**, the legislation of Senator Bob Hertzberg[25] was signed by the Governor Jerry Brown in September 2016, since the reached solution is found in other direction. The law that defined the crime took effect in January 2017, in order to become illegal in the American State through a specific law. As it can be seen previously, as an example of other countries, the Federal Prosecutor from California handled the issue using existent statutes of extortion. But the SB 1137[26] started 2017 providing a clear sign for the cyber criminals, clearly setting forth that prosecutors needed to convict the kidnappers of data. The law determines the conduct of kidnapping personal data for ransom a punishable crime with penalty of 2, 3 or 4 years of imprisonment in California.

It creates, therefore, an evident tension between the necessities to structure the legal order in accordance with the principle of legality, especially important in criminal terms, particularly when it refers to cyber crimes.

---

economic and social welfare of the population, which the disturbance or destruction would have a significant impact to not maintain its function. **5.ª** The crime have been committed through some manner referred in article 264. If the acts have been resulted of an extreme severity, the greater level penalty might be imposed. (…). **Article 264 bis - 1.** It will be punished with the imprisonment penalty of six months to three years the one that, without being authorized and through a serious manner, he will be punished by imprisonment from six months to three years who, without being authorized and seriously, have obstructed or interrupted the functioning of an unrelated computer system; (…).

23 In order to have an idea of the threaten, it is important to make a self-inquiry: In which way the leakage of information could damage an individual if it is in the possession of a malicious hacker? How it would be if the information were widespread? For example: private conversation with friends on *WhatsApp*; email account with message to the lawyer' private photographs saved in the smartphones; Tinder profile with Matches and conversations; Candy Crush account level 568 with hundred of hours invested; spreadsheet of expenses and corporate files saved in Google Drive.

24 According to the **Chilean Law** related to cyber crime n. 19223 - **Article 1º.** The one that, destroys maliciously or make unavailable a treatment system of information or its parts or components, or hinder, obstructs or modify its functioning, will suffer a penalty of imprisonment in medium or maximum level. If the consequences of conducts affect the data contained in the system, it shall be applied the penalty determined in the previous subsection, in its maximum level. **Article 3º.** The one that, maliciously, case damage or destroy the data contained in a treatment information system will be punished with imprisonment in its medium level.

25 *Read more in:* http://sd18.senate.ca.gov/news/9272016-gov-brown-signs-legislation-punishing-ransomware

26 *Read more in:* **Senete Bill n. 1137 – LEGISLATIVE COUNSELS DIGEST – *CHAPTER 725* -** http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1137

Thus, they are especially significant for this study, the order of specificity and the legal certainty, for the reason that from the State of California, the law can fulfill with the criminal function, avoiding the existence of ambiguous terminologies.

3. The threaten to the Global Digital Economy and the Internet of Things

The difficulty to require a solution, which is not an easy task, is directly connected with the capitalist modernization process of social evolution. The new threaten, as it could be analyzed previously, is connected to the global digital economy, which has been growing significantly for the last years. The industry is working to connect objects to Internet, rising the productivity and innovation.

In accordance with the highlighted by ESET in its report: **Tendencies 2017 - *"The Security as Hostage"***, prepared by specialists of its laboratory of investigation, the Ransomware will continue to be one of the most relevants main actors of the next year. Its threat is exponentially greater as the ***Internet of Things*** settle in or lives and the number of devices multiply. The report suggests that during the next year of 2017, the Ransomware will keep his protagonist's role, and it will arise others, named as ***Ransomware of Things or IoT.*** As suggested by Stephen Cobb, 2017 could be the year of ***Jackware,*** word that refers to the transfer of Ransomware more beyond the computers and portable devices[27]. In 2017, the *Cybersecurity Insiders*, published the ***RANSONWARE 2017 REPORT***, mentioning that the "Ransomware is one of the fastest growing security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. IT and cybersecurity professionals are quickly recognizing ransomware attacks as a significant threat. Eighty percent of respondents perceive ransomware either as an extreme threat (38%) or moderate threat (42%). Very few respondents (5%) see ransomware as no threat at all[28].

