Boss, Our Data Is in Russia – a Case-Based Study of Employee Criminal Liability for Cyber-Attacks

Renaud Zbinden, Luca Brunoni and Olivier Beaudet-Labrecque
Insitut de lutte contre la criminalité économique, HEG Arc, HES-SO // Haute école de Suisse occidentale

This paper was presented at Botconf 2023, Strasbourg, 11-14 April 2023, www.botconf.eu
It is published in the Journal on Cybercrime & Digital Investigations by CECyF, https://journal.cecyf.fr/ojs

Abstract

The following position paper discusses the topic of employee criminal liability in the context of ransomware attacks. Through a series of case studies, it analyses whether, under Swiss law, employees who have facilitated the success of an attack can be qualified as co-authors or accomplices.

After an overview of the applicable legal framework, this paper analyses three case studies inspired by actual ransomware attacks. It focuses in particular on the element of intent, which is a prerequisite in most cybercrime laws, and which can, under certain conditions, also be applied to behaviors that appear to be the result of "mistakes"; it also discusses the role that in-house cybersecurity training (or the lack thereof) can have in this context.

Drawing from the results of the analyzed cases, this paper then presents a series of recommendations aimed at reinforcing cybercrime prevention within institutions, while also touching upon topics such as cyber-insurances and certification labels.

Keywords: Ransomware, Cyber-attack, Criminal liability, Employee liability, switzerland, Criminal law, Cybersecurity.

1 Introduction

In recent years, ransomware attacks have become more and more frequent [1]. In Switzerland, numerous cases have been reported in the media, such as those involving administrative and academic institutions, medical practices, and other public and private organizations. Following a cyber incident caused by ransomware, the affected organization faces numerous disadvantages regarding its image, data, finances, sustainability, and recovery. In some cases, the attacked organization pays quickly, or after some negotiations, the price demanded, in order to regain access to its data and resume its activities.

Often, the perpetrators reside in foreign states and are difficult to identify and therefore can escape prosecution. However, people within the targeted organization who played a voluntary or involuntary role in the success of the attack can also fall under the scope of criminal rules. In the latest cases reported in Switzerland, the vast majority of computer breaches were the result of employees' voluntary or involuntary actions. Simple inattention or an insignificant action can cause an infection of the organization's whole computer system. As a result, many organizations are implementing training courses and awareness campaigns to help their employees mitigate cyber risks and avoid attacks.

In order to better understand the issues of employee criminal liability in the context of a ransomware attack, as well as to support organizations in their prevention efforts, the Institut de lutte contre la criminalité économique (ILCE) / The Institute for Combatting Economic Crime conducted an exploratory study which is based on the analysis of concrete cases. The objective of this article is to present the first results of these analyses.

Below, an analysis of the criminal legal framework will highlight the provisions applicable in Switzerland during a cyber ransomware attack. Then, three scenarios which are based on true facts will be presented and analyzed from the point of view of Swiss criminal law. These analyses will clarify several aspects related to the criminal liability of employees and provide recommendations to limit the risks of their participating in a successful ransomware attack.

2 The Legal Framework

The Budapest Convention on Cybercrime (CCC) [2], implemented by the Council of Europe on November 23, 2001, was the first international convention designed to combat cyberspace crime. It was ratified by 68 countries, including Switzerland, France, the United States and Turkey. The main objective of this pact is to establish a common criminal policy, in order to protect society from cybercrime by harmonizing national legislation and facilitating international cooperation [3] [4]. The CCC deems these offenses applicable to ransomware attacks are actions such as: breaking into a protected computer system (art. 2 and 3 CCC), illegal interception of data or systems (art. 4 and 5 CCC) and computer fraud (art. 8 CCC) [5] [6].

