THE CRIMINALIZATION OF THE RANSOM PAYMENT IN RANSOMWARE ATTACKS

— A COMPARATIVE ANALYSIS UNDER COMMON AND CIVIL LAW COUNTRIES

Masters of Transnational Law

Under the guidance of Professor Pedro Freitas

Catarina Ferreira da Silva

N.º 147021006

Global School of Law | UCP Lisbon
March, 2023

To me.

Acronyms, Abbreviations and Terminology

CPP	Código Penal Português | Portuguese Criminal Code
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
N.C.G.S	North Carolina General Statutes
OFAC	Office of Foreign Assets Control
StGB	Strafgesetzbuch
UK	United Kingdom
US	United States
USA	United States of America

Table of Contents

1. Introduction 6

2. Cybercrimes: the particular case of ransomware attacks 8

2.1. Notion and Elements. Commodity Ransomware and Ransomware as a Service (RaaS) 8

2.2. The cyber extortion element 9

3. Ransom Payment 10

3.1. Why should victims not pay the ransom? 10

3.2. Why do victims pay the ransom? 11

4. The criminalization of the ransom payment 13

4.1. Arguments For and Against 14

4.2. Legal Analysis of the Criminalization 16

4.2.1. The elements of a crime 16

4.2.1.1. *Actus Reus* 17

4.2.1.2. *Mens Rea* 20

4.2.1.2.1. The problem of duress and necessity as a defense 22

4.2.1.2.2. Brief Mention to the Crime of Criminal Association under Article 299.º of the Portuguese Criminal Code 26

4.2.1.3. Corporations' criminal liability 27

4.3. Parallel with Terrorism Kidnapping regime 28

5. Brief Overlook to the Insurance Company's Role 31

6. Recommendations and alternatives to criminalization. Analysis of initiatives already implemented 32

7. Conclusion 35

8. Bibliography 37

8.1. Books 37

8.2. Articles 38

8.3. Websites 40

1. Introduction

According to the 2021 Europol's Annual Internet Organized Crime Threat Assessment, ransomware attacks continue to be a dominate threat in the area of cybercrimes year after year, increasingly focusing on large corporations and public institutions, mainly in the healthcare and education sectors[1]. This is justified by the fact that these targets are more willing to pay the demanded ransom either because they have more economic power or because they are least likely to be able to support downtime - if a hospital sees it electricity power being affected due to a ransomware attack which, in it turns, implicated that all medical machines were temporarily inoperative, its willingness to pay the demanded ransom gets comprehensively higher. In 2021, the average ransom payment was US 812.360,00, 4.8% more than in 2020[2].

With the majority of companies and services converting their business to an online model, especially after the COVID-19 pandemic, the quantity of possible cybercrime targets has increased exponentially and with that the amount of ransomware attacks. In fact, by 2025, these crimes are expected to cost more than US$10 trillion annually to the world[3]. When it comes to ransomware attacks, 66% of organizations were hit by a ransomware attack in 2021 as opposed to the 37% in 2020 - this represents an increase of 78% over a course of a year[4]. On the other hand, over the first half of the year of 2021, Coalition, a major US insurance company, noted an increase of 67% of ransomware attacks claims on the healthcare sector, that, according to this entity, is mainly due to the fact that these were the more vulnerable industries in times of COVID-19 since they were more concerned about providing critical patient care than focusing their human and economic resources on protecting their digital assets[5].

On top of this, not only the amount and the costs of ransomware attacks are increasing, but also the seriousness of the damages caused by it. On September of 2020, a ransomware attack to the IT system of a German Hospital led to a woman losing her life because she had to be transferred to another Hospital[6]. Even though indirectly, this case is able to show the extent

[1]Available at https://www.europol.europa.eu/ accessed on 15/01/2023.
[2] SOPHOS, *The State of Ransomware 2022 Report*, Pag.5 available at https://www.sophos.com/.
[3] MORGAN Steve, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025'*, Cybercrime Magazine, Nov. 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed 8/10/2022).
[4] SOPHOS, *ob.cit.* Page 3.
[5] Coalition 2022 Cyber Claims Report, Page 10. Available at https://info.coalitioninc.com/. Accessed on 15/01/2023.
[6] German hospital hacked, patient taken to another city dies, AP news, 17/09/2020. Available at https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94. Accessed 9/10/2022).

of the consequences that these attacks can have and how threatening they can be not only on a financial point of view, but also on a humanitarian one.

As previously mentioned, the majority of ransomware attacks are done with the sole purpose of demanding a ransom. A demand under the threat that either the victim will not get the encrypted data back or that the data will be leaked to the general public. Either way, it must cause significant pressure to the victim in a way that makes her feel compelled to pay the ransom instead of reaching out to the law enforcement. Compelled enough to disregard the common knowledge that by paying the ransom, the victim is contributing to financing these criminal organizations. A moral dilemma in which the self-interest of the victim is very often given priority towards the necessity of making global efforts in fighting the perpetuation of these kinds of crimes. Thanks to this tendency, the cybercriminals have been able to get the necessary financial resources to improve their material, techniques and expertise and with that engaging in attacks progressively more sophisticated and effective. It is a vicious cycle that the cyber community, governments, and law enforcement have been uniting efforts in trying to break.

Among multiple initiatives, one that stands out is the possibility of criminalization of the ransom's payment in a way that by not allowing the victims to pay the ransom it will remove from cybercrime organizations their main source of profit and thus reducing their activity. Even though this debate is not new in areas such as Terrorism Kidnapping and Maritime Piracy, the new digital era has extended it to cyber criminality, more particularly to ransomware attacks.

In chapter two we begin by explaining what ransomware is and its elements, in particular the extortion element. Then we move on to an analysis of the reasons why, on the one hand, victims should not pay the ransom and, on the other, why they nevertheless tend to do it. Chapter four is the core of our Paper by breaking down all the legal specific requirements that a ransom criminalization must obey: *actus reus* and *mens rea*, eventual defenses and legal personhood; while comparing the problematic with the more developed doctrine of terrorism kidnapping. Moving towards the end, chapter five briefly brings attention to a third party that plays an important role in ransomware attacks - insurance companies. Finally, in chapter six we expose recommendations that have been given if a criminalization is to take place and analyze eventual alternatives that either were proposed or already put into place.

2. Cybercrimes: the particular case of ransomware attacks

2.1. Notion and Elements. Commodity Ransomware and Ransomware as a Service (RaaS)

There is no consensual definition of *cybercrime* as a legal concept. In the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, cybercrime was generally referred as to "any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. (...) it encompasses any crime capable of being committed in an electronic environment."[7]. On the other hand, this concept can be unfolded in two subcategories: cybercrime in a narrow sense (as a *computer crime*), where the security of computer systems and the data processed by them are the target of the offense; and in a broader sense (as a *computer-related crime*), where is included any illegal activity carried out by a computer system or network[8].

One type of cybercrimes are the ones carried out through the implementation of *ransomware* on a computer system. Ransomware is a type of malicious software (malware) that gives rise to the practice of two different crimes: hacking and cyber extortion[9]. For this purpose, *hacking* consists of the unauthorized access to a computer material (either data or system) by infiltrating a malware capable of encrypting, locking, stealing or deleting any information and thus disabling its access from the owner[10]. In order to regain access to the affected material, the victim is psychologically manipulated into paying a demanded ransom (*cyber extortion*). Therefore, three main elements are always present on this type of attack: *assets*, i.e., the material that is targeted, an *action*, encryption, locking, deleting and stealing and, finally, *blackmail* or *cyber extortion* through which cybercriminals coerce the victim by means of threats demanding something in return for the material's availability[11]. This malware is introduced on the computer system mainly through two vectors: phishing e-mails and brute-forcing on Remote Desktop Protocol (RDP)[12].

[7]Available at https://digitallibrary.un.org/. Page 4 §9. Accessed on 20/01/2023.
[8]Available at https://digitallibrary.un.org/. Page 5 § 14. Accessed on 20/01/2023.
[9] BORRION Hervé and CONNOLLY Alena Yuryna, *Your Money or Your Business: Decision-Making Processes in Ransomware Attacks*, in Forty-First International Conference on Information Systems, India 2020., Page 1.
[10] LI Chen, LIAO Qi, *Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling ransomware*, in ARES 2020, August 25–28, Virtual Event, Ireland 2020. Page 1.
[11] 2022 ENISA Threat landscape for Ransomware Attacks, Page 8. Available at https://www.enisa.europa.eu/. Accessed on 21/01/2023.
[12] ENISA Threat Landscape 2021, Pages 34-35. Available at https://www.enisa.europa.eu/. Accessed on 21/01/2023.

In the early years of ransomware, the majority of it would be spread either by the malware authors themselves, highly technically savvy individuals, or by persons who would resort to *commodity ransomware*. Commodity ransomware operators would "take advantage of preexisting work, often copying and modifying leaked or shared source code, causing the formation of ransomware families"[13]. By 2016, reports started to show a new tendency of ransomware practice, the *Ransomware as a Servic*e (RaaS)[14]. Groups of programmers would create a base ransomware and then either licensing it, charging, for example, a fee on the amount collected from the attack, or selling it. This became a game changer in cyber criminality since, on the one hand, allowed criminals with very little knowledge on programing to have access to ransomware and, on the other, maximized the profits of these kinds of attacks since the initial expenditure in developing the ransomware code did not exist. The access of ransomware became open to anyone on the DarkWeb who had the means to pay for this kind of service.