The interconnectivity of electronic devices in society – ***the so-called Internet of Thing*** (IoT) – promise to connect electronic devices used in a daily routine, as appliances, industrial machines, video cameras, printers, routers, televisions and including refrigerators. This became the door entrance for the cyber criminals, in which the development depends on the technical innovation[29]. It must be taken into account that the Ransomware does not only attack computers, but also portable devices, where we store several important data. This makes it more dangerous, because the security system of these devices is not very effective. "From there it comes the huge quantity of data that people will have daily, since the more is the usage of these technologies, the more will be the information available, the more will be the information obtained by the kidnappers and, consequently, more valuable" (STAIR, 1998, p. 4).

For instance, some cities as Barcelona already offers intelligent parking meters that operates through Wi-Fi, providing for the users real time updates about available vacancies and allowing the payment of smartphones. Also, using the Internet of Things, doctors will be able to collect data from medical connected devices, including monitors installed at home. All of these electronic devices became a vulnerable tool[30], since, more than shopping in the supermarket and having access to the vacuum cleaner with *RANSOMWARE* techniques, hackers promise to take over the control of other machines that are more dangerous for the users' health.

27 *Available in:* http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/ - *Access in 01-03-2017.*

28 *Available in:* https://www.cybersecurity-insiders.com/portfolio/2017-ransomware-report/ *Access in: 03.05.2018.*

29 The gigantic quantity of new threats to electronic devices that we daily use made the manufacturers of hardware be careless in relation to the security of Internet of Things. For this reason, it was created a rift of security with such serious consequences as the attacks occurred in the EEUU when overturned companies as Amazon, Spotify and Netflix. Known as Bonets, they send malicious electronic mails to detect the confidential password and distribute the ransomware. *Available in*: http://www.pandasecurity.com/spain/mediacenter/noticias/botnets-amenaza-internet-las-cosas/ - *Access in 12-16-2016.*

30 **IF YOU HAVE A SMART TV. PAY ATTENTION BECAUSE IT CAN BE KIDNAPPED.** If until now the Ransomware only attacked computers and smartphones, there are stories that the Smart TV are the "new" victims. Darren Cauthon, a software engineer, revealed that, in a Christmas Day, his Smart TV was infected with a Ransomware. According to a tweet with the TV's photograph, it seems that the Smart TV was infected by a Ransomware Cyber. Police, as known as *Flocker, Frantic Locker, or Dogspectus*. *Available in:* https://pplware.sapo.pt/internet/tem-uma-smart-tv-muita-atencao-que-pode-ser-raptada/ - *Access in: 01-03-2017.*

Another example of a high-level threaten are cars, which are used to be equipped with special technologies that require the Internet access, giving benefits to the driver[31]. However, with *RANSOMWARE* techniques, hackers will be able to program these cars in order to make the engine accelerate in an uncontrolled way, for example, and worse, making unavailable the braking system. Considering, for example, that the last innovation in motorcycle will be the intelligent helmet which promises to integrate an expanded reality to show information in real time for the motorcycle drivers. The motorcycle companies promise to release soon technologies that will provide the prognosis of the roads to the drivers, with access of directions, traffic and time.

This type of sabotage, that uses the *malwares* infections, will be even more a concern for the society while the public and private services are gradually transferred for this cyberspace (LLINARES, 2012, p.58). These are facts that bring concerns, since the cities are developing every day more by using technology and data in public administration, in fact, this tendency will deepen even more, *the counterpoint is the necessity to protect the privacy of the citizens in the face of the ransomware threat*. As this technology will be able to reduce costs and bring greater efficiency and reliability for the private and public sector. It is exactly in this point where the problem is for the industry and consequently the digital economy[32].