Since January 1, 1995, Swiss law has already included several offenses specific to cybercrime. The criminal provisions which apply to ransomware cases are mainly listed in the Swiss Criminal Code (SCC) and in the Federal Act on Data Protection (FADP). A series of legislative amendments have adapted these provisions to the CCC requirements, as well as to the constant change in criminals' modus operandi [7]. In this paper, particular attention will be paid to the following provisions: unauthorized obtaining of data (art. 143 SCC); obtaining personal data without authorization (art. 179novies SCC); unauthorized access to a data processing system (art. 143bis SCC); damage to data (art. 144bis SCC); extortion (art. 156 SCC). Indeed, these offenses will be detailed in the analysis of the cases below.

It is also worth noting that currently, in Switzerland, there is no legal obligation for an organization to publicly communicate that it has suffered a cyber-attack [8]. Nevertheless, organizations under the supervision of the Swiss Financial Market Supervisory Authority (FINMA) have a legal obligation to report a cyber-attack according to art. 29 al. 2 of the Swiss Financial Market Supervisory Authority Act (FINMASA; SR 956.1) [9] and soon, operators of critical Swiss infrastructures will also be obliged to report cyber-attacks according to the amendment of the Information Security Act [10].

3 Case Studies

This study includes three ransomware attack scenarios based on true l facts [11], for which only the scenario has been adapted and completed with available information. Each situation involves a different organization with IT security issues which have specifically been tailored to their business. The organizations' cyber risk awareness level, as well as their security measures, all vary and range from high to low.

In each scenario, a company employee performed actions which influenced the success of the attack. These acts will be analyzed to determine if one or more criminal provisions are applicable. This analysis will focus on the objective (punishable behavior) and subjective (degree of intent) aspects of each selected offense. It will also be a question of determining the degree of employee participation in the highlighted offense, therefore particularly distinguishing between the degree of co-perpetrator and accomplice. However, possible justifying facts such as: self-defense, lawful necessity, or consent will then be taken into account to determine the unlawfulness of the conduct.

3.1 Cyber-Attack on a Hospital

The first case concerns a Lorobot cyber-attack on a hospital, this ransomware encrypts popular file extensions [12]. The infection was spread through a phishing email sent to an employee. It is based on a real cyber-attack which took place in 2019 [11].

3.1.1 FACTS

A hospital employs 170 staff. The number of patients exceeds the planned intake which forces the employees to work harder. The hospital handles confidential patient data; therefore a private company is contracted to back up the servers weekly. Management was aware of the cyber risks however, had not taken the time to educate its employees. Although, a draft IT charter was being drawn up.

One day, Albert, an accounting department employee, received an email containing an Excel file from an unknown sender. Without paying any attention, he downloaded the file and opened it on his computer. Instantly, all the hospital's data was encrypted by the Lorobot ransomware, as well as the backup files which were also saved on the company's server. A high ransom in Bitcoins was demanded by the cybercriminals in exchange for the decryption key.

3.1.2 ANALYSIS

By his behavior, Albert causes his organization's data breach which is followed by financial blackmail. Therefore, the criminal provisions of damage to data (art. 144bis ch. 1 SCC) and extortion (art. 156 SCC) are also potentially applicable.

The objective elements of art. 144bis al. 1 SCC are fulfilled, because the object of the crime is the organization's computer data and Albert's behavior is considered as an act of damage, in other words, the disabling and blocking of computer data caused by the encryption of the Lorobot ransomware.

The subjective element of art. 144bis ch. 1 SCC requires that the offense be intentional. In this scenario and with the known information, it is difficult to assert that Albert acted with awareness and intent (art. 12 al. 2 SCC) since he was not sufficiently aware of the risks and consequences of opening the attachments on his computer [13]. In contrast, Swiss criminal law stipulates that the subjective element is also fulfilled if the perpetrator acts out of dol éventuel. Dol éventuel "implies that the perpetrator is indifferent to the realization of the crime, so that he or she must inwardly approve or consent to it. The perpetrator contemplates the harmful result and accommodates this, or even accepts it as such." [14] In this scenario, Albert was never aware of the cyber risks and no technical or organizational measures were put in place, therefore it may be difficult for Albert to consider the consequences of his act. If we consider Albert as a perpetrator, he does not realize the subjective element [15], therefore the applicability of the data damage provision should be excluded. Therefore, it has to be considered whether Albert can be prosecuted as an accessory to the crime, assuming that the cybercriminal who initiated the attack is the perpetrator (he/she fully meets the elements of the crime).

For Albert to be prosecuted as an accomplice (art. 25 SCC), it is necessary that he makes a causal contribution to the realization of the offense [16]. This contribution can be physical or psychological [17]. In this scenario, Albert's contribution is physical, since he downloads and opens an infected file on his computer. Then, to be incriminated as an accomplice, he must have the intention of facilitating the offense, however the dol éventuel is sufficient. More concretely, "he must both know or be aware that he is assisting in a given criminal act and want to or accept it" [18]. As we have seen above, it seems difficult to establish such acceptance, especially since Albert was never made aware of the cyber risks, therefore his responsibility as an accomplice should also be excluded.

Regarding extortion (art. 156 SCC), the first objective element to be realized is that Albert must use a means of coercion, which means violence or the threat of serious harm to the organization. In this scenario, Albert does not use violence against his organization and does not threaten the organization with serious harm; since the encryption of the data has already been achieved, it is no longer a threat. Therefore, extortion is to be excluded, both for principal and accessory participation, since the offense has not been committed.

To conclude, this first scenario, in the light of the provisions analyzed, Albert does not seem to risk any criminal consequences as a perpetrator or accomplice, for infecting his organization with ransomware.

3.2 Cyber-Attack on an Academic Institution

The second scenario is based on a cyber-attack which affected an academic institution in 2021. The computer system was infected with ransomware, which was caused by an employee downloading free software.

3.2.1 FACTS

An academic institution has just over 1800 students and approximately 350 employees. The students' personal data, as well as the data of applied research are stored on the server under the supervision of an IT department. The data contained on this server includes confidential and sensitive data. An IT charter must be signed by all students and employees before they are enrolled or recruited. In addition, all employees are trained on cyber risks as soon as they start their job and two mock infection tests are carried out per year, in order to improve awareness and adapt training methods.

One day, Bertrand, an employee of the institution, needed to use software "X" for his work. He looked in the software center provided by the IT department, but the software was unavailable. Therefore, he decided to download it from the Internet and found that normally it is payable. After several searches, he found the cost-free software on another site. Being very satisfied, Bertrand downloaded it and installed it on his workstation. Several days passed and one morning, Bertrand noticed that the files on his computer were encrypted and that he could only access one text file; the latter informed him that the computer system was infected by the Locky ransomware, this malware encrypts files, making them inaccessible and unusable. The message stated that the data had been copied and would be published on the Dark web if the organization does not pay a ransom in Bitcoins. Bertrand hurriedly contacted the IT department. However, the head office refused to pay the ransom and shut down the organization's servers in order to assess the damage caused by the cyber-attack. At first sight, several computers were infected. Further analysis had to be carried out before the computer system could be put back into operation, which meant that the employees could not work for an indefinite period of time.

3.2.2 ANALYSIS

Through his actions, Bertrand damages the organization's data and allows it to be stolen. In a second step, the organization is being blackmailed and suffers immediate financial damage by forbidding its employees to work on the computer server. The criminal provisions to be considered in relation to Bertrand's behavior are unauthorized obtaining of data (art. 143 SCC), obtaining personal data without authorization (art. 179novies SCC), damage to data (art. 144bis al. 1 SCC), as well as extortion (art. 156 SCC).

Art. 143 SCC and art. 179novies SCC are composed of the same punishable conduct, with the only difference being that in the latter scenario, the stolen data is personal and sensitive. In this situation, Bertrand does not gain control of the data, but allows the cybercriminal to steal it. Thus, as Bertrand does not commit the theft, he does not qualify as a co-perpetrator within the meaning of art. 143 SCC and art. 179novies SCC. However, since the cybercriminal fully realizes the punishable conduct and his intention is clearly identified, it must be examined whether Bertrand can be prosecuted as an accomplice. Bertrand contributed to the offenses of art. 143 SCC and 179novies SCC by downloading and installing infected software on his/her workstation. Therefore, it is necessary to analyze whether Bertrand acted intentionally, by dol éventuel. In this scenario, since Bertrand was repeatedly made aware of the cyber risks (training and mock tests), he had to exercise particular caution and therefore consider the harmful results of his behavior. However, in order for the dol éventuel to be admitted, Bertrand must also recognize the danger and come to terms with the potential damage to the protected legal asset, in this case the right to dispose of data in the broad sense and sensitive data [19] [20]. This element seems to be lacking in this scenario, because Bertrand's behavior, as soon as he noticed the cyber-attack, was to alert the IT department. Therefore Bertrand's behavior is rather a matter of conscious negligence [21]. Thus, Bertrand does not risk criminal prosecution as an accessory to the offenses of art. 143 SCC and 179novies SCC, despite the fact that his actions violated several articles of the company's IT charter.

In the case of damage to data (art. 144bis al. 1 SCC), the analysis of the objective and subjective elements for primary participation leads to the same conclusions as in the first scenario: Bertrand does not face any criminal prosecution as the perpetrator. However, it is still necessary to examine whether the cybercriminal participated in the crime of damaging data as an accessory. As a reminder, for Bertrand to act as an accomplice, he must be aware of the real possibility of the damage which will be caused therefore Bertrand does not face any criminal consequences under the data damage provision.

In this scenario, Bertrand's conduct also results in the encryption of the data, the threat of publication and the demand for ransom. Thus, the four objective elements of extortion (art. 156 SCC), meaning: the use of a means of coercion, the realization of an act detrimental to the victim's financial interests, damage and a causal link, are fulfilled. The subjective elements of the offense are intention and the purpose of enrichment. Bertrand does not have the intent to enrich himself, therefore it is not possible for him to be the main participant in the crime. On the other hand, the cybercriminal commits the offense and is therefore to be considered as the perpetrator of the crime. It is necessary to analyze whether Bertrand can be prosecuted as an accomplice. In this scenario, Bertrand is again acting with conscious negligence, since he must be aware of the real possibility of the damage being caused, but is unhappy with the result.

In conclusion, Bertrand does not face any criminal consequences as a principal and accessory participant for the criminal provisions mentioned above. On the other hand, he may face other sanctions, such as: civil or administrative prosecution due to his failure to comply with the organization's IT charter.

3.3 Cyber-Attack on a Watchmaking Company

The third scenario concerns the ransomware infection of a watch company. This scenario is inspired by true facts about a computer attack in Switzerland in 2020 [11]. The infection of the computer system happens because of a contaminated USB stick on an employee's computer.

3.3.1 FACTS

A watch company employs more than 15,000 people and has worldwide revenues of more than 7.3 billion Swiss Francs per year. The data collected by the organization contains confidential information concerning customers, employees, and suppliers. The company is aware of cyber risks and allocates a considerable annual budget to reduce the risk of a cyber incident occurring. Every employee signs an IT charter and several training courses are organized for employees. In addition, mock tests are carried out twice yearly and, depending on the results, further training is mandatory for the employees concerned.

One day, Clément, who had been an administrative employee for 30 years, received a letter of dismissal for reasons of company reorganization. He was very unhappy with this news and tried to negotiate another role with the director and the HR department however, without success. Being highly disappointed and wishing to take revenge, he learned about the existence of ransomware-as-a-service and managed to acquire the software by agreeing to pay 50 percent of the revenues to the criminal organization which developed the malware. On the eve of his last day of work, Clément prepared a USB stick which contained the Netwalker ransomware, which is dangerous malware with a double extortion tactic of asking for a ransom and leaking data on the Dark web. He arrived at work early in the morning, copied the entire customer data onto a hard drive, then inserted the USB stick into a company computer and immediately left the premises. Instantly, all the organization's data was encrypted and a ransom of six million Bitcoins was demanded. Some days later, Clément published part of the stolen data on the Dark web and contacted the company to increase pressure for the ransom to be paid. The company paid the ransom and Clément paid three million to the criminal organization.

3.3.2 ANALYSIS

Through his behavior, Clément demonstrates the intention to take revenge and harm his organization. First, he acquires ransomware from the Internet. Second, he copies the entire company's data and encrypts the data servers with the Netwalker ransomware which was installed on a USB stick. Finally, he publishes confidential data on the Darknet and demands a ransom from the company.

With the presented state of affairs, Clément extracts all personal data from the company, which means that he gains control over the data, most of which is not intended for him. Thus, the first two objective elements of art. 143 SCC and 179novies SCC are fulfilled. Since the data is located in the company and physical protection (secure entrance door) protects access, the criterion that the data is specially protected is also met. In a second step, Clément sends a ransom note to the company, which establishes his purpose of unlawful enrichment. Clément's removal of the data is intentional, as he is determined to firmly act (art. 12 SCC) [22]. All the elements of the abovementioned offenses have been fulfilled, which incriminates Clément as the perpetrator. There is no evidence that the offense is unlawful. Finally, Clément is guilty, because his behavior cannot be qualified as an error in the sense of the law and because of his awareness of cyber risks, he is aware of the illegal nature of his behavior.

If the ransomware installed by Clément encrypts the company's data, this constitutes an act of damage under art. 144bis al. 1 SCC. The second objective element of the crime of damage to data is also fulfilled, because the object of the harm concerns computer data. Clément's act of damage is intentional for the reasons developed in the previous offense. With these facts, Clément fulfils all the elements of art. 144bis al. 1 and is considered to be the perpetrator.

Regarding art. 156 SCC, the first objective element is achieved, due to the fact Clément uses a means of coercion against the company, by threatening to publish the rest of the stolen data on the Dark web. He also achieves the other objective elements by giving the company the option of paying six million in Bitcoins to stop the computer attack. The breach is complete as the company suffers financial damage by paying the ransom. The causal link between the act of coercion, the prejudicial act and the damage is clearly established. With regard to the subjective constitutive elements, the offense requires a purpose of unlawful enrichment and intention. These two elements are present in the statement of facts. Thus, Clément fulfils all the elements of art. 156 SCC as a perpetrator of the offense.

Clément's conduct is also punishable under s. 35 FADP. When Clément publishes the company's data on the Dark web, he violates his duty of discretion. Since the company processes customers', employees', and suppliers' confidential data, it is obvious that secret and sensitive personal data or personality profiles are involved in the processing. Moreover, the publication of this data on the Darknet, is divulged without the consent of the persons concerned, therefore according to the law, the disclosure is carried out unlawfully. In order for Clément to be prosecuted according to art. 35 FADP, it is necessary that the company files a complaint.

In conclusion, in this scenario, Clément is guilty of unauthorized obtaining of data (art. 143 SCC), obtaining personal data without authorization (art. 179novies SCC), damage to data (art. 144bis ch. 1 SCC), extortion (art. 156 SCC) and breach of professional confidentiality (art. 35 FADP). Different contests (real or ideal) will apply before Clément's sentence is set.

4 Discussion and Recommendations

The case study below demonstrates the importance for organizations to implement strategies to educate employees on cyber risks and keep them informed of the latest threats. Employee liability (criminal, civil and contractual) could be addressed in such training, using examples and case studies to emphasize the importance of complying with company guidelines and ensuring that mistakes are not made which could lead to cyber infections. Additionally, improved training strategies can also help companies better comply with the requirements of cybersecurity-enhancing solutions on the market, such as purchasing cyber insurance or obtaining a certification label.

Despite a wide variety of existing cybersecurity tools, organizations are indeed facing difficulties in ensuring effective digital security. In recent years, several private and public initiatives have been launched in Switzerland to help organizations maintain their cyber security. Despite cyber insurance not being mandatory in Switzerland, it is one of the proposed solutions and has been since 2018 [4]. This insurance generally covers all financial consequences of cyber events [23]. However, taking out cyber insurance imposes certain obligations on the organization, such as: implementing technical security measures and raising employee awareness of cyber risks. Each insurance policy specifies in its terms and conditions the level of training and awareness required for employees, although in many cases no training standards are currently imposed. Failure to meet contractual obligations can result in a reduction in compensation for damages.

Several institutions have developed certification labels to support small, medium and large organizations in cybersecurity. In the vast majority of cases, to obtain certification, organizations are required to conduct a vulnerability study, followed by a phishing campaign among employees. Certification is awarded when the phishing campaign achieves a response rate which is below a certain threshold. On the other hand, it is repeated if the percentage is too high. Accreditation usually ends with the implementation of organizational

measures to improve cybersecurity, such as: the establishment of a user charter and an information security policy. These documents are developed with employee participation, which effectively makes them more aware of cybercrime issues.

To improve organizations' cybersecurity and reduce the risk of being infected by ransomware, authorities and organizations such as the National Cyber Security Centre (NCSC) [24]and NoMoreRansom.org [25], recommend taking various measures. From a technical perspective, the use of multi-factor authentication is now considered an essential security measure for accessing organizational resources and services. To enhance security, the organization must also use powerful and robust detection and protection solutions (specialized software). In addition, automatic scheduling of software updates and security applications, such as: an antivirus and a firewall, is another important measure to avoid security breaches. Finally, educating employees on displaying file extensions and disabling macros can also help to improve the organization's security.

At the administrative level, the organization can assess an employee's computer security knowledge and awareness upon recruitment with the aim of tailoring training and technical measures which can be installed on the employee's computer. It is also recommended to organize a cyber incident response process early therefore the employees are aware of the procedures to follow in the event of a computer threat. Finally, the organization must establish a computer charter with employees' participation in order to define the rules of computer usage and also each workers' responsibility in this area.

5 Conclusion

In view of the above, it seems obvious that the criminal liability of employees will be difficult to establish in the case of a ransomware attack, particularly because of the difficulty of proving the subjective element - intention - even at its weakest level, the dol éventuel. If, on the other hand, this aspect can be established, Swiss law has a regulatory framework leading to the potential application of several norms, depending on the modus operandi of the ransomware and the severity of the consequences. It seems obvious that, except in the case of an intentional infection or a gross case of dol éventuel, the consequences of the error committed will mainly have to be evaluated on a civil and contractual level. However, recognizing the limits of criminal liability remains important, and the results of this preliminary study may be helpful in better understanding - and reducing - the risks of infection due to employee error.

To avoid the occurrence of a cyber incident, all actors in the organization must take steps and enforce certain security standards. This contribution focuses on employee responsibility; however, it is essential to mention that the organization must also take its own responsibility in the matter. It is essential that the organization provides its employees with the tools and training to ensure the security of its IT devices. If it does not and a cyber incident occurs, it would be interesting to study the organization's criminal and civil liability. The organization's involvement in cybersecurity could become a justification for engaging its liability instead of the employee's.

Finally, cyber insurance and cybersecurity certification labels are suitable solutions to improve the security of organizations. Unfortunately, very few organizations invest money in these tools and in cybersecurity in general, despite the relatively accessible cost. However, the price of effective cybersecurity is likely to increase. Indeed, according to a French report on cyber insurance, the "claims to premiums" ratio has risen from 84 percent to 167 percent in 2020 [26].

It is also important to remember that the Swiss legal framework relevant to cybercrime will be modified by the legislator in the coming years. For example, it would be interesting to study the changes in the criminal provisions of the FADP which will come into effect as of September 1, 2023 [27] and to follow with interest the legislative changes regarding the obligation to report cyber incidents. These legal adaptations are supported by the recent institutional changes of the National Cyber Security Centre (NCSC). Thus, all these adaptations demonstrate that the state clearly has the will to improve the fight against cybercrime.

Authors' Details

Renaud Zbinden

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
renaud.zbinden@he-arc.ch

Luca Brunoni

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
luca.brunoni@he-arc.ch

Olivier Beaudet-Labrecque

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
olivier.beaudet-labrecque@he-arc.ch

References

[1] N. Pinguely, "Les hôpitaux suisses subissent plusieurs millions d'attaques chaque mois," *24heures.ch*, April 2022.

https://www.24heures.ch/les-hopitaux-suisses-subissent-plusieurs-millions-dattaques-chaque-mois-520894752923.

[2] "Convention du 23 novembre 2001 sur la cybercriminalité." (SR 0.311.43).

[3] J. Müller, *La cybercriminalité économique au sens étroit: analyse approfondie du droit suisse et aperçu de quelques droits étrangers*. PhD thesis, Université de Lausanne, Faculté de droit et des sciences criminelles, 2012.

[4] B. Klett and S. Stirnimann, "Cyber-crime : Verantwortung und vorgehen im ernstfall," *Sécurité & Droit*, vol. 2, pp. 71–78, 2017.

[5] S. Werly, "La transposition de la convention du conseil de l'europe sur la cybercriminalité en droit suisse," *Medialex*, pp. 121–123, 2010.

[6] J. Müller, "Le droit matériel suisse est-il conforme aux exigences minimales posées par la convention du conseil de l'europe sur la cybercriminalité ?," *sic!*, vol. 6, p. 332, 2016.

[7] S. Métille and J. Aeschlimann, "Infrastructures et données informatiques: quelle protection au regard du code pénal suisse?," *ZStrR: Schweizerische zeitschrift für strafrecht*, vol. 132, no. 3, pp. 283–317, 2014.

[8] Conseil fédéral, "La confédération examine la possibilité d'introduire une obligation de déclarer les cyberincidents," *admin.ch*, December 2019. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-77526.html.

[9] S. Fanti, "De l'obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA – communication FINMA sur la surveillance 05/2020." swissprivacy.law, December 2020. https://swissprivacy.law/43/.

[10] Conseil fédéral, "Le conseil fédéral soumet au parlement le message concernant l'obligation de signaler les cyberattaques contre les infrastructures critiques." admin.ch, December 2022. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-92030.html.

[11] C. Pugnetti and C. Casián, "Cyber risks and swiss smes: an investigation of employee attitudes and behavioral vulnerabilities," 2021. ZHAW Zürcher Hochschule für Angewandte Wissenschaften.

[12] L. Brenet and T. Brenet, *Cyberespace et cyberattaque : Comprendre et se protéger !* Paris: Afnor éditions, 2022.

[13] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 12 N 4.

[14] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 12 N 15.

[15] "ATF 69 IV 75, consid. 5."

[16] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 25 N 5.

[17] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 25 N 6-8.

[18] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 25 N 10.

[19] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 12 N 18.

[20] Tribunal fédéral, "Arrêt du tribunal fédéral 6b_604/2017 du 18 avril 2018, consid. 2."

[21] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 12 N 32.

[22] M. Dupuis *et al.*, *Petit commentaire, Code pénal*. 2 ed., 2017. Art. 12 N 7.

[23] J. de Werra and Y. Benhamou, "Cyberassurance: instrument utile pour la cybersécurité des entreprises? analyse juridique et recommandations des mesures étatiques concernant les cyberassurances visant à protéger les entreprises (pme)," *Jusletter*, August 2020.

[24] NCSC, "Ransomware." ncsc.admin.ch, Decembre 2020. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-bedrohungen/ransomware.html.

[25] NO MORE RANSOM, "Comment se prémunir d'une attaque par rançongiciel ?." nomoreransom.org, 2021. https://www.nomoreransom.org/fr/prevention-advice.html.

[26] AMRAE, *Lumière sur la cyberassurance (LUCY)*. 2021.

[27] Conseil fédéral, "Nouveau droit de la protection des données à partir du 1er septembre 2023." admin.ch, August 2022. https://www.admin.ch/gov/fr/accueil/documentation/communiques/communiques-conseil-federal.msg-id-90134.html.

PAGE LEFT BLANK