2.2. The cyber extortion element

As previously mentioned, a key feature of criminality resorting to ransomware is the extortion pursued by the attackers. In its simplest form, *extortion* is here accomplished by demanding the payment of a certain amount under the threat that the data or system at stake will remain non-accessible. However, in order to increase the pressure on the victims or, in cases where the victims have managed to regain access (for example, due to preexistent backups), to still carry the attack forward, cybercriminals have resorted to *double extortion* which, in its turn, consists of two threats. The first is the maintenance of the data encrypted or locked, like in the simple extortion. The second one can either be public exposure, i.e., the attacker leaks the information to the general public or to a specific group or person/entity for free or be the sale to a third-party of the concerned digital assets[15]. In fact, there are cases where the leakage of information can be more damaging for the victim than the mere inability to access it. The disclosure of business secrets may ruin all the competitive advantage of a company, the exposure of compromising files may result in criminal liability or the leakage of personal data on the application of millionaire fines - these are some of the examples where the second layer of extortion can effectively increase the willingness of the victim to pay the ransom. In more sophisticated cases, the data is even held hostage on a "leak or dump-site" owned by the

[13] CABLE Jack, OOSTHOEK Kris and SMARAGDAKIS Georgios, *A Tale of Two Markets: Investigating the Ransomware Payments Economy*, 2022. Page 2.
[14] CABLE Jack, OOSTHOEK Kris and SMARAGDAKIS Georgios, *ob.cit*., Page 2.
[15] LI Zhen and LIAO Qi, *ob.cit.*, calls the ransomware that resorts to double extortion the Ransomware 2.0.

attackers while the negotiations are ongoing[16]. We do have to keep in mind, however, that the double extortion makes only sense for the cybercriminals if the data has a certain nature: first of all, the data must be "sharable", meaning that if we are talking about a ransomware attack that disrupts a system, in practice, there is no data to share or sale - the simple extortion is the only option. On the other hand, for the cases where the second extortion is public exposure, the data must either hold some sort of public relevance (e.g., the commitment of a crime) or its exposure must affect the victim greatly. Finally, in the case of threat of selling, the data must obviously have market value.

3. Ransom Payment

On the victims' perspective, when confronted with a ransom demand they find themselves in a deadlock where, on the one hand, they see their data being taken away or their services blocked possibly leading to their business crumbling down and, on the other hand, they are afraid that the attackers do not keep their promises and the data is not returned. The ethical dilemma is also predominant here since the victims get conflicted between the moral duty of not contributing to the growth and prosperity of these organizations and the temptation to just pay the ransom and get rid of the problem.

3.1. Why should victims not pay the ransom?

Multiple institutions have already made public statements firmly discouraging victims from not paying the ransom. The FBI is one of them, stating that "paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity"[17]. In 2019, the United States Conference of Mayors issued a resolution expressly against the payment of ransom in ransomware attacks towards local US government entities[18]. Indeed, studies show that in 2021 only 61% of the organizations who paid the ransom got the encrypted data back, but only 4% out of those got all the data back[19]. Plus, even if the data is returned, and now in particular to the cases of double extortion, nothing guarantees that the data is not nevertheless exposed.

[16] ENISA Threat landscape 2021, Page 36.
[17] Common Scams and Crimes, Scams and Safety, Official Website of FBI. Available at https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware. Accessed on 25/01/2023.
[18] Resolution adopted at the 2019 87th Annual Meeting. Available at https://www.usmayors.org/the-conference/resolutions/?category=a0D4N00000FCb3LUAT&meeting=87th%20Annual%20Meeting.
[19] SOPHOS, *The State of Ransomware 2022: Survey*, April 2022. Page 4.

On the other hand, the more tech dependent companies and entities get, the more powerful cyberattackers become. Such power reflects not only on the quantity and diversity of data that can be targeted, but also on the amount that they can demand as ransom. A part from the revenue that they can have through the sale of the stolen data, what typically happens in ransomware attack is that these criminal groups get their funding by the payment of ransom that, in its turn, is used to pursue multiple goals: personal profit, financing other criminal activities, such as human or drug traffic or, more simply, to improve the ransomware business model allowing criminals to develop their codes and computer systems, hire more skillful hackers and get better infrastructures.

A point worthy to be mentioned in this regard, although considerably less important than the above mentioned, is the fact that paying the ransom leaves a precedent to that particular victim. Cyber criminals usually seek for victims that look more fragile and more prone to paying the ransom. Even if at first sign that was not the case, once a certain victim pays the ransom following an attack, nothing guarantees that is not willing to do it again in future cases.

3.2. Why do victims pay the ransom?

Regardless of what ethics, statistics or economics say, the truth is that 46% of victims have paid the demanded ransom in 2021[20]. However, this data shall be analyzed with critical eyes since most of the companies that suffered from a ransomware attack opt by not disclosing whether they have or not paid the ransom and this is mainly due to the fact that we developed on the previous chapter - admitting that they cave in is a way of showing weakness, not only towards cyber criminals but also towards their customers and competitors.

According to Michael Daniel, President and Chief Executive of the Cyber Threat Alliance[21]companies tend to pay the ransom because they

> feel they have no choice, whether it's due to the threat of insolvency, reputational damage stemming from service interruptions, or the potential for loss of life or wide-scale economic disruption. (…) Indeed, from a purely short-term, organizational viewpoint, paying a ransom is often an economically rational decision[22].

[20] SOPHOS, *The State of Ransomware 2022: Survey*, April 2022. Page 4.
[21] The Cyber Threat Alliance is a non-profit organization composed of international companies and institutions of the cybersecurity field, whose main purpose is to improve the overall cybersecurity of the global digital ecosystem.
[22] TIDY Joe, *Ransomeware: Should paying hacker ransoms be illegal?*, BBC News, 20/05/2021. Available at https://www.bbc.com/news/technology-57173096. Accessed on 26/01/2023.

On a study carried out by BORRION and CONNOLLY[23][24], they came to the conclusion that multiple factors influence the decision-making process of the victims to pay the ransom, among which we particularly highlight the risk of bankruptcy, the type of the affected data and the fear of incrimination.

Regarding the risk of bankruptcy, these Authors concluded that it has a more significant weight on private entities as opposed to public ones since the former are generally more profit driven than the latter ones and thus the financial implications tend to be a relevant factor to be taken into consideration when confronted with a ransom demand. In fact, in certain cases, paying the ransom is less expensive than the post-attack recovery costs.

Another important factor is the typology of the affected data. In order to pursue a successful ransomware attack, the asset must have a significant value either to the victim or to a third-party directly connected to it. The value does not have to be necessarily economic wherefore academic research, sensitive or privileged information, for example, although perhaps with little economic relevance, may hold enough importance for the victim to feel compel in paying the ransom. The assessment of the relevance of the data to the victim and the consequences of its loss are naturally part of the due diligence that cybercriminals have to undertake before the attack.

Lastly, under this study, the Authors found out that the fear of incrimination plays an important role in the decision-making process of the victims. It is mainly connected with the duty of report that the companies that process personal data have, in their quality of data controllers, when it comes to occurrence of events that affect such data[25]. This duty is due to the affected data owner and if breached entitles the data protection authority to impose an administrative fine that can go up to EUR 10.000.000,00[26]. This possibility is often alleged by the cybercriminals in order to increase the pressure on the victims, especially since the demanded ransom is presumably lower than this value.

Another factor outside of the mentioned study worthy to mention is the undeniable lack of trust of the victims in the law enforcement capacities. Even though law enforcement agents have made considerable efforts in combating cyberattacks by improving their technological skills, cybercriminals are still a step ahead and it is not always possible for law enforcement to

[23] BORRION Hervé and CONNOLLY Alena Yuryna, *Reducing Ransomeware Crime: Analysis of Victims' Payment Decisions*, at Computers & Security 119, Elsevier, 2022.
[24] This case study examined 41 ransomware attacks that occurred between 2014 and 2018 whose victims were large, medium and small enterprises from the public and private sector.
[25] According to article 34.º of the GDPR.
[26] According to article 83.º n.º 4 a) of the GDPR.

unlock or decrypt the files/systems, at least with the desired speed. Consequently, victims aiming for a quicker recovery often fall into the temptation to pay the ransom even though they know that recovery is not guaranteed.

4. The criminalization of the ransom payment

One solution that has been on the agenda of Governments and institutions to fight the ransomware plague is the criminalization of the ransom's payment. In this sense, by criminalizing it, victims are no longer able to "just pay to get rid of" and are not only obliged to report to the law enforcement about the attack but also to leave in the hands of the latter the application of the adequate and necessary legal measures. However, this solution is far from being unanimously accepted by the cybersecurity community since, despite its (or at least apparent) immediate ability to deprive the growth of ransomware attacks substantively, the criminalization of the victim's payment has important cons that must be addressed. On the other hand, law principles and conditions must be respected in order for a new type of crime to be created which, in its turn, may vary among jurisdictions.

For the time being, no Government has implemented a straightforward decision that outlaws ransom payments altogether. Nevertheless, organizations and policymakers have already publicly expressed their opinion on the ban and even some legislative initiatives have already been put into place. In the State of New York, two bills have been introduced to the Senate in order to prohibit municipalities from paying ransomware attackers: a bill introduced by Senator Phil Boyle to prohibit local governments from using taxpayer money to pay the ransom "Notwithstanding any other provision of law, after January first, two thousand twenty-two, local and state taxpayer moneys shall not be used to pay ransoms in response to ransomware attacks"[27] and another one introduced by Senator David Carlucci according to which "No municipal corporation or other government entity shall pay ransom in the event of a cyber-attack against such municipal corporation or such government entity"[28]. In 2022, North Carolina[29] and Florida[30] became the first U.S States enacting laws prohibiting state entities from making a ransom payment or communicating with a threat actor following a cyberattack[31]. In

[27]Bill S7246. Available at https://trackbill.com/bill/new-york-senate-bill-7246-relates-to-creating-a-cyber-security-enhancement-fund-and-restricting-the-use-of-taxpayer-moneys-in-paying-ransoms/1831809/.
[28]Bill S7289. Available at https://trackbill.com/bill/new-york-senate-bill-7289-relates-to-prohibiting-the-paying-of-ransom-in-the-event-of-a-cyber-attack/1843400/.
[29] N.C.G.S. § 143-800.
[30] The State Cybersecurity Act (§ 282.318 Fla. Stat.).
[31] PAINTER RANDALL Karen, MCNELIS III Joseph, *Two States Now Prohibit Public Entities from Paying Ransoms* in Connell Foley: Legal Blogs and Updates, 18/08/2022. Available at

Australia, in the sequence of a massive cyberattack against Medibank Private Ltd, Australia's biggest health insurer, Australia's Home Affairs Minister Clare O'Neil admitted that the Government would consider making illegal the payment of ransoms under cyberattacks[32].

4.1. Arguments For and Against

As we have already had the chance to mention previously, the main arguments for the criminalization of the ransom payment are the funding of criminal activity and the low chances of getting the data back.

As for the arguments against it, from the study of the current doctrine about this matter, we have gathered a substantial amount of them.

Firstly, criminalizing the payment of the ransom is assuming that the victims, even after the cyberattack, will still have the necessary financial capacity to support *downtime*, i.e., the time between the attack and the moment where the system or files lost will be effectively reestablished - either due to law enforcement aid or to self-mechanisms that the company itself put into action. However, at the same time, even if that financial capacity exists, there are types of companies that by its very nature simply cannot support any downtime like organizations that are considered to be essential to society, such as, for example, hospitals, schools, energy providers, and other critical infrastructures[33]. This problem will then lead to what some authors consider the "chicken game". Jen Ellis, Vice President of Community and Public Affairs of Rapid7[34] believes that this game will consist of criminals just shifting their focus towards those companies and organizations that are least likely to deal with downtime. In this way, criminals will expect the harm to society caused by the downtime to apply the necessary pressure to ensure they get paid[35].

Secondly, in certain cases, *paying the ransom is financially more advantageous to the victim* than not paying since the ransom may be less expensive than the post-attack recovery costs. It is misleading to assume that the only companies that are targeted with a ransomware attack are the ones that have a weaker security infrastructure. Nowadays, with the incomparable high speed with which technology has been developing, ransomware is constantly being

https://www.connellfoley.com/blog/Two-States-Prohibit-Public-Entities-Paying-Ransoms. Accessed on 23/01/2023.

[32] MCKEITH Sam, *Australia to consider banning paying of ransoms to cyber criminals*, Reuters, 14/11/2022. Available at https://www.reuters.com/technology/australia-consider-banning-paying-ransoms-cyber-criminals-2022-11-12/. Accessed on 2/02/2023.

[33] Ransomware Task Force, *Combating Ransomeware - A comprehensive Framework for Action: Key Recommendations from the Ransomeware Task Force*, IST, April 2021. Page 49.

[34] Software company that provides multiple services of cybersecurity in computer systems.

[35] TIDY Joe, *ob.cit*.

readjusted and redesigned in order to break the most sophisticated and updated security systems. Companies have been heavily investing in their security and therefore any interruption of those systems can imply unconceivable damages, perhaps even higher than the amount demanded by the attackers.

Another argument is that criminalization might be *counterproductive*. In recent studies was found that 45% of the victims of cyberattacks do not report them to law enforcement for fear it will slow things down, and 37% because they have paid the ransom and do not want to get in trouble[36]. If even with paying the ransom being legal people tend to not report cyberattacks, it is predictable that these numbers may increase once the payment is criminalized. The bias to hide from law enforcement the details of the attack will increase due to fear of being punished. On the other hand, the FBI have already spoken in this regard raising concerns for the aggravating factor that by not reporting the ransomware attack these companies only give to cyber attackers another motive for extortion by blackmailing them for paying the ransom and not sharing that to law enforcement[37] - it is a case to say

The cure is worse than the disease.

It must be also noted that, because of its very nature, the criminalization of ransom payment will *not be effective in preventing cases of double extortion*. In Chapter 2.2 we explained that some cases of double extortion consist of the threat of selling the data which, in its turns, presupposes that such data holds any market value. Well, even if the cyber criminals get no financial benefit from the ransom, they can still achieve it through the sale of the data. In a sense, by criminalizing the ransom payment, not only it is encouraging the growth of a parallel market - the sale and purchase of stolen data - but also increasing the odds of privileged information being openly disclosed, namely affecting third-party rights like, for example, in the case of personal data.

Moreover, it shall be taken into consideration the *risk of attention shift or jurisdiction selection* from the cyber attackers to States where the ransom payment has not (yet) been criminalized. Alike any other matter, the heterogeneity in laws across jurisdiction has the unavoidable consequence of enabling criminals to strategically choose their targets as to select the ones whose applicable law will not prevent them from freely paying the ransom[38]. This has

[36] Statistics come from a recent study, commissioned by Talion and carried out by One Poll in June 2021. One Poll surveyed the attitudes of 1000 UK employed adults and 200 UK IT Security Professionals. Available at https://talion.net.

[37] https://edition.cnn.com/2021/07/27/politics/senate-judiciary-ransomware-hearing/index.html.

[38] With the same reasoning, see BUNDY C. Elizabeth, *Rescuing Policy and Terror Victims: A Concerted Approach to the Ransom Dilemma* in Michigan Journal of International Law, Vol. 37, Issue 4, 2016. Page 730.

typically happened in cases of terrorism kidnapping where due to the limited number of States that expressly assumes a position of no-concessions negotiating and thus not paying ransom to terrorists, although not criminalizing it, little is accomplished towards deterrence of this criminal activities - "[i]nstead of deterring kidnapping schemes or inhibiting funding at a broad-reaching level, the prohibitions have merely shifted organizational efforts toward kidnapping nationals of countries that are known to make payments."[39]

Another criticism that can be appointed towards a criminalization is the *States' obligation to protect international human rights*. When a couple of paragraphs above we talked about the issue of downtime, we mentioned a particular type of victims whose correct functioning and integrity are essential for human's safety and health (e.g., health care facilities, nuclear stations, electricity companies, among others). In these cases, when a ransomware attack strikes, the consequences of system interruption have the potential to directly affect peoples' life and safety[40] and thus international fundamental rights. In this sense, victims might be confronted with a situation where if they do not pay the demanded ransom, people's right to life, for example, might be violated, having no choice but to pay. By criminalization this type of behavior, the State can be violating its core duty of protection under international human right law[41].

Last but not least, in some countries such as in the USA, not only is the ransom payment not criminalized (apart from the States of North Carolina and Florida), but it also is even deductible in taxes. Accordingly, to tax experts, "companies have long been able to deduct losses from more traditional crimes, such as robbery or embezzlement (…) [therefore] ransomware payments are usually valid too"[42].

4.2. Legal Analysis of the Criminalization

4.2.1. The elements of a crime

Generally speaking, both common and civil law countries recognize that a crime is composed of two elements: an objective and a subjective element.

[39] BUNDY C. Elizabeth, *ob.cit*. Page 730.
[40] In this regard, see Chapter 1 §3.
[41] BUNDY C. Elizabeth, *ob.cit*. Page 734.
[42] CBS, *Extorted by ransomware gangs? The payments may be tax-deductible*, CBS News, 21/06/2021. Available at https://www.cbsnews.com/news/ransomware-payments-may-be-tax-deductible/. Accessed on 10/02/2023.

In common law, the former element is the *actus reus* and the latter the *mens rea*. The general principle is that a person shall not be convicted of a crime unless it was proved beyond reasonable doubt[43]

> (a) that he[/she] has caused a certain even or that responsibility is to be attributed to him[/her] for the existence of a certain state of affairs, which is forbidden by criminal law [***actus reus***], and (b) that he[/she] had a defined state of mind in relation to the causing of the event or the existence of the state of affairs [***mens rea***].

In civil law, the *actus reus* roughly corresponds to the "tipo objetivo de ilícito" and the *mens rea* to the "tipo subjetivo de ilícito". For the sake of simplification, we will resort to the common law terminology of these elements.

On the other hand, even in the existence of a crime, there are a number of situations where the author, although had committed a crime, is not punished by it due to the particular circumstances under which the crime was performed - the so-called *defenses*.

When theorizing about a potential criminalization of the ransom payment, the lawmakers must fulfill this prerogative and find legal basis for, on the one hand, determine the need to consider the payment of the ransom under a ransomware attack an objectively criminal act, i.e., worthy of being forbidden by criminal law and, on the other hand, sustaining the existence of a ransomware victims' state of mind in accordance with the one also required by criminal law.

4.2.1.1.*Actus Reus*

First and foremost, for a crime to exist, there must be an action or omission carried out by a specific person that is censored and punished by the criminal law. It is thus not sufficient that such conduct is illegal, but it must be worthy of criminal law regulation, although it can be also regulated under other fields of law. So, one must ask, on what grounds can a State determine that paying a ransom to a ransomware criminal group is a *criminal wrongdoing*?

"To criminalize a certain kind of conduct is to declare that it is a public wrong that should not be done, to institute a threat of punishment in order to supply a pragmatic reason for not doing it, and to censure those who nevertheless do it"[44]. In order to do so, lawmakers must bear in mind fundamental criminal principles that underlie the whole criminal legal system. These principles are multiple, and each criminal law Author has their perspective on them. For

[43] HOGAN Brian and SMITH J C, *Criminal Law*, Seventh Ed., Butterworths, 1992. Page 28.
[44] ASHWORTH Andrew and HORDER Jeremy, *Principles of Criminal Law*, Seventh Ed, Oxford University Press, 2013. Page 22.

the purpose of our paper, we will focus on the principles that we considered to be particularly problematic or important on an eventual criminalization of the ransom payment. However, this is not intended as a means to create any sort of principles hierarchy or to imply that other principles should not be overlooked in this regard.

A cornerstone idea governing criminal law is that this field of law should, by its very nature, be reserved to the protection of fundamental legal rights and values considered as such by the community - "serious antisocial acts that must be abandoned"[45] that justify the harshest sanctions[46] - although, for Authors such as ASHWORTH, many of the conducts that are criminalized might not be more than a practical political choice as to control a certain activity without necessarily implying the element of social condemnation[47]. This is the underlying premise of the *Principle of criminalization in ultima ratio* or one of the branches of the Minimalism Principal[48], according to which

> [a] conduct should only be criminalized and the criminal justice system only be applied as a last resort, *i.e.*, if all other avenues [meaning, others field of law] that are less coercive than criminal law fail to sufficiently forestall or repress the harmful conduct[49]

On a European level, this principle has already been acknowledged, even though under the interpretation of the Principle of Proportionality, namely by the European Commission

> Criminal investigations and sanctions may have a significant impact on citizens' rights and include a stigmatising effect. Therefore, **criminal law must always remain a measure of last resort**. This is reflected in the general principle of proportionality (as embodied in the Treaty on European Union and, specifically for criminal penalties, in the EU Charter of Fundamental Rights) .[50] (emphasis added)

In this sense, any legislative initiative towards an eventual criminalization of the ransom must take into consideration this underlying idea that outlawing the payment of ransoms has and must always be done in a last resort manner. However, it must also acknowledge the

---

[45] ASHWORTH Andrew, *Principles of Criminal Law* in Clarendon Law Series, Third Ed., Clarendon Press Oxford, 1999. Page 1.

[46] We do however shall make the disclaimer that, nowadays, the lines between a severe sanction and a non-severe sanction are increasingly blurry and are under a subjective analysis. There might be cases where a civil sanction (e.g., monetary) might be much more severe for the individual than a suspended imprisonment order, for example.

[47] ASHWORTH Andrew, *ob cit.* Page 1.

[48] According to ASHWORTH Andrew, *ob cit.* Page 35.

[49] JENDLY M. and VAN KEMPEN P.H.P.H.M.C., *Overuse in the criminal justice system ; Le recours excessif au système de justice pénale : on criminalization, prosecution and imprisonment : aux sanctions et poursuites pénales et à la détention* in International Penal and Penitentiary Foundation n º 47, intersentia, 2019. Page 6.

[50] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*, Brussels, 20.9.2011 COM(2011) 573 final, Page 7.

difficulty of such assessment, i.e., when is the breaking point? When can a lawmaker be in position to determine that any other measure failed to achieve the concrete purpose of the criminalization of the ransom payment? An effort must be made by Governments in order to exhaust all possible legislative alternatives, mainly by creating civil or administrative laws in order to set a legal environment deterrent of ransom payments.

Another relevant principle, particularly relevant in common law countries, is the *Harm Principle* according to which a states' authority on criminalizing a certain behavior lays on the fact that this one provokes a certain harm to others or creates an unacceptable risk of its occurrence. The main usefulness of this principle is to restrict criminal law from penalizing conducts that are regarded as immoral or otherwise socially unacceptable but that do not cause or have a risk to cause harm to others. This does not entail, nonetheless, that the moral, cultural and political nature of the peoples' legitimate interests that are being protected shall not be recognized and considered[51]. In the case of paying ransom, the harm, or more accurately the risk of harm, is mainly not directed to a specific victim (it would only be the case if it could be proven that a specific payment of ransom was used to finance a specific ransomware attack), but to the public in general - it promotes criminal activity[52]. There is no immediate materialization of the harm - like in typical cases as a murder where the harm is the loss of the victim's life - but the harm is fractionated in time instead. The conduct of paying ransoms "may not be wrongful or harmful in itself, but it [could have been] criminalized because of the consequences that may flow from it. (...) the risk is explicit"[53] - the conduct has a *remote harm*. In this regard, ASHWORTH and HORDER[54] expose two objections for the criminalization in the case of remote harms that demonstrate to be particularly relevant in the case of ransomware attacks. On the one hand, "if conduct is criminalized on account of what it might lead another person to do, such an intervening voluntary act should relieve the original actor of criminal liability, and so it is the person who does that voluntary act who should be penalized". On the other hand, if the conduct "is not harmful in itself[, then it] should not attract liability, or (...) at least not unless it is accompanied by an intention to encourage, assist, or commit a substantive offense". Transposing to the ransomware problematic, the former critic explains that basically the control over the existence of harm, i.e., the decision of whether to provoke harm or not, is in the hands of cyberattackers and not in the hands of the ransomware victims and therefore they

[51] ASHWORTH Andrew and HORDER Jeremy, *ob.cit.* Page 28.
[52] There is a "public wrong", see ASHWORTH Andrew and HORDER Jeremy, *ob.cit.* Page 30.
[53] ASHWORTH Andrew and HORDER Jeremy, *ob.cit.* Page 38.
[54] ASHWORTH Andrew and HORDER Jeremy, *ob.cit.* Page 38-39.

should not be held liable for that. At the same time, according to the latter critic, because the objective conduct of paying the ransom is not harmful in itself, it shall only be criminalized if it is done with an intention to encourage the substantive offense that is to help cybercriminals to carry on with ransomware attacks[55]. Nevertheless, these Authors appeal for the necessity of taking into consideration the magnitude of the harm and the likelihood of its occurrence, admitting that criminal law also should look for the overall people's welfare.

For civil law countries, the narrative is not so much focused on the existence of harm but more about the *legal good* that is at stake. Among the multiple legal goods that are considered to be worthy of protection, in the case of a ransom payment prohibition, in our opinion, the one that can be claimed is the public peace, albeit abstractly. "The mere existence of criminal associations, linked to their inherent dynamics, undermines the feeling of peace that the legal order aims to create (...) and the belief in the maintenance of that peace to which citizens are entitled, replacing them with a notorious feeling of generalized fear"[56]. The action of paying the ransom implies a special danger for the legal good into question - public peace - since, by serving the purpose of funding criminal activity, increases the likelihood of future crimes to be committed. By criminalizing such behavior, under civil law, this could be framed in those crimes called crimes of *abstract danger*

> where certain behaviors are typified in the name of their typical danger to a legal good, but without the need to prove it in the concrete case: **there is an irrebuttable presumption of danger and, therefore, the agent's conduct is punished regardless of whether or not he has created an effective danger to the legal good.** (emphasis added).[57]

4.2.1.2.*Mens Rea*

"Guilty mind" is the translation to *mens rea*. However, guilt shall not here be taken as a feeling *per se* since "[a] man may have *mens rea* (...) without any feeling of guilt on his part. He may (...) be acting with a perfectly clear conscience, believing his act to be morally, and even legally, right, and yet be held to have *mens rea*."[58]. This element allows the criminal justice system to "decide whether the defendant deserves punishment according to their mental state at

[55] This line of thought goes along with the similar criminalization debate on terrorism kidnapping further developed on Chapter 4.2.4.
[56] FIGUEIREDO DIAS Jorge de, *Comentário Conimbricense do Código Penal - Tomo II*, Coimbra Editora, 1999. Page 1175 §5. Our translation.
[57] FIGUEIREDO DIAS Jorge de, *Direito Penal: Parte Geral, Tomo I: Questões Fundamentais A Doutrina Geral do Crime*. 3ªEd, Gestlegal, 2019. Page 360 §45. Our translation.
[58] HOGAN Brian and SMITH J C, *ob.cit.* Page 53.

the time of committing the crime, and if so, what type of punishment(s) the defendant deserves"[59].

The basic assumption of *mens rea* is that criminal liability should only exist when the defendant committed a crime that he/she intended, or even though it did not, it knew or should have known about the risk of doing so and still brought it about. The deconstruction of this general premise in legal terms differs between jurisdictions, but the main concepts in this regard are intention and negligence[60]. Depending on the type of crimes, a different type of *mens rea* is demanded.

The person is regarded as to have *intention* if the fulfillment of the *actus reus* appears to be the true purpose of the conduct[61], i.e., the person had the real intention of causing harm, affecting or putting in danger the legal good - there is a *direct intention*. Nonetheless, there are also cases where intention is "recognised when the realization of an act that fills a type of crime is represented as a possible consequence of the conduct, there is [intention] **if the agent acts in conformity with that realization**"[62] - existence of an *eventual intention*. For the common law doctrine, here the concept of intention translates into a *willful blindness*[63].

In the case of *negligence*, the victim, although not having intention, in both perspectives, acted without the due care that, in accordance with the specific characteristics of the case and their personal conditions, was supposed to have. It is thus necessary that the victim is imputed a certain duty of care and consequently that the unwanted unlawful result was predictable and avoidable for a prudent person[64] - the personal attitude of carelessness with the law and its norms is the manifestation of guilt required by the *mens rea*. Contrary to what happens in eventual intention or willful blindness, a negligent person does not conform to the possibility of causing harm or violating a legal good - either they act without even acknowledging such possibility or, if they do, they do not resign with that (they negligently belief that although possible, the harm will not happen).

---

[59] AL-SHAMARI Dr. Khalid Saleh, *The Emergence of Mens Rea in Common Law and Civil Law Systems*, in Kilaw Journal, Vol.7, Issue 1, Series N.º 25, 2019. Page 96.

[60] There are Authors and legal systems that make a distinction between the concepts of recklessness and negligence and how they are included in *mens rea*, but such analysis, although important, holds little relevance on the matter that we propose to study and therefore it is outside of the scope of this Paper. In this regard, see WILLIAMS Glanville, *Criminal Law: The General Part*, 2nd Ed., Steven & Sons Limited, 1961. Pages 100-103; HOGAN and SMITH, *ob.cit.* Page 69, AL-SHAMARI Dr. Khalid Saleh, *ob.cit.* Pages 111-115.

[61] FIGUEIREDO DIAS Jorge de, *Direito Penal: ob.cit.* Page 427 §35.

[62] FIGUEIREDO DIAS Jorge de, *Direito Penal: ob.cit.* Page 433 §44.

[63] On this topic see MARCUS Jonathan L., *Model Penal Code Section 2.02(7) and Willful Blindness* in The Yale Law Journal, Vol. 102, N,º 8, Symposium: Economic Competitiveness and the Law, 1993. Pages 2231-2257.

[64] FIGUEIREDO DIAS Jorge de, *Direito Penal: ob.cit.* Page 1007 §10.

In paying the ransom, there is no doubt that in the action of the victims we cannot see a direct intention - victims do not pay the ransom in order to finance criminal activity, but rather to regain access to their data or system. Therefore, such payment can only be criminalized on the basis of eventual negligence/wilful blindness or negligence - the victims in paying the ransom are either aware of the possibility of, even if indirectly, being financing criminal activity, resigning or not to that idea.

4.2.1.2.1. The problem of duress and necessity as a defense

Underlying all concepts of *mens rea* is the fact that in order to hold any person criminally liable is necessary that they are "sufficiently aware of what they are doing, and of the consequences it might have, [and] that they can fairly be said to have chosen the behavior and its consequences"[65] - this is moreover the ultimate expression of the Principle of Autonomy - they had a choice: to act legally or illegally (or to disregard the possibility of acting illegally) and they nevertheless chose the latter. In this sense, for these purposes, guilt is an ethical-legal censure directed at an individual for not having acted differently on the assumption that the agent is endowed with freedom, with the power to act otherwise[66].

There can be guilt without punishment, but never punishment without guilt.

Nonetheless, despite the law's assumption of individuals' freedom of choice, it is not naive - lawmakers do recognize that there are cases where such liberty does not exist or is limited and thus where it is not possible to exist guilt - the act is not fully voluntary. Either the lack of it is due to internal or external factors of the agent[67]. The former cases are directly related to the *agent's capability of being held criminally liable* and concerns his/her biological conditions to enable them to acknowledge the illegality of the act or the risk of it. - at the time of the occurrence of the facts, the agent must have been vested by all the necessary mental conditions for it to be possible to censure the agent for not having acted otherwise. Causes of legal incapacity are mainly minority[68] and mental disorders[69]. On the other hand, the latter case results

[65] ASHWORTH Andrew, *ob.cit.* Page 160.
[66] CORREIA Eduardo, *Direito Criminal*, Vol.1, Almedina, 2016. Page 316.
[67] These are overall a set of defenses that can be argued upon prosecution in order to exonerate the defendant.
[68] The relevant criminal age varies across jurisdictions.
[69] This assessment is always done on a case-by-case basis, meaning that such lack or limitation of freedom must be towards the specific act. For example, if a person has a biological tendency to steal things (kleptomaniac), his conditions shall only be relevant upon the practice of the crime of robbery because it is only regarding this type of crime that his freedom is restricted due to biological conditions. Such a condition becomes thus irrelevant if he undertakes, for example, a sex crime.

from the environment and concrete circumstances in which the crime was committed - cases of *defenses.* Outside facts, i.e., unrelated to biological characteristics of the agent itself, that takes away his/her freedom of decision or, even if he/she has some left, it would not be expected to act otherwise.

When a person's freedom of choice is restricted, two different arguments can be raised: *duress* and *necessity*. Both concepts "concerned with situations in which a person is faced with a choice between two unpleasant alternatives, one involving his committing a breach of the criminal law and the other some evil to himself or others"[70]. They differ on the cases in which they can be argued.

Duress is a legal concept that only exists in common law countries. The particular case of duress by threat generally exists when

> the actor engaged in the conduct charged to constitute an offense because he was coerced to do so by (...) a threat to use, unlawful force against his person or the person of another, that a person of reasonable firmness in his situation would have been unable to resist.[71]

Nonetheless, the common law doctrine and jurisprudence have only being admitting duress in cases of particular gravity, cases where the threat concerns the death or serious personal injury - "while the present [common] law appears to be that a threat of serious personal injury is the minimum which is acceptable to find a defense to *any* crime, a higher minimum may be required for crimes of great gravity"[72]. Along the same lines, we have the International Law that, under Article 31 (1) (d) of the Rome Statute of the International Criminal Court (ICC) restricts the invocation of duress to the more serious type of threats

> The conduct which is alleged to constitute a crime within the jurisdiction of the Court has been caused by duress resulting from a threat of imminent death or of continuing or imminent serious bodily harm against that person or another person, and the person acts necessarily and reasonably to avoid this threat, provided that the person does not intend to cause a greater harm than the one sought to be avoided. Such a threat may either be:
>
> (i) Made by other persons; or
>
> (ii) Constituted by other circumstances beyond that person's control.

According to HOGAN and SMITH, duress by threat has been accepted as a defense to manslaughter, criminal damage, arson, theft, handling, perjury, among others. The only crimes left out of the duress umbrella are forms of treason, murder and attempted murder[73].

---

[70] LAIRD Karl and ORMEROD David, *Smith, Hogan and Ormerod's Criminal Law*, 5th Ed., Oxford University Press, 2018. Page 367.
[71] Section 2.09 Model Penal Code.
[72] HOGAN Brian and SMITH J C, *ob.cit.* Page 237.
[73] HOGAN Brian and SMITH J C, *ob.cit.* Page 234.

On the other hand, there is *necessity* which is shared by common and civil law countries[74]. Alike duress, criminal law is infringed not due to a free action (or omission) of a person but rather to an external force that made the unlawful act the only viable and demandable choice. The difference is that necessity is not restricted to cases where only the death or serious bodily harm is at stake, but rather demands a proportionality test between the harm or legal good that is trying to be protected and the one that is affected - there is a choice of evils in which one of them must be justifiably greater than the other in order to supersede.

> Whoever, when faced with a present danger to **life, limb, liberty, honour, property or another legal interest** which cannot otherwise be averted, commits an act to avert the danger from themselves or another is not deemed to act unlawfully if, **upon weighing the conflicting interests, in particular the affected legal interests and the degree of the danger facing them, the protected interest substantially outweighs the one interfered with.** However, this only applies to the extent that the act committed is an adequate means to avert the danger[75] (emphasis added).

In a nutshell, for a defense by necessity to proceed, it must be proved that:

1. There is a present danger to life, limb, liberty, honor, property or another legal interest of any nature (not necessarily criminal);
2. The danger cannot be averted by any other means besides the unlawful act;
3. The legal interest that is aimed to be protected substantially outweighs the one being affected;
4. The unlawful act is an adequate means to protect the superseded legal interest; and
5. In jurisdictions such as Portugal, the danger was not voluntarily by the agent, except when protecting the interest of a third party[76].

Taking into consideration all the above mentioned, it is not hard to see its implications on the criminalization of a ransom ban in ransomware attacks. In the scenario where paying the ransom constitutes a crime, it must be ensured that no defense can be easily argued in order to exempt criminal liability under penalty of defeating the purpose of criminalization.

As we have seen, the defense of *duress* can only be argued if the victim is under threat of death or serious bodily harm, which is not the typical situation in ransomware attacks

[74] In civil law there is the distinction between necessity as a *justification* and as a *defense*. Essentially, necessity as a justification is only restricted to certain legal goods - life, physical integrity, honor and liberty and does not require a proportionality test, being only taken into consideration the particular circumstances of the case. Its field of application is therefore much narrower than the one of necessity as a defense that, in its turn, can be applied to any kind of "legal interest" (not necessarily a criminal legal interest).
[75] Section 34 StGB. Our translation.
[76] Article 34 (c) of the CPP.

(although cases are getting increasingly more serious). The same problem arises under International Law[77].

In the case of *necessity* as a defense, the scenario is much more complex. Although at first sight this defense may look much more arguable in cases of ransomware by the mere fact that its scope of application is not limited to the most serious situations of danger like duress - it is only required a present danger to a legal interest - many other tests that shall be carried out may compromise its invocation. First and foremost, the danger created by the ransomware cannot be adequately cautioned by any other means besides the payment of the ransom, i.e, the victims cannot have at their disposal, in a timely manner, any alternative that could effectively safeguard both interests or at least be less burdensome. Redirecting the case to law enforcement can be a possible alternative in many cases but not in all - the inevitable slowness of law enforcement in solving the problem can constitute a reasonable obstacle for victims that cannot suffer downtime, thus making the ransom payment the only adequate and effective means. On the other hand, as we will see further on, there are certain measures already implemented with the purpose of helping victims to be able to overcome the attack autonomously, like for example the "No More Ransom" website[78] but it is questionable whether they can indeed be considered as an adequate alternative, especially because for that such a tool would have to be of general knowledge. Secondly, the legal interest that is aimed to be protected shall substantially outweigh the one being affected. This will always have to be a case-by-case assessment by weighing up all the specific circumstances of the case: the sanctions' framework, the intensity of the harm to the legal good or, in cases where such harm as not yet been done, the degree of the risk and the typology of the legal goods are indicative criteria often proposed by the doctrine[79]. Thirdly, in certain jurisdictions, the situation of danger cannot have been voluntarily created by the victim. This requirement gains particular relevance in the case of ransomware since most of the attacks

[77] A possible hypothesis that we could not fail to mention is the **strict liability doctrine**, applied on "offenses for which a person may be convicted without proof of intention, knowledge, recklessness, or negligence" (SINGER Richard G., *The Resurgence of Mens Rea: III - The Rise and Fall of Strict Criminal Liability*, in Boston College Law Review, Vol.30:337, 1989. Page 337) and thus without the need to prove *mens rea*. Surely that in civil law countries this is more or less irrelevant since the principle of culpability does not allow for a purely objective criminal liability, but it seems that common law does open up an opportunity that may very much be appealing to many legislators to take advantage of. Even if a defense based on duress might be difficult to hold up, a criminalization on the basis of strict liability can withdraw such risk by not demanding any *mens rea* proof. For more on this topic, see MOORE Michael S., *The Strictness of Strict Liability*, in Crim Law and Philos, 12:513–529, 2018. Page 515, SCOTT JR. Austin W. and LaFAVE Wayne R., *Substantive Criminal Law: Criminal Practice Series*, Vol. 1, Sections 1.1 to 5.11, West Publishing Co., 1986. Page 341, among others.

[78] See Chapter 6.

[79] PINTO DE ALBUQUERQUE Paulo, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2nd Ed., Universidade Católica Portuguesa, 2010. Page 185 §10 and 11.

are successful due to the lack of adequate cyber security measures implemented by the victims. According to the majority of the Portuguese doctrine, the situation of danger had to be created premeditatedly so that, by taking advantage of it, the legal interests of the injured party can be sacrificed[80]. Therefore, "even if the danger has been intentionally caused by the agent, but without the said goal, [necessity] (...) cannot be denied"[81]. In this regard, while one may censure the victim's conduct for failing to implement adequate cybersecurity measures that could have effectively prevented the ransomware attack, this should not be a reason to take away his ability to invoke necessity as a defense, since, in principle, such a failure was not done with the

4.2.1.2.2. Brief Mention to the Crime of Criminal Association under Article 299.º of the Portuguese Criminal Code

Under n.º 1 of the article 299.º of the Portuguese Criminal Code "whoever promotes or founds a group, organization or association whose purpose or activity is directed to the commission of one or more crimes is punished with a prison sentence of one to five years"[82]. Additionally, the same penalty is applied to "(...) any person supporting them, namely by supplying arms, ammunition, instruments of crime, guards or premises for meetings, or any assistance in recruiting new members"[8384]. For the purposes of the law, it is considered as a criminal group, organization or association a team of at least three people acting in concert over a certain period of time[85].

In this sense, since the list is non-exhaustive, other means of support such as providing funds to these associations can be framed under this type of crime which, in its turn, would be the case of the ransom payment. Plus, "(...) it is sufficient that the support granted is **beneficial in the abstract for [the organization]**"[86], not being required that the funds end up actually being used to pursue further criminal activities.

[80] In this sense, FIGUEIREDO DIAS Jorge de, *Direito Penal: ob.cit*. Page 444, CORREIA EDUARDO, *Direito Criminal Volume II*, Almedina, 2000, Pages 86-87 and TAIPA DE CARVALHO Américo, *Direito Penal, Parte Geral, Volume II, Teoria Geral do Crime*, Publicações Universidade Católica, 2004, Pages 238-239.
[81] RODRIGO NUNES Duarte Alberto, *O estado de necessidade em Direito Civil* in JULGAR Online, 2017. Page 42. Our translation.
[82] Our translation.
[83] Article 299.º n.º 2 of CPP. Our translation.
[84] With a similar wording see Section 129 StGB.
[85] Article 299.º n.º 5 of CPP.
[86] PINTO DE ALBUQUERQUE Paulo, *ob.cit.* Page 1167 §29. Our translation.

Criminal liability for a person who pays the ransom under a ransomware attack can emerge from the crime of criminal association counting that the criminal group fulfills the requirements of the law (at least three members and with a consistent activity over time). An important obstacle however is that ransomware attacks take place through internet and technological means where anonymity is one of the biggest advantages for cybercriminals. This makes prosecution of this crime almost impossible due to the difficulty in determining and proving the identity of cybercriminals.

4.2.1.3.Corporations' criminal liability

Until now, we have talked about the legal requirements that lawmakers must see fulfilled in order to criminalize the ransom payment conduct. But for any conduct there must exist an author. Perhaps, at first sight, it would have made more sense to firstly address the issue of the conducts' author into question and then analyze the conduct itself, but, as we will see, there were certain concepts such as *mens rea* and strict liability that had to be enlightened first for a better understanding of this matter.

When the direct victim of a ransomware attack is an individual and thus it is this one, one its own behalf, that pays the ransom, the question of authorship and criminal imputability of the fact is plain and simple. The problem is that the majority of these attacks are not against those persons but rather against institutions and corporations - although the payment in itself has to be carried out by an individual, it is done on behalf of the company.

Corporations' liability has for long been consensual in fields of law such as civil or administrative law, but criminal law has always had difficulty in recognising it since corporations are mindless legal entities and thus incapable of having any sort of guilt, any *mens rea*. Plus, "punishments such as imprisonment or death (...) could have no application to an inert body."[87].

In common law, an important legislative instrument is the Model Penal Code (MPC) where a lot of countries get inspiration for their own laws. In a nutshell, Section 2.07 of the MPC recognizes criminal liability to a corporation when either (i) the crime is committed by an agent of the corporation acting in its behalf and within his/hers scope of functions[88] or it was authorized, requested, commanded, performed or recklessly tolerated by the board of directors or by a high managerial agent action on the corporations' behalf and on the exercise of their

[87] WELLS Celia, *Corporations and Criminal Responsibility*, in Oxford Monographs on Criminal Law and Justice, Clarendon Press Oxford, 1993. Pages 99-100.
[88] Section 2.07 (1) (a)

functions[89]; or (ii) a strict liability is imposed by the law[90]. Regarding civil law countries, corporations' liability is very much like the first set of cases of common law (point (i)), but, as expected and in accordance with the principle of culpability, there is no strict liability option[91]. Plus, in 1983 the Council of Europe issued the Recommendation N.º R(88)18[92] stating that "Enterprises should be able to be made liable for offences committed in the exercise of their activities, even where the offence is alien to the purposes of the enterprise"[93], namely by "applying criminal liability and sanctions (...), where the nature of the offence, the degree of fault on the part of the enterprise, the consequences for society and the need to prevent further offences so require."[94].

Nowadays, corporations' criminal liability is more or less commonly accepted across jurisdictions, although with some differences. In this sense, a corporation that is targeted by a ransomware attack can indeed be held criminally liable if an individual proceeds with paying the ransom on its behalf within his/hers functions or someone else through previous authorization or order by a representative of the corporation. Under common law systems, a strict liability may also be possible towards these legal entities. The punishments can go from paying a fine, dissolution, among others[95]. Such liability may not exempt an eventual liability of the individual itself that makes the payment.

4.3. Parallel with Terrorism Kidnapping regime[96]

The problematic of ransom payments has for decades been a very hot topic for Governments and a reason for a lot of thinking by the doctrine in the field of Terrorism kidnapping. Ransomware attacks, although a recent reality and product of the new digital era, share a lot of characteristics to more "traditional" crimes such as terrorism kidnapping when it comes to their *modus operandi* and legal questions.

The first step taken towards addressing the need to stop funding terrorism was through the International Convention for the Suppression of the Financing of Terrorism adopted by the United Nations in December 1999. The primary concern of this Convention was to stop

[89] Section 2.07 (1) (c)
[90] Section 2.07 (2)
[91] As an example, see Article 11.º of the CPP, Article 121-2 of the French Criminal Code, Section 30 of the German Act on Regulatory Offences.
[92] Available at https://rm.coe.int/.
[93] Appendix to Recommendation Point 1.
[94] Appendix to Recommendation Point 3 (a).
[95] See, for example, the ones proposed by the Council of Europe on the Recommendation R(88)18 Point 7.
[96] Very similar questions arise in Sea Piracy Kidnapping and thus the majority of literature approach these two crimes together when it comes to the problem of ransom payment.

financing terrorism, highlighting the urgent need for international cooperation among Countries in designing and implementing instruments to prevent the financing of terrorism[97] by the prosecution and punishment of its perpetuates[98]. In this sense, under it it would constitute an act of funding of terrorism any pursued by a "person by any means, directly or indirectly, **unlawfully and willfully** provides or collects funds with the **intention that they should be used or in the knowledge that they are to be used**"[99] for a terrorist act. However, by referring to an act *unlawful* and *willful*, according to BUNDY[100] the Convention did not aim to be applied to legitimate interests of humanitarian undertakings, "reflect[ing] the drafters' intent to preserve, among other humanitarian endeavors, the ability to negotiate for the freedom and safety of hostages", namely through the payment of demanded ransoms.

Moving closer to the particular issue of ransom payments, the United Nations Security Council has issued several Resolutions within the scope of terrorism. For example, the Resolution 1373, adopted under the aftermath of the 9/11 attack, decided to

> Criminalize the **willful provision or collection, by any means**, directly or indirectly, **of funds by their nationals** or in their territories with the intention that **the funds should be used, or in the knowledge that they are to be used,** in order to carry out terrorist acts[101] (emphasis added).

By omitting the unlawfulness requirement, it could be suggested that ransom payments could fall under the scope of this Resolution. Nevertheless, not only it did not expressly designate the payment of ransoms as a form of funding terrorism activity but also the Resolution restricted the criminalization to the provision of funds to terrorists with the *intention* or *knowledge* that they were to be used to pursue other terrorist acts. A link must therefore be established between the act of providing funds to a certain terrorist organization and the intention or knowledge of using those funds to finance further terrorist activity.

Giving a step further and finally intentionally addressing the payment of ransoms, on 2012 the Financial Action Task Force, an independent inter-governmental body established in 1989 by the G7 member states whose main purpose was to develop and promote policies of global financing system protection against money laundering, terrorist financing and financing

[97] KAZMIR Sima, *The Law, Policy, and Practice of Kidnapping for Ransom in a Terrorism Context* in International Law and Politics, Vol. 48:325. Page 326.
[98] Convention's Preamble § 13.
[99] Article 2.º of the Convention. Emphasis added.
[100] BUNDY C. Elizabeth, *ob.cit*. Page 721.
[101] United Nations Security Council Resolution 1373 (2001) Point 1 (b).

of proliferation of weapons of mass destruction[102], issued a set of Recommendations among which "[c]ountries (...) should criminalize not only the financing of terrorist acts but also the financing of terrorist organizations and individual terrorists **even in the absence of a link to a specific terrorist act or acts**."[103] (emphasis added). In this way, the necessity for the link is withdrawn.

Nevertheless, it was not until 2015 that an initiative took place expressly devoted to the problematic of ransom payments where the Security Council in its Resolution 2133 called upon all Member States to "prevent terrorists from benefiting directly or indirectly from ransom payments or from political concessions and to secure the sage release of hostages"[104] and to "encourage private sector partners to adopt or to follow relevant guidelines and good practices for preventing and responding to terrorist kidnapping without paying ransoms"[105]. From this Resolution on, others were enacted mentioning the payment of ransom and reinforcing its discouragement[106].

Currently, there are countries, such as the United States, United Kingdom and Australia that have made public their no-concession policy of not paying ransoms to terrorists and thus willing to sacrifice lives in a short term in order to achieve the long-term goal of deterring future criminal activity. Nonetheless, at present, no country criminalizes such payment by their nationals, natural and legal persons[107].

A terrorism kidnapping criminalization faces, in our opinion, two general problems. On the one hand, the moral dilemma that no one wants to get confronted with. As much beneficial as a ransom ban would have been in the long term for society, terrorists are holding hostage someone's son, brother or father. How can any prosecutor censure a father that was willing to pay anything for his son's freedom? Plus, one of the goals of criminal law is to deter individuals from committing crimes because they would rather not be punished". As DUTTON[108] points out "[o]ne can imagine that the threat of imprisonment would not deter a great number of parents from paying a ransom if doing so meant that their child might not be murdered by terrorists". When it comes to ransomware attacks, it is true that their seriousness is increasingly

[102] FATF (2012-2018), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2023. Page 2. Available at https://www.fatf-gafi.org/. Accessed on 22/02/2023.
[103] Recommendation 5.
[104] Resolution 2133 Point 3.
[105] Resolution 2133 Point 10.
[106] See United Nations Security Council Resolutions 2160, 2161 and 2199.
[107] DUTTON Yvonne M. and BELLISH Jon, *Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban* in Cornell International Law Journal, Vol. 47, Issue 2, Article 2, 2014. Pages 311-312.
[108] DUTTON Yvonne M., *Funding Terrorism: The Problem of Ransom Payments* in Funding Terrorism San Diego Law Review, Vol. 53: 335, 2016. Page 361.

coming close to the one of terrorism since, has we have seen before, cybercriminals are focusing on victims that run critical social services since those are the ones with less predisposition to hold down time[109]. The right to life and freedom may also be at stake if hospital energy services are compromised, for example. Nevertheless, that is not always the case - a substantial part of ransomware victims are companies who highly value their data, not because they may compromise human life, but for commercial reasons and here the moral dilemma does not hold the same meaning. In a nutshell, the conflict of values and interests in terrorism kidnapping is always the same - funding terrorism *vs* human life and freedom - whereas in ransomware attacks it is not which, in its turn, softens the dilemma. On the other hand, as we have seen in chapter 4.2.1.2.1., the defense of duress can be argued in cases where the victim is under threat of death or serious bodily harm which, although with little impact on ransomware attacks (at least for the time being), can be greatly used in terrorism kidnapping[110].

5. Brief Overlook to the Insurance Company's Role

The exponential growth of cyberattacks has an impact not only on the companies that are considered the victims, but also on other institutions that are somewhat related to them. One particularly important case is Insurance Companies that during the second half of 2021 experienced an increase of 23% in ransomware claims[111].

Despite the undoubted popularity of Insurance Companies nowadays regarding cyber protection, questions have arisen concerning their role in fighting cyber criminality, particularly ransomware attacks. On the one hand, these institutions believe that the underwriting process demands qualified due diligence on the insured companies, since they must fulfill a set of security measures in order to mitigate the risk and effects of cyberattacks. In this way, awareness is spread, and the daily practice of cyber hygiene is rooted in the insured companies[112]. Nevertheless, on the other hand, not only the existence of cyber coverage gives a sense of security to the insured companies, but it also gives it to the attackers. In other words, even when a company, at first sight, does not seem particularly appealing to cybercriminals due to its lack of financial capacity to pay an interesting amount of ransom, the fact that they have cyber insurance that will cover any damage or cost with an eventual cyberattack, changes the

[109] See Chapter 4.1. §3.
[110] See DUTTON Yvonne M. and BELLISH Jon, *ob.cit*. Page 319, KAZMIR Sima, *ob.cit*. Pages 350-353, DUTTON Yvonne M., ob.cit., Page 362, BUNDY C. Elizabeth, *ob.cit.* Page 772.
[111] Coalition 2022 Cyber Claims Report, Page 9.
[112] Cyber Insurance Blog, *The Surprising Reasons Cyber Insurance Can Stop Ransomware Attacks*, ProWriters. Available at https://prowritersins.com/cyber-insurance-blog/should-companies-pay-ransomware-demands/ Accessed on 15/03/2023.

scenario. In fact, among the files that a cybercriminal can have access to in order to pursue his ransomware attack are insurance policies and contracts. In this way, criminals can have a prior outlook of what are the types of attacks covered by the insurance, the particular specifications and, more importantly, the value of the coverage limits.

In a nutshell, even though good cyber insurance coverage can give a sense of strength and protection to companies that are more exposed to cyberattacks, that same feeling is spread to cybercriminals. As a result, the companies' vulnerability increases, and the odds of a successful ransom demand are higher. Due to that, some believe that the prohibition of paying the ransom of ransomware attacks should be shifted to the prohibition of the coverage by insurance companies of those exact attacks. Accordingly, to Russell Haworth, CEO of Nominet[113], "changing the law so that firms can't claim ransomware payments on insurance would be a smart move to shift how businesses respond to attacks". Sharing the same opinion, Ciaran Martin, founding chief executive of the UK's National Cyber Security Center, stated that "you have to look seriously about changing the law on insurance and banning these payments, or at the very least, having a major consultation with the industry"[114].

The problem is that it is unclear to what extent that prohibition will effectively withdraw companies from paying ransoms, and not simply amplify the damages that they will incur with a ransomware attack, making it, in the end, hard for them to get back on their feet after an attack. Consequently, companies will be then more leaning towards the payment since the cost of not doing so may be unbearable. It is a vicious cycle that seems not to have a clear-cut solution.

6. Recommendations and alternatives to criminalization. Analysis of initiatives already implemented

Reaching towards the end of our discussion it is safe to say that a criminal ban of ransom payments entails multiple issues and questions that require time to address and debate on. Nevertheless, even if it is reached the conclusion that the conditions are met to create a new type of crime, the transition must be smooth and thoughtful. The Ransomware Task Force[115] identified three factors that Governments should consider in order to mitigate the potential negative impacts of such criminalization. The first step is the *timeline* - Governments and other institutions involved need time to adapt to such a drastic change in the law. Careful victim

[113] UK Company manager of the uk. Domain name.
[114] SABBAGH Dan, *Insurers 'funding organised crime' by paying ransomware claims*, The Guardian, 24/01/2021. Available at https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims. Accessed on 4/03/2023.
[115] Ransomware Task Force, *ob.cit.* Page 50.

protection and support programs need to be put into place and, for example, insurance policies need to be updated by Insurance Companies. Additionally, "a prohibition statute should establish milestones or conditions that would need to be met before the prohibition would go into effect". Secondly is *phasing*: the prohibition should be implemented by phases, where an order should be followed. Last but not least is the *victim's protection and support*. This has been an aspect that profoundly concerns the doctrine and cyber professionals as it is the most essential piece without which the new law's enactment is set to failure. As we have the opportunity to mention, one of the biggest reasons companies insist on paying the ransom is because they cannot afford downtime. The costs that they would have to suffer by not respecting the cybercriminals' demand would be much higher than the amount of ransom. If lawmakers want to prohibit companies from paying the ransom, they must create a set of mechanisms and tools to be at the company's disposal in order to help them come out of the ashes and put themselves together.

More conservative approaches to criminalization have been developed. One of the alternatives is the *obligation of a ransom payment report*. In 2021, a bill was proposed to the Senate of the United States in this regard, according to which[116]

> An entity, including a covered entity and except for an individual, a small organization, or a religious institution, that makes a ransom payment as the result of a ransomware attack against the entity **shall report the payment to the Director not later than 24 hours after the ransom payment has been made**. (emphasis added)

In fact, this initiative of report has already been implemented in Australia where companies must report to the Australian Cyber Security Centre that they were the target of a ransomware attack and that they intend to pay the demanded ransom. This mandatory reporting scheme has the goal not to prevent victims from paying the ransom but rather to allow law enforcement to know about the attack, the intention of paying, and the payment method. This last aspect gains special relevance when it consists of payment with cryptocurrency because, in that way, "if [victims] move quickly enough, there's the possibility law enforcement could take action against cryptocurrency exchanges before the money is pulled out of them", says Tim Watts, Shadow Assistant Minister for Communications and Cyber Security at the Australian Parliament[117]. However, an important aspect must be highlighted in this regard: by demanding a report from targeted companies, law enforcement and Governments must protect the

[116] S.2407 - Cyber Incident Notification Act of 2021, Section 2232 (a) (2).
[117] SADLER Denham, *Govs considers new crypto and ransomware laws*, InnovationAus, 26/05/2021. Available at https://www.innovationaus.com/govt-considers-new-crypto-and-ransomware-laws. Accessed on 10/03/2023.

companies' confidentiality, ensuring that their report is not disclosed to the general public. This is extremely relevant because especially big tech companies see their reputation as greatly based on the trust of the consumer that their data is protected, and no privacy infringements may occur. Well, if the occurrence of a ransomware attack on a certain company is licked, the consumer's trust may be irretrievably damaged or even lost. In this sense, an obligation of reporting the attacks aspires to thrive, especially among big tech companies and be complied with, confidentiality may be necessary to guarantee.

On another note, a measure that is already implemented is *civil liability* for whoever, directly or indirectly, engages, namely by providing funds, with entities or individuals on OFAC's Specially Designated Nationals and Blocked Persons List[118]. This is a strict liability "meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC"[119]. Among the blocked persons, there are numerous cyber actors known for carrying on ransomware attacks. Recently, the U.S Department of the Treasury issued an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[120], clarifying that not only are subject to this liability the victims of ransomware attacks (since they pay them the demanded ransom), but also any financial institutions and money services businesses that facilitate the ransom payment on their behalf. This liability consists of pecuniary sanctions and can be mitigated namely by the victims' and financial institutions' implementation of a risk-based compliance program and by their promptness of voluntarily reporting to law enforcement the attacks' details (e.g., ransom payment demand, payment instructions, etc.)[121].

Finally, some countries and tech companies have implemented more *cooperative measures*. Talion created the #RansomAware movement, whose main purpose is to provide companies with a cybersecurity community where they feel able to talk about the attacks, share their experience and inform others, all anonymously. According to the pioneers of this movement, "we believe that the more companies who expose how they were attacked, by whom, if they paid the ransom and if their data was recovered, the more we can learn about attacker tactics, techniques, and procedures to build better defenses: Forewarned is

[118] Available at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.
[119] Page 4.
[120] September 21, 2021. Available at https://home.treasury.gov/
[121] Pages 4 and 5.

Forearmed"[122]. On the other hand, the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Center, Kaspersky and McAfee have come together on the creation of the "No More Ransom" website (https://www.nomoreransom.org/) where companies can find help in decrypting their data without having to pay the criminals[123].

7. Conclusion

Ransomware attacks are the 21st century gold mine that is no longer restricted to highly technological skilled criminals becoming rather accessible to pretty much anyone who has the financial capacity to acquire the malware. It goes beyond States' borders and can weaken the most sophisticated computer system. At the same time, the damages are getting increasingly more serious which moves these types of crimes closer to international top priority crimes such as terrorism kidnapping.

The key challenge is to know how to draw back the long-term public interest (of not funding criminal activities) and the short-term private interest of victims (get the data back and restore the business activity) into a better alignment. Ideally, victims would not be found in this dilemma because alternative mechanisms are at their disposal to get their data back, such as law enforcement and other cyber security institutions. Nevertheless, we cannot be naive. If there is one thing for sure, cybercriminals work 24/7 in their technical skills, software, and equipment development, making it very hard for institutions to keep up with such an evolutionary rhythm.

The hypothesis of criminalizing the ransom payment faces important challenges that may slow down its process of implementation or even prevent it. As we have seen, the respect for the principle of criminalization *in ultima ratio* burdens lawmakers to exhaust every single legislative alternative before claiming criminal law protection. On the other hand, attending the elements of a crime, even if both *actus reus* and *mens rea* could be considered to be fulfilled (even if this latter requirement is withdrawn by common law's strict liability approach), a criminalization would be ineffective if duress or necessity could be easily argued by ransomware victims. While the defense of duress of common law countries as perhaps a more remote but nonetheless possible impact, - since ransomware attacks since is not far-fetched to see a ransomware attack causing serious personal injury or even death to individuals, - the necessity defense of civil law countries must be a useful defense tool to ransom payers if the legal requirements are shown to the Court to be met.

[122] Available in https://talion.net/ransomaware/.
[123] Available in https://www.nomoreransom.org/en/about-the-project.html.

At the same time, the particular case of ransomware with double extortion may never be extinct, even with criminalization. In fact, banning the ransom payment will only make it more appealing to cyber criminals since it is a two-way street: either they resort to it in order to put more pressure on victims in paying the ransom or, if unsuccessful in doing so, they can still get some funding by selling the data on the parallel market (in cases where such is possible).

Terrorism kidnapping legislation has already made significant progress on regulating ransom payments but has not yet reached a direct prohibition. Among other contingencies, at the end of the day, Governments do not want to be responsible for prioritizing the long-term goals of ending with terrorism over the immediate violation of fundamental human rights. Neither they are ethically capable of demanding such to their nationals. Here is where ransomware and terrorism kidnapping move apart: terrorism kidnapping is constantly more frightening to human rights than ransomware, which demands a much more careful approach from Governments than in the latter. The ethical dilemma is much more intense and a more conservative position towards ransom criminalization is more understandable to exist when rights such as right to live and freedom are at stake rather than rights to personal data or to property. In this sense, the fact that a ransom ban has not yet found its way in terrorism kidnapping does not compromise the success of a similar initiative in ransomware.

On the other hand, in our opinion, the ransom payment can, in jurisdictions such as Portugal, be already criminally punished under the crime of criminal association, although in a very limited way – it is excluded in cases where cybercriminals are "lonely wolfs", for example, and is of very difficult prove due to the very predominant anonymity with which ransomware attacks are often undertaken.

Finally, being a criminalization perhaps a premature step taking into consideration all the above said, it is important to highlight two aspect that Governments should be particularly concerned about: (a) adopting a set of transactional measures in order to create an environment where companies feel safe declining to pay the ransom, either because they trust on law enforcement in getting their data back or that, at least, financial support is guaranteed in order to help them to get back on their feet; and (b) do not neglect their educational duty by spreading awareness among potential victims for the importance of adequate cyber hygiene and that backing up the data is no longer bulletproof. Strict security measures should be common practice from the smallest to the biggest companies.

8. Bibliography

8.1. Books

ASHWORTH Andrew, *Principles of Criminal Law* in Clarendon Law Series, Third Ed., Clarendon Press Oxford, 1999.

ASHWORTH Andrew and HORDER Jeremy, *Principles of Criminal Law*, Seventh Ed, Oxford University Press, 2013.

CORREIA Eduardo, *Direito Criminal*, Vol.1, Almedina, 2016.

CORREIA EDUARDO, *Direito Criminal Volume II*, Almedina, 2000.

FIGUEIREDO DIAS Jorge de, *Comentário Conimbricense do Código Penal - Tomo II*, Coimbra Editora, 1999.

FIGUEIREDO DIAS Jorge de, *Direito Penal: Parte Geral, Tomo I: Questões Fundamentais A Doutrina Geral do Crime*. 3ªEd, Gestlegal, 2019.

HOGAN Brian and SMITH J C, *Criminal Law*, Seventh Ed., Butterworths, 1992.

JENDLY M. and VAN KEMPEN P.H.P.H.M.C., *Overuse in the criminal justice system ; Le recours excessif au système de justice pénale : on criminalization, prosecution and imprisonment : aux sanctions et poursuites pénales et à la détention* in International Penal and Penitentiary Foundation n.º 47, intersentia, 2019.

LAIRD Karl and ORMEROD David, *Smith, Hogan and Ormerod's Criminal Law*, 5th Ed., Oxford University Press, 2018.

PINTO DE ALBUQUERQUE Paulo, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2nd Ed., Universidade Católica Portuguesa, 2010.

SCOTT JR. Austin W. and LaFAVE Wayne R., *Substantive Criminal Law: Criminal Practice Series*, Vol. 1, Sections 1.1 to 5.11, West Publishing Co., 1986.

TAIPA DE CARVALHO Américo, *Direito Penal, Parte Geral, Volume II, Teoria Geral do Crime*, Publicações Universidade Católica, 2004.

WELLS Celia, *Corporations and Criminal Responsibility*, in Oxford Monographs on Criminal Law and Justice, Clarendon Press Oxford, 1993.

WILLIAMS Glanville, *Criminal Law: The General Part*, 2nd Ed., Steven & Sons Limited, 1961.

8.2. Articles

10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders of April 2000. Available at https://digitallibrary.un.org/record/404748.

2021 Europol's Annual Internet Organized Crime Threat Assessment. Available at https://www.europol.europa.eu/.

2022 ENISA Threat landscape for Ransomware Attacks. Available at https://www.enisa.europa.eu/.

AL-SHAMARI Dr. Khalid Saleh, *The Emergence of Mens Rea in Common Law and Civil Law Systems*, in Kilaw Journal, Vol.7, Issue 1, Series N.º 25, 2019.

BORRION Hervé and CONNOLLY Alena Yuryna, *Your Money or Your Business: Decision-Making Processes in Ransomware Attacks*, in Forty-First International Conference on Information Systems, India 2020.

BORRION Hervé and CONNOLLY Alena Yuryna, *Reducing Ransomeware Crime: Analysis of Victims' Payment Decisions*, at Computers & Security 119, Elsevier, 2022.

BUNDY C. Elizabeth, *Rescuing Policy and Terror Victims: A Concerted Approach to the Ransom Dilemma* in Michigan Journal of International Law, Vol. 37, Issue 4, 2016.

CABLE Jack, OOSTHOEK Kris and SMARAGDAKIS Georgios, *A Tale of Two Markets: Investigating the Ransomware Payments Economy*, 2022.

Coalition 2022 Cyber Claims Report. Available at https://info.coalitioninc.com/.

DUTTON Yvonne M. and BELLISH Jon, *Refusing to Negotiate: Analyzing the Legality and Practicality of a Piracy Ransom Ban* in Cornell International Law Journal, Vol. 47, Issue 2, Article 2, 2014.

DUTTON Yvonne M., *Funding Terrorism: The Problem of Ransom Payments* in Funding Terrorism San Diego Law Review, Vol. 53: 335, 2016.

ENISA Threat Landscape 2021. Available at https://www.enisa.europa.eu/.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*, Brussels, 20.9.2011 COM(2011) 573 final.

FATF (2012-2018), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2023. Page 2. Available at https://www.fatf-gafi.org/.

KAZMIR Sima, *The Law, Policy, and Practice of Kidnapping for Ransom in a Terrorism Context* in International Law and Politics, Vol. 48:325.

LI Chen, LIAO Qi, *Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling ransomware*, in ARES 2020, August 25–28, Virtual Event, Ireland 2020.

MARCUS Jonathan L., *Model Penal Code Section 2.02(7) and Willful Blindness* in The Yale Law Journal, Vol. 102, N,º 8, Symposium: Economic Competitiveness and the Law, 1993.

MOORE Michael S., *The Strictness of Strict Liability*, in Crim Law and Philos, 12:513–529, 2018.

Ransomware Task Force, *Combating Ransomeware - A comprehensive Framework for Action: Key Recommendations from the Ransomeware Task Force*, IST, April 2021.

RODRIGO NUNES Duarte Alberto, *O estado de necessidade em Direito Civil* in JULGAR Online, 2017.

SINGER Richard G., *The Resurgence of Mens Rea: III - The Rise and Fall of Strict Criminal Liability*, in Boston College Law Review, Vol.30:337, 1989.

SOPHOS, *The State of Ransomware 2022 Report*. Available at https://www.sophos.com/.

8.3. Websites

AP News, *German hospital hacked, patient taken to another city dies*, AP news, 17/09/2020. Available at https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.

CBS, *Extorted by ransomware gangs? The payments may be tax-deductible*, CBS News, 21/06/2021. Available at https://www.cbsnews.com/news/ransomware-payments-may-be-tax-deductible/.

Common Scams and Crimes, Scams and Safety, Official Website of FBI. Available in https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

Cyber Insurance Blog, *The Surprising Reasons Cyber Insurance Can Stop Ransomware Attacks*, ProWriters. Available at https://prowritersins.com/cyber-insurance-blog/should-companies-pay-ransomware-demands/.

MCKEITH Sam, *Australia to consider banning paying of ransoms to cyber criminals*, Reuters, 14/11/2022. Available at https://www.reuters.com/technology/australia-consider-banning-paying-ransoms-cyber-criminals-2022-11-12/.

MORGAN Steve, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025'*, Cybercrime Magazine, Nov. 13, 2020. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

PAINTER RANDALL Karen, MCNELIS III Joseph, *Two States Now Prohibit Public Entities from Paying Ransoms* in Connell Foley: Legal Blogs and Updates, 18/08/2022. Available at https://www.connellfoley.com/blog/Two-States-Prohibit-Public-Entities-Paying-Ransoms.

SABBAGH Dan, *Insurers 'funding organised crime' by paying ransomware claims*, The Guardian, 24/01/2021. Available at https://www.theguardian.com/technology/2021/jan/24/insurers-funding-organised-by-paying-ransomware-claims.

TIDY Joe, *Ransomeware: Should paying hacker ransoms be illegal?*, BBC News, 20/05/2021. Available at https://www.bbc.com/news/technology-57173096

https://talion.net.

https://edition.cnn.com/2021/07/27/politics/senate-judiciary-ransomware-hearing/index.html

https://rm.coe.int/

https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

https://home.treasury.gov/

https://talion.net/ransomaware/

https://www.nomoreransom.org/en/about-the-project.html