To give an overview of the danger, in February 2016, two hospitals in Germany were victims of *RANSOMWARE,* the hackers stopped the operation of all system[33]. These devices use to have a lot of confidential information, however, the security and privacy in general are a secondary concern[34]. As stated by Vice President of European Security, in an interview given for the Spanish newspaper "*El Mundo*", the European regulation of personal data is an "*Attack Industry*". According to Ramy Houssaini, what it seems more serious is that the European regulation is provoking an incentive for hackers, because they will be aware that a company can lose a lot of money in case they suffer an attack, both in economic fine, as well by the reputational damage and the loss of reliance of its clients[35]. Pursuant to inquiries of IT Corporate Risks 2016, made by Kaspersky Lab, the cost of a *malware* attack encrypted to PME in Europe can reach an amount of more than 88 thousand euros[36].

The biggest difficulty is that these new machines will compile information, habits and tendencies of the operators, given that this information will be able to be kidnapped, putting at risk the personal data of its users. The problem is that the *cyberthreats* will be even more intelligent, autonomous and complex to detect than ever. Also, it is expected that these attacks are directed to high-level profile, as celebrities, politics and big companies. This is the reason of the necessity of a specific criminal protection, before the eminence of *Cyberterrorism*.

31 **TENDENCIES 2017 OF ESET: The security as a hostage.** While you are having a dream you listen to your alarm clock of your smartphone, open your eyes and turn off your smartwatch. Your Smart TV welcome you turned on with the news of the day in the maximum volume. You look at the temperature and realize that it is a cold winter morning. You car, as all nights, waits for you parked in front of your home, and you know that if you do not start it to warm the engine, it will be difficult to start-up. To save time, you take your smartphone, open the app of your car and start from the comfort of your kitchen, but there is a problem: the car does not start! You try several times until you restart the app, but is comes up a notification on the screen: "Your car in unavailable". ***If you wish to start it again, please deposit 0,5 Bitcoins in this account.*** Now go back to your dream. Do you think this situation is possible? Is the Internet of Things vulnerable to attacks and threatens as Ransomware? *Available in:* http://www.welivesecurity.com/la-es/2016/12/15/tendencias-2017-de-eset-seguridad/ - *Access: 01-03-2017.*

32 The intelligent devices will not be the only viable scope, but the hackers will also center to attack the critical infrastructures, of which depends on the physical, economical or public security of a country.

In summary, vital to the daily development of a society. *Available in:* http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/ - *Access in 01-03-2017.*

33 It seems that every day new stories comes up about attacks of ransomware in companies, particularly in hospitals and school. Due to the nature of "life or death" of information in hospitals can lead to some individual to give in the criminals demands, believing that this is the best was to restore the access, some school are also giving in to these demands. *Access in: 01-03-2017.*

34 *Read more in:* http://www.welivesecurity.com/la-es/2016/12/15/tendencias-2017-de-eset-seguridad/.

35 *Available in*: http://www.elmundo.es/economia/2016/12/05/58452ef8468aeb63058b45c5.html. *Access in 12-21-2016.*

36 *Read more about the issue in*: https://www.dinheirovivo.pt/opiniao/ransomware-o-rei-do-cibercrime/#sthash.tuhGwKCz.dpuf - *Access in: 01-03-2017.*

4. Final considerations

The conduct, *in casu*, is a current problematic that attempts against the information security, in particular in what it refers to the systems and to electronic data. With this idea in mind, the discussion aimed to focus on the necessity (or not) to create a new definition of crime in order to solve this new type of technological kidnap. Even still considering the reprehensible nature of the legislative agglomeration of the Criminal Law, it was chosen the legislative reform on the matter. In order to reach such conclusion, it was necessary to acknowledge the social transformations occurred in the last decades, reason why it is concluded the necessity to adapt the Criminal Law into the new realities in its primary mission to protect legal interests, such as the information.

By means of the analysis of the comparative-deductive method of the several legislations related to this matter, namely the Spanish, American, Brazilian and Colombian legislations, that it is possible to detect the problem of the extortion, intrinsic requirement of the discussed crime. When analyzing the Spanish and Colombian cases, for instance, it can be concluded that the legislators had the intention to define as a new crime the *Ransomware*, however, they made a point to mention only the issue on the obstruct of the electronic system, putting aside the "extortion". The consequence of the letter in effect in these countries will inevitably lead them to a legal uncertainty. The fact is that, when analyzing some judicial decision on the issue, it was noted the application of joinder of offenses, in general, the crime of the electronic damage, trespass and obstruction, in joinder with the extortion crime. The problem is that the legal interest protected in extortion crime (traditional crime), it differs from the one committed online. In the latter, the legal interest protected is the data and electronic systems, in extortion, it is the property and the physical and psychological integrity. Thus, the legal interests are not the same. Then, as the example of the Maryland state in the United States, the suggestion is the creation of a specific crime, in which is can be included the Ransonware with the specifies that the electronic crimes demand. The Brazilian case is even worse, since there is not specific legislation, handling new problems with old solutions.

Finally, it was noted the necessity to modify the criminal definitions already existent and its urgent adaptation, with the creation of different criminal definitions that correspond to the new sociological reality of data and electronic systems.

5. Bibliographical reference

Barranco, María Concepción Gorjón. *Ciberespacio y delito: la transposición de los instrumentos internacionales.* In Política Criminal ante el reto de la delincuencia transnacional. (Dir. Ana Isabel Pérez Cepeda). Tirant lo Blanch, Valencia, 2016.

Borja Jiménez, Emiliano. *Globalización y Concepciones del Derecho Penal* in estudios Penales y Criminológicos XXIX**.** ISSN 1137-7550 **-** Universidad de Santiago de Compostela, 2009

Costa Andrade, Manuel da; Castanheira Neves, Rita. *Direito Penal Hoje – novos desafios, novas respostas.* Coordenação Manuel da Costa Andrade e Rita Castanheira Neves. Coimbra: Editora Coimbra, 2009.

Llinares, Fernando Miró. *EL CIBERCRIMEN - Fenomenología y Criminología de la delincuencia en el ciberespacio.* Marcial Pons: Madrid, 2012.

Sain, Gustavo Raúl. *Delito y Nuevas Tecnologías: fraude, narcotráfico y lavado de dinero en internet.* 1ª. Edición. Ciudad Autónoma de Buenos Aires: Del Puerto, 2012.

Stair, Ralph M. *Princípios de Sistemas de Informação: uma abordagem gerencial.* Trad. Maria Lúcia Iecker Vieira e Dalton Conde de Alencar. 2.ed. Rio de Janeiro: LTC Editora, 1998.

6. Sites accessed

https://www.cybersecurity-insiders.com/portfolio/2017-ransomware-report/

http://www.silicon.es/a-fondo-como-ataca-ransomware-como-frenarlo-2321602#jJYGyeeXwfcwug2R.99

https://www.google.com/maps/d/u/0/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=39.650962715373
15%2C-94.99983505&z=4
https://www.dinheirovivo.pt/opiniao/ransomware-o-rei-do-cibercrime/#sthash.tuhGwKCz.dpuf
http://www.redeszone.net/2016/11/01/los-dispositivos-moviles-iot-cloud-seran-los-principales-objetivos-los-cibercriminales-2017/
https://derechodelared.com/2015/12/17/historia-del-ransomware-infografia/comment-page-1/
http://www.europapress.es/portaltic/sector/noticia-empresas-pagan-media-500-euros-recuperar-datos-ataque-ransomware-20161202143624.html
http://www.channelbiz.es/2016/11/29/un-ransomware-ataca-la-ciudad-de-san-francisco/
http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1137
http://sd18.senate.ca.gov/news/9272016-gov-brown-signs-legislation-punishing-ransomware
http://www.ticbeat.com/seguridad/ransomware-de-las-cosas-2017-informe-eset/
http://www.pandasecurity.com/spain/mediacenter/noticias/botnets-amenaza-internet-las-cosas/
https://pplware.sapo.pt/internet/tem-uma-smart-tv-muita-atencao-que-pode-ser-raptada/
http://www.welivesecurity.com/la-es/2016/12/15/tendencias-2017-de-eset-seguridad/
http://www.elmundo.es/economia/2016/12/05/58452ef8468aeb63058b45c5.html