The Legal Risks of Ransomware Payments

Delphine Sarrasin*

Sara Pangrazzi**

Pauline Meyer***

Ransomware attacks are a malicious kind of cyberattack where attackers use malware that encrypts an organization's data and extort their victims. Not only the attacks themselves, but also a subsequent ransom payment to a cybercriminal may lead to considerable damages and involve risks for a victim. This article examines some key legal risks in the Swiss criminal context regarding ransom payments by the victim as well as by third parties. It analyzes potential criminal offences, corporate liability, and possible justifications for paying ransom, emphasizing the need for case-specific assessments. Despite this focus on criminal law, there are also civil or contractual legal obligations that can become relevant. And as paying ransoms often has a transnational component (since a criminal might act from abroad and big corporations often have international subsidiaries or assets), such possible cross-border legal consequences, consequences under foreign law or under embargo provisions are also briefly mentioned.

Ransomware-Angriffe sind eine böswillige Art von Cyberangriffen, bei denen Angreifer Malware verwenden, die die Daten einer Organisation verschlüsselt, und ihre Opfer erpressen. Nicht nur die Angriffe selbst, sondern auch eine anschließende Lösegeldzahlung an einen Cyberkriminellen kann zu erheblichen Schäden führen und Risiken für Opfer mit sich bringen. Dieser Artikel beleuchtet einige zentrale rechtliche Risiken im schweizerischen Strafrechtskontext im Zusammenhang mit Lösegeldzahlungen durch das Opfer sowie durch Dritte. Er analysiert potenzielle Straftaten, Unternehmenshaftung und mögliche Rechtfertigungsgründe für die Zahlung von Lösegeld und betont die Notwendigkeit fallspezifischer Beurteilungen. Trotz dieses Schwerpunkts auf dem Strafrecht können auch zivil- oder vertragsrechtliche Verpflichtungen relevant werden. Und da die Zahlung von Lösegeldern oft eine grenzüberschreitende Komponente hat (da ein Krimineller möglicherweise aus dem Ausland agiert und große Konzerne oft über internationale Tochtergesellschaften oder Vermögenswerte verfügen), werden auch solche möglichen grenzüberschreitenden Rechtsfolgen, Konsequenzen nach ausländischem Recht oder nach Embargobestimmungen kurz erwähnt.

Contents

* Delphine Sarrasin, Master's degree in Law, PhD candidate at the University of Lausanne.
** Sara Pangrazzi, Dr. iur. des., University of Zurich.
*** Pauline Meyer, Master's degree in Legal Professions Law, PhD candidate at the University of Lausanne.
The authors thank Prof. Sylvain Métille and Prof. David-Olivier Jaquet-Chiffelle for the fascinating exchanges on this subject and for the proofreading. This paper is written in the context of the NRP-77 project «Promoting trust in cybersecurity through ethics and law», financed by the SNF, Internet: https://www.nfp77.ch/en/JTLSBgi4qITuxdwd/project/promoting-trust-in-cybersecurity-through-ethics-and-law (accessed 10.7.2023).

I. Introduction

Ransomware attacks have become one of the greatest threats for the (Swiss) economy and administration.[1] Ransomware attacks are a malicious kind of cyberattack where perpetrators use malware that encrypts an organization's data and demand payment to restore access.[2] Attackers may additionally threaten to disclose the information to authorities, competitors, or the public (double extorsion). They might also want to threaten the customers of the victim organization (triple extorsion). Such attacks are described as being attractive to cybercriminals «because they can encrypt systems with comparatively little effort and because individual companies and organizations pay large amounts of ransoms to reverse the encryption».[3] Thereby, the risks of ransomware attacks affect business operations of *all* kinds and across *all* sectors and industries. Various prominent examples continue to illustrate the severity and scope of such ransomware attacks, with victims suffering different degrees and types of harm for entire businesses and value supply chains within and across national borders.

Recent internationally known ransomware incidents led to huge amounts of ransom being paid to criminals: in early May 2021, energy provider Colonial Pipeline paid a USD 4.4 million ransom after its operations were shut down by a ransomware attack.[4] A few weeks later, in early June, JBS – a leading global food company – paid a USD 11 million ransom following an attack that affected its facilities in the USA, Australia, and Canada, temporarily forcing the company to suspend its operations.[5] Although these are examples of large international corporations, even Swiss companies and smaller businesses are regularly affected: in May 2020, Stadler Rail was demanded a USD 6 million ransom after its data was encrypted.[6] And in July 2021, a popular Swiss price comparison website, comparis.ch, was shut down by ransomware criminals requiring USD 400,000 in cryptocurrencies to put it back online.[7] Despite the relatively smaller sums, these companies, as well as their core business, can be severely affected in such a case.

These known cases are only very few examples of an estimated huge number of unreported cases globally and it is very difficult to know how many victims actually pay ransoms.[8] Many companies pay large sums of money covertly when they fall victim to a ransomware attack. They often do so in the hope of avoiding reputational risks and to repair the operational and monetary damage caused. The reasons for such payments are often related to the quality of companies' back-ups, to a possible urgency in terms of time, to the estimated costs of the system outage, whether they have cyber insurance or if their data is threatened to be made public.[9] Most companies hence decide to pay because of internal calculations. If they feel that paying the ransom is less expensive than enduring an operational business blockage and restoring a whole IT system, they may think a payment is economically justified.[10]

---

1 See e.g. Swiss National Cyber Security Centre (NCSC), Semi-annual Report 2022/1, 3.11.2022, Internet: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/lageberichte/NCSC_2022-1_HJB_EN.pdf.download.pdf/NCSC_2022-1_HJB_EN.pdf (accessed 24.7.2023), 24 ; Postulate Graf-Litscher 21.4512 «Améliorer la protection contre les rançongiciels» submitted on 16.12.2021, Internet: https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20214512 (accessed 24.7.2023).

2 For a definition of ransomware attacks see: NIST, Ransomware Risk Management: A Cybersecurity Framework Profile, 2.2022, Internet: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf (accessed 24.7.2023), 1; Yaniv Benhamou/Louise Wang, Cyberattaque et ransomware: risques juridiques à payer et assurabilité des rançons, RSDA 2023, 80 ff., 80.

3 See e.g. postulate 21.4512 (n. 1).

4 Collin Eaton/Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $ 4.4 Million Ransom, The Wall Street Journal, 19.5.2021, Internet: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 (accessed 18.7.2023). Part of the ransom was recovered, see Amanda Macias/Christina Wilkie, U.S. recovers $ 2.3 Million in Bitcoin paid in the Colonial Pipeline Ransom, 7.6.2021, Internet: https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html (accessed 13.4.2023).

5 Jacob Bunge, JBS Paid $ 11 Million to Resolve Ransomware Attack, The Wall Street Journal, 9.5.2021, Internet: https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781 (accessed 18.7.2023); Alvaro Marañon/Benjamin Wittes, Lawfare, 11.8.2021, Internet: https://www.lawfareblog.com/ransomware-payments-and-law (accessed 13.4.2023).

6 Giorgio Müller, Hacker stellen Stadler Rail ein Ultimatum – Spuhler will hart bleiben, NZZ, 29.5.2020, Internet: https://www.nzz.ch/wirtschaft/hacker-stellen-stadler-rail-ein-ultimatum-ld.1558845?reduced=true (accessed 10.7.2023).

7 Swiss Info, Ransomware Attackers Demand $400'000 from Swiss Website, 8.6.2021, Internet: https://www.swissinfo.ch/eng/sci-tech/ransomware-attackers-demand--400-000-from-swiss-website/46770612 (accessed 13.4.2023).

8 ENISA, Threat Landscape Report on Ransomware Attacks, 29.7.2022, Internet: https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg (accessed 13.4.2023).

9 Ransomware Task Force, Combatting Ransomware, A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force, 2021, Internet: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf (accessed 24.7.2023), 12.

10 Chainalysis Team, Ransomware Revenue Down As Many Victims Refuse to Pay, 19.1.2023, Internet: https://blog.chainalysis.com/

Ransom payments are an important part of the criminal phenomenon of «ransomware attacks», as the main reason for these attacks is profit.[11] This is why it is important to try to minimize the payments. It is recommended by the Swiss National Cyber Security Centre (NCSC), as well as by other (foreign) governmental authorities, not to pay ransoms.[12] This is based on multiple – and by far not only legal – reasons. Firstly, doing so only incentivizes the criminal business behind ransomware attacks and makes the criminals more powerful.[13] With the money they can continue their activities, making more victims along the way. Secondly, the victim of a ransomware attack has no guarantee that their data will be restored once the ransom is paid. According to a 2021 study by the cybersecurity firm Sophos[14], organizations, on average, are only able to recover 65 % of their files after a payment, leaving over one third of their data inaccessible.[15] 29 % of respondents reported that only 50 % or less of their files were restored, and only 8 % of victims got all their data back.[16] Also, computers will mostly still be infected, adding further costs to remove malware and replace infrastructure and hardware after a payment is issued. Thirdly, by paying a ransom, a company might become an attractive victim for further attacks.[17]

However, although the list of reasons not to pay ransoms could go on, some victims still choose to pay. Hence, the more and more governments began thinking of regulatory levers to reduce the number of payments made to criminals. In this sense, even a possible ban of ransom payments was discussed by different states. Although a ban could constitute an interesting lever, such a criminal law regulation needs careful evaluation. To assess if such a ban could be a good idea and whether it would generate an added value, one should first look at the current legal framework to see if some forms of ransom payments are already penalized. Therefore, this paper will focus on some important legal offences according to Swiss criminal law that could be relevant in the context of ransomware payments.

This paper aims to apprehend the current Swiss legal landscape to see whether ransom payments can already be illegal under certain circumstances. In other words, this paper provides an overview of the current legal risks for companies, organizations, and natural persons facing a demand for a ransomware payment. The analysis includes potential risks for the victims as well as for possible third parties (such as insurers or computer security incident response teams [CSIRTs]) that might be involved in a payment. Although the last part will pick up certain (international) risks that go beyond criminal law, the main focus is on Swiss criminal law.

II. Legal Risks to Consider in the Swiss Context

A. A Swiss Context Only Exists in an International Context

As stated before, ransomware attacks are one of the most pressing threats to *all* kinds of organizations, ranging from small businesses to large and transnational enterprises across healthcare, retail, manufacturing, and other vital sectors. The (legal) circumstances of individual companies affected by ransomware attacks may therefore become complicated. Firstly, there are many internationally operating, complex, and economically intertwined large corporations and supply chains. Many companies work with several partners (suppliers, third-party providers) who deliver different products such as raw materials, services, or technologies – nationally, but also internationally.[18] As a result, many businesses are not only operating transnationally but also often depend on external – and sometimes international – goods, partners, and/or services in order to keep their daily operations going and towards which they have certain contractual obligations. Secondly, the payment of ransom in itself proves very complex. In the event of a ransomware attack, it is mostly not very clear to whom (and in which country) the fee will ultimately be paid. CWT Global, for instance, paid a settlement fee

reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/ (accessed 13.4.2023).

11 Ransomware Task Force (n. 9), 28. We can see that the decrease on the revenue caused by ransomware attacks is correlated with victims paying less, see Chainalysis Team (n. 10).

12 NCSC, Encryption Malware – What Next?, Internet: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html (accessed 13.4.2023).

13 *Ibidem*.

14 Sophos, The State of Ransomware 2021, Report, 4.2021, Internet: https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffh-qsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 (accessed 24.7.2023).

15 *Ibidem*; Chris Beck/Blake Fleisher, Does It Ever Make Sense for Firms to Pay Ransomware Criminals?, Insurance Journal, 8.7.2021, Internet: https://www.insurancejournal.com/news/international/2021/07/08/620508.htm^t (accessed 13.4.2023).

16 Sophos (n. 14).

17 Sophos (n. 14).

18 On supply chain attacks see: NCSC, Semiannual Report 2/2021, 5.5.2022, Internet: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/lageberichte/NCSC_2021-2_HJB_EN.pdf.download.pdf/NCSC_2021-2_HJB_EN.pdf (accessed 24.7.2023), 7.

in Bitcoin worth USD 4.5 million[19] without specifically knowing who was behind the attack. Bitcoin, like other cryptocurrencies, provide a fast payment service option making ransomware payments simple for victims while involving little risk for the criminals. As transactions through cryptocurrencies are difficult to track, they allow criminals to receive money with a high degree of anonymity. Bitcoin is a decentralized, public digital payment infrastructure that works because of the public blockchain network. This network basically allows for the receiving and sending of value by anyone and from anyone *in the world* that has access to a computer and an internet connection.[20] This is a novelty in the sense that, unlike every other electronic payment tool, Bitcoin (at least at this stage) works without any intermediary.[21] Hence, cryptocurrencies can be easily laundered through the darknet, allowing the cashing-out of funds easily, anonymously, and – importantly – regardless of national borders.[22] If the paid hacker group is indeed located abroad, this makes the problem an inherently international (potentially also political) one. However, this background information notwithstanding, the following chapters illuminate some concrete legal provisions that might become relevant for individuals and companies with connecting legal factors in Switzerland.

B. Legal Risks for a Victim Paying a Ransom

Today, Swiss law does not consider a payment of a ransomware *per se* to be a criminal offence.[23] However, depending on whom the money is paid to and under which circumstances, there are some existing legal provisions a victim needs to be aware of. Key criminal offences include the participation in or the support of a criminal or terrorist organization (art. 260ter CrimC), the financing of terrorism (art. 260^{quinquies} CrimC) and money laundering (art. 305bis CrimC), all of which are examined below.

1. Criminal or Terrorist Organization (art. 260ter CrimC)

In certain cases of ransom payments, one could consider the application of art. 260ter para. 1 lit. b CrimC (support of a criminal organization); more precisely in the event a victim of a ransomware attack would be funding a criminal organization through a payment. To commit this offence, there must be a form of intentional support of that organization.

A criminal organization is an organization pursuing criminal aims whose structure and workforce are kept secret.[24] It needs to consist of three or more people and is legally characterized by concrete elements, such as professionalism/commerciality, the absence of transparency, internal rules, the possibility to change its workforce without being endangered, etc.[25] There are different organizations that can be considered criminal organizations today. These can be as traditional as the mafia or new organizations that are specialized in cyberattacks like Evil corp.[26]

Art. 260ter CrimC does not only apply to someone actively participating in the activities of a criminal organization (art. 260ter CrimC para. 1 let. a) but is also applicable to someone merely supporting such an organization (para. 1 let. b). In both cases, however, the same penalties apply. In the case of someone paying a ransom to a criminal organization, para. 1 let. b could, at first glance, be applied, as the definition of «support» is quite large.[27] Examples are the delivery of weapons, the administration of heritage property and the providing of logistical support.[28]

---

19 Jack Stubbs, «Payment sent» – Travel Giant CWT pays $ 4.5 Million Ransom to Cyber Criminals, 31.7.2020, Reuters, Internet: https://www.reuters.com/article/uk-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-45-million-ransom-to-cyber-criminals-idUKKCN 24W26P?edition-redirect=uk (accessed 13.4.2023).

20 Peter Van Valkenburgh, The Public Internet Needs Public Payments Infrastructure, Coin Center, 11.10.2018, Internet: https://www.coincenter.org/the-public-internet-needs-public-payments-infrastructure/ (accessed 13.4.2023).

21 *Ibidem*.

22 See hereto: Orlando Scott-Cowley, Ransomware Payments: Funding the Business of Cybercrime Veeam, 4.9.2017, Internet: https://www.veeam.com/blog/frequent-methods-for-ransomware-payments.html (accessed 13.4.2023).

23 Benhamou/Wang (n. 2), 83.

24 BSK StGB-Engler, art. 260ter N 5, in: Marcel Alexander Niggli/Hans Wiprächtiger (editors), Basler Kommentar StGB, 4th edition, Basel 2019 (cit. BSK StGB-author).

25 BSK StGB-Engler (n. 24), art. 260ter N 6 ; CR CP II-Livet/Dolivo-Bonvin, art. 260ter N 5 ff., in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (editors), Code pénal II, Commentaire romand, Basel 2017 (cit. CR CP II-author).

26 BSK StGB-Engler (n. 24), art. 260ter N 13; The U.S. Department of the Treasury mentioned Evil Corp as an example in the frame of its sanction lists, see U.S. Department of the Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 21.9.2021, Internet: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (accessed 14.4.2023), 3.

27 Message du 30 juin 1993 concernant la modification du Code pénal suisse et du Code pénal militaire (Révision du droit de la confiscation, punissabilité de l'organisation criminelle, droit de communication du financier), FF 1993 III 269 ff. (cit. Message organisation criminelle), 293 f.

28 Message organisation criminelle (n. 27), 293 f.; Andreas Donatsch/Marc Thommen/Wolfgang Wohlers, Strafrecht IV, Delikte gegen die Allgemeinheit, 209 f.

Technically, paying a sum of money to a criminal organization could support its activities, as it would typically need the money to continue them.[29] In a similar sense, the use of ransomware proceeds to finance terrorism, human trafficking, and/or the proliferation of weapons is considered a risk that the G7 and the Institute for Security and Technology have expressed their concern about.[30]

According to the Swiss Federal Supreme Court, the act of supporting the organization must be conscious and intentional.[31] The entity or person making the payment would be likely to act intentionally (from the perspective of dolus eventualis, «dol éventuel», «Eventualvorsatz») from the moment that it *accepts the possibility* of the offence being committed, even if it does not wish for it to occur.[32] Though someone paying a ransom cannot always know with certainty to whom the money is going to, and generally does not wish to support a criminal organization, we believe a reasonable person should be aware that there is a realistic risk the perpetrator of a ransomware attack could be a criminal organization (especially when they claim to be such an organization) and that a payment could potentially support it. In this sense, the act of willfully paying a ransom could imply that the victim accepts this possibility. The intention – or dolus eventualis – regards both the support as well as the fact that the payment is made to a criminal organization. Even if the attribution of ransomware attacks and their respective payments (especially in cryptocurrencies) is difficult, we believe that the moment a victim thinks or assumes it is paying to a criminal organization, the offence could be considered intentional (dolus eventualis). However, the outcome will always depend on the specific circumstances of the case. In this sense, in practice there is often the difficulty of properly distinguishing between conscious negligence and dolus eventualis, whereas the «in dubio pro reo» principle will have to be considered.[33]

The only reason the dolus eventualis could be negated in a case of an illegal payment according to art. 260ter CrimC is that the person is under «absolute coercion».[34] One could argue about the absolute coercion in a case where, having tried every conceivable maneuver to recover its encrypted data, an organization under pressure ends up paying a ransom for it. In our view, for absolute coercion to be considered met, while always assessing the respective circumstances at hand, the data would have to be particularly sensitive (e.g., if patients of a hospital are endangered because of the data encryption), and the case a particularly acute and pressured one. Nevertheless, the fact that there is no guarantee to restore the data, that the attackers will not publish it, and that another attack can be avoided, should also be included in the appreciation. By contrast, depending on the concrete circumstances, an absolute coercion could potentially be denied in a case in which an organization pays to avoid the publication of «merely uncomfortable» information, as it can never know if paying would prevent any publication in the future and as there might be other appropriate measures that could be taken to that end.[35] However, regardless of the scenario, it will always come down to balancing the interests involved. In short, the concrete interpretations of support, intent, and possible justifications according to art. 260ter CrimC remain open and might be raised and concretized by judicial bodies. This concept as well as the constituent elements must always be examined in the circumstances of each case.

2. Financing Terrorism (art. 260^{quinquies} CrimC)

One could question if paying a sum of money to the perpetrator of a ransomware attack could be a way to finance terrorism. Art. 260^{quinquies} para. 1 CrimC states that «any person who collects or provides funds with a view to financing a violent crime that is intended to intimidate the public or to coerce a state or international organization into carrying out or not carrying out an act shall be liable to a custodial sentence not exceeding five years or to a monetary penalty».

However, para. 2 specifies that the person who «merely acknowledges the possibility that the funds he or she

---

29 CR CP II-Livet/Dolivon-Bonvin (n. 25), art. 260ter N 22; Umberto Pajarola/Moritz Oehnen/Marc Thommen, art. 260ter StGB N 450, in: Jürg-Beat Ackermann (editor), Kommentar, Kriminelles Vermögen, Kriminelle Organisationen, Zurich 2018.

30 Ransomware Annex to G7 statement, 13.10.2020, Internet: https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf (accessed 20.2.2023), 2; Ransomware Task Force (n. 11), 17.

31 BGE 132 IV 132 c. 4.1.4.

32 BGE 137 IV 1 c. 4.2.3, JdT 2011 IV 328; BSK StGB-Niggli/Maeder (n. 24), art. 12 N 52; CR CP I-Villard/Corboz, art. 12 N 64, in: Laurent Moreillon/Alain Macaluso/Nicolas Queloz/Nathalie Dongois (editors), Code pénal I, Commentaire romand, Basel 2021 (cit. CR CP I-author).

33 On the blurred boundary between dolus eventualis and conscious negligence, see CR CP I-Villard/Corboz (n. 32), art. 12 N 70-75b; BSK StGB-Niggli/Maeder (n. 24), art. 12 N 59; TF, 6B_238/2013, 22.11.2013, c. 10. If the person thinks he/she is paying a criminal organization, but in reality is not, he/she will not benefit from the error of fact as the court will judge the act according to the circumstances believed to be by the victim, cf. art. 13 CrimC.

34 CR CP I-Villard/Corboz (n. 32), art. 12 N 49.

35 One could argue that paying to try to avoid the publication of highly sensitive data (e.g. biometric data) may be justified.

provides may be used to finance terrorism» does not commit an offence under this article. That is because in this case the person paying doesn't provide funds «with a view to financing a violent crime that is intended to intimidate the public or to coerce a state or an international organization into carrying out or not carrying out an act» as stated in para. 1. A ransom payer will often not pay with the intent or the view that the money will specifically finance terrorism. It follows that this provision, in practice, will mostly not be applicable to the payment of a ransom if there was no intent that the money will or may be used for the purpose of terrorism.

Even in cases where the victim paying the ransom does know of the organization behind the ransomware attack (for example the Lazarus Group, which is thought to be responsible for the WannaCry attack[36]), art. 260^{quinquies} para. 2 would probably prevent a prosecution of the victim. Though criminal organizations are often vocal about their criminal or terrorist achievements, it remains that the victim usually does not pay the ransom with a view to finance said organization's violent crimes, but rather in the hopes of recovering his or her data. In most cases, the victim does not want that money to be used to finance terrorism. Since art. 260^{quinquies} para. 2 CrimC specifically excludes «Eventualvorsatz»/«dol éventuel» as a constitutive element,[37] this provision is not likely to be applicable in such scenarios. Similarly, the Federal Council considers that «proof is required that the author actually had the aim of promoting the terrorist acts and that he sought to achieve this aim by financially supporting that terrorist organization».[38]

3. Money Laundering (art. 305bis CrimC)

Art. 305bis CrimC states that «any person who carries out an act that is aimed[39] at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanor shall be liable to a custodial sentence not exceeding three years or a monetary penalty.»

Behaviors that are generally known to be *suitable* to frustrate the origin, the tracing or forfeiture of assets are sufficient, without there being a need for the frustration to have occurred.[40] It is often the case that ransomware attacks are committed by an individual or a group located outside of Switzerland, meaning that a money transfer from a Swiss account to a foreign account or in cryptocurrencies must be made. Generally, the doctrine is of the opinion that a money transfer from an account located in Switzerland to a foreign account is suitable to frustrate the tracing of assets.[41] Likewise, paying a sum of money in cryptocurrencies, which is frequently requested by the perpetrator, can be considered suitable to frustrate the identification of the origin and the tracing of the assets. That is especially the case if the payment is made through hidden websites or the darknet, since these websites are only accessible via a specific browser that protects their users' identities. The best known of these browsers in this regard is the Tor Browser, which encrypts all traffic, offers anonymous browsing and has the specificity to protect IP addresses of users and therefore prevents their attribution.[42] Deanonymizing the user and decrypting the data is possible but takes time and requires the use of more resources than the identification of a user and the transaction on the surface web.

In order to constitute money laundering, a predicate offence according to art. 10 para. 2 CrimC is required since the assets which are being laundered must originate from a felony or aggravated tax demeanor.[43] In the case of a ransomware attack, the perpetrator himself could, depending on his actions and among others, be guilty of an unauthorized obtaining of data (art. 144bis CrimC) or extortion (art. 156 CrimC),[44] which, according to art. 10 para. 2 CrimC, are both felonies if, in the case of art. 144bis

---

36 Nicole Perlroth, More Evidence Points to North Korea in Ransomware Attack, The New York Times, 22.5.2017, Internet: https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html (accessed 19.2.2023).

37 BSK StGB-Fiolka (n. 24), art. 260^{quinquies} N 20; CR CP II-Livet/Dolivo-Bonvin (n. 25), art. 260^{quinquies} N 18; Ursula Cassani, Le train de mesures contre le financement du terrorisme: une loi nécessaire?, RSDA 2003, 293 ff., 297.

38 Message du 26 juin 2002 relatif aux Conventions internationales pour la répression du terrorisme et pour la répression des attentats terroristes à l'explosif ainsi qu'à la modification du Code pénal et à l'adaptation d'autres lois fédérales, FF 2002 5014, 5065 f.

39 It is relevant to note that the English translation of «geeignet/«propre à» into «aimed» leaves a certain room for interpretation.

40 BSK StGB-Pieth (n. 24), art. 305bis N 49; PK StGB-Pieth/Schultze, art. 305bis N 17, in: Mark Pieth/Stefan Trechsel (editors), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4th edition, Zurich 2021 (cit. PK StGB-author); Donatsch/Thommen/Wohlers (n. 28), 502 f.

41 BSK StGB-Pieth (n. 24), art. 305bis N 49, but the Swiss Supreme Court was more careful in TF, 6B_453/2017, 16.3.2018, c. 7.2, saying that money laundering should only be admitted if the transaction is able to frustrate the confiscation of the assets in the foreign country.

42 Daniel Moore/Thomas Rid, Cryptopolitik and the Darknet, Survival 58, N 1 (2016), 7 ff., Internet: https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085 (accessed 24.7.2023), 15 ff.

43 BSK StGB-Pieth (n. 24), art. 305bis N 11; PK StGB-Pieth/Schultze (n. 40), art. 305bis N 10.

44 Fabian Teichmann/Léonard Gerber, Les attaques classiques par ransomware, Jusletter IT 7.6.2021, N 15 ff.

CrimC, the offender has caused major damage, or he or she acts for commercial gain (art. 144 CrimC para. 1 second sentence, para. 2 second sentence).

However, money laundering requires that the author knows or must assume that the assets which are being laundered originate from a felony or aggravated tax demeanor, which means that the assets actually need to «preexist» and originate from said possible felonies. In the scenario of a ransomware payment, it can be argued that there are no preexisting criminal assets since it is precisely the payment of the ransom with the victim's money that creates them.[45] On this view, the assets of the victim themselves are not considered to be stemming from a criminal activity, which could exclude the prosecution of the victim for money laundering.[46] However, it could also be possible that, depending on the circumstances at hand, a prosecutor would try to affirm money laundering more extensively. Based on how early in a chain of events one assumes money laundering to occur, it could possibly even be argued that a payment (out of the victim's funds) could be considered to be originating from the initial criminal activity of which it mostly is a constitutive element. In fact, the transaction itself often leads to the fulfillment and is the *result (damage/unlawful gain) of the predicate crime* (e.g., art. 156 CrimC). And as in the case of a ransom payment, the predicate crime happens with the knowledge of the victim, he or she knows or could potentially be expected to at least assume that the cybercriminal is committing a felony and that the paid sum will consequently stem from it (see next paragraph for the required intent).[47] As money laundering is constituted an offence against the administration of justice, it primarily aims at the protection of a state's interest in an investigation and prosecution of a(n) (initial) crime as well as its access to and confiscation of the funds deriving from that crime.[48] To that end, even just the *danger of a possible concealment* and the complicating of the traceability of criminal assets can already be relevant (as it is an «abstraktes Gefährdungsdelikt» / «délit de mise en danger abstraite»).[49] However, even if a prosecutor might try this reasoning, the authors generally agree that the asset should not be considered as preexisting according to art. 305bis CrimC since the original offence is being committed by the payment.

Furthermore, for money laundering to be committed, a certain degree of intention is required. In this context, dolus eventualis is sufficient,[50] meaning that the author of a payment only needs to «be aware of the circumstances that give rise to a pressing suspicion of facts that legally constitute a felony and accept the possibility that said facts have occurred». Even if the author doesn't know the legal definition of a felony, the respective actions might still be prosecuted if he or she contemplates and accepts that it is an act punishable by a significant sentence.[51] A victim that is being extorted by a cybercriminal could therefore generally be expected to be aware that the ransomware attack it is affected by could constitute a criminal (potentially commercial) offence that is punishable by a significant sentence. Furthermore, it seems reasonable to expect that by paying an anonymous criminal *through cryptocurrencies* the victim at least takes into consideration that there is a possibility of the concealment of these assets that are relevant to the administration of justice and that the money will most likely not be easily traceable afterwards. However, there needs to be a certain degree of intent that «aims» at the frustration of such assets and the difference between dolus eventualis and conscious negligence may, as for supporting a criminal organization (art. 260ter CrimC), raise questions.[52] Therefore, in sum, we consider it unlikely that a ransomware victim would be prosecuted for money laundering and that the courts would argue in this direction.

4. Other Possible Offences

In relation to ransomware payments, further offences could potentially become relevant. Among them is the handling of stolen goods (art. 160 CrimC), extortion (art. 156 CrimC), the unlawful use of financial assets (art. 141bis CrimC), and criminal mismanagement (art. 158 CrimC). Though it is not the aim of this paper to enumerate all of them, it must be noted that although estimated unlikely, these and further offences could apply depending on the concrete situation at hand. For example, should the victim of a ransomware pay the ransom using

---

45 With a similar reflection, cf. Benhamou/Wang (n. 2), 83.

46 Except in a situation in which the person within the organization would knowingly pay the ransomware with money originating from another felony or aggravated tax demeanor.

47 A similar question could be raised with art. 144bis para. 2 CrimC.

48 See BGE 129 IV 322 c. 2.2.4 with references.

49 BSK StGB-Pieth (n. 24), art. 305bis N 38; PK StGB-Pieth/Schultze (n. 40), art. 305bis N 17; Donatsch/Thommen/Wohlers (n. 29), 502 f. In this context it is further noteworthy that at least financial intermediaries have to observe increased due diligence obligations according to the Anti-Money Laundering Act when making such payments.

50 BSK StGB-Pieth (n. 24), art. 305bis N 59; CR CP II-Cassani (n. 25), art. 305bis N 42; PK StGB- Pieth/Schultze (n. 40), art. 305bis N 21.

51 CR CP II-Cassani (n. 25), art. 305bis N 43.

52 See supra II.B.1.

a third party's money entrusted to it without the latter's consent, art. 138 CrimC (misappropriation) could come into consideration.

Since criminal law principally applies to individuals, all the above-mentioned provisions mainly address individual behavior, even in a corporate environment. However, as it is mainly organizations and companies that are victims of ransomware attacks, corporate criminal liability according to art. 102 CrimC may not be excluded. In cases where the victim of the ransomware is a member of an undertaking (ranging from the CEO to an employee),[53] the latter's criminal liability can be engaged if it is impossible to identify the member who paid or decided the payment of the ransom because of a lack of organization within the company. However, if the person who made the payment is identified, art. 102 CrimC is not applicable, and that person will be the prosecutable entity.[54]

To impute responsibility to the company in the sense of art. 102 para. 1 CrimC, the payment must have been made in the course of commercial activities (i.e., any activity aimed at producing or exchanging goods or providing services).[55] Moreover, these commercial activities have to be in accordance with the objects of the undertaking, meaning that the offence is either an illicit means or an illicit incident occurring in the pursuit of an undertaking's licit goal.[56] However, there is no need for the payment to be made for the benefit of the company.[57] It must then be determined whether the payment of a ransom can be considered as having been made in the course of commercial activities. Since the primary aim of such a payment is to recover access to the undertaking's data, it can be argued that it does serve the interest of the company as the latter needs its data to accomplish its goals, whatever they may be.

Moreover, although art. 260ter CrimC could be taken into consideration in the case of a ransom payment by an individual employee,[58] art. 102 para. 2 CrimC is likely to (also) apply in this context. It states that «the undertaking is penalized irrespective of the criminal liability of any natural persons, provided the undertaking has failed to take all the reasonable organizational measures that are required in order to prevent such an offence». It follows that to apply para. 2, the undertaking must have failed to assure the application of these relevant legal obligations as well as the reasonable and necessary measures to prevent such a critical payment, which in turn led to or enabled the offence.[59] While it does not matter if the lack of organization actually favors the offence in para. 1, there must at least be a hypothetical causal link between the two elements in para. 2.[60]

Consequently, in the case of a ransomware payment, we cannot exclude that art. 102 para. 2 CrimC could apply. Although it is not *per se* illegal to make such a payment, the authorities strongly recommend not to proceed to such a payment.[61] Even if it could be difficult to determine whether a company has taken all reasonable and necessary measures to ward off the risk of one of its members supporting a criminal organization by paying a ransom, one could argue that the observation of certain standards can objectively be expected. These could entail, for instance, employee trainings and instructions on what to do when facing a ransomware attack or the establishing of internal guidelines stating that employees should not pay, etc.

5. Legitimate or Mitigatory Act in a Situation of Necessity (art. 17 and 18 CrimC)

If a person commits a criminal offence on legally excusable grounds, these serve as grounds of justification and can lessen the penalty. More specifically, legitimate (art. 17 CrimC) or mitigatory (art. 18 CrimC) acts in a situation of necessity can arise and lessen or even cancel a penalty if a person aims to save a protected legal interest. For these provisions to apply, the victim needs to be facing an imminent danger that he or she cannot ward off by other reasonable means.[62] The danger faced should be actual, concrete, and not otherwise avertable.[63] The offence committed by the victim should be appropriate to

---

53 CR CP I-Macaluso (n. 32), art. 102 N 28; Matthias Forster, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006, 154 ff.

54 Marc Jean-Richard/Laurence Uttinger/Dania Tremp, art. 77 N 26, in: Jacques-André Schneider/Thomas Gächter/Thomas Geiser (editors), LPP et LFLP, 2nd edition, Bern 2020.

55 BSK StGB-Niggli/Gfeller (n. 24), art. 102 N 79.

56 CR CP I-Macaluso (n. 32), art. 102 N 34; BSK StGB-Niggli/Gfeller (n. 24), art. 102 N 91.

57 CR CP I-Macaluso (n. 32), art. 102 N 37.

58 See *supra* II.B.1.

59 PK StGB-Trechsel/Jean-Richard (n. 40), art. 102 N 19a.

60 Niklaus Schmid, Einige Aspekte der Strafbarkeit des Unternehmens nach dem neuen Allgemeinen Teil des Schweizerischen Strafgesetzbuchs, 779 f.; PK StGB-Trechsel/Jean-Richard (n. 40), art. 102 N 19.

61 NCSC (n. 12); with the same opinion: Benhamou/Wang (n. 2), 81.

62 BSK StGB-Niggli/Göhlich (n. 24), art. 102 N 10.

63 *Idem*, art. 102 N 16; PK StGB-Trechsel/Geth (n. 40), art. 17 N 7.

avert the respective danger,[64] be necessary, and respect the proportionality *stricto sensu*.[65]

In the context of a possible legal justification of ransomware payments it could be argued as follows: firstly, as the victim has no real guarantee that by paying a ransom he or she will be able to recover the encrypted data, that the data will not be published, or that the organization will not be reattacked, it is not sure whether the payment is an appropriate means to save the goods endangered by the extortion.[66] It is not always possible to decrypt some or all of the encrypted data, or to avoid other damaging consequences.[67] Secondly, the payment would need to be necessary in order to be justified. However, a payment could be seen as necessary and appropriate in some cases, while not being necessary or adequate in others. For example, an organization which does not have proper offline backups and sees the ransom payment as the only way to recover the data, versus a company that is not operationally blocked by a ransomware attack because of successful backups. However, one could argue that paying the ransom is never the only way to recover the data and that there are always other remedies (such as asking for help from the responsible authorities that can provide assistance before a payment is made). Thirdly, the offence committed by the payment (potentially art. 260ter CrimC) should be proportionate to the prior offence (i.e., extortion according to art. 156 CrimC). This means that the interests the organization wants to defend need to generally outweigh the ones endangered by the criminal's attack.

Hence, to apply art. 17 CrimC in the ransomware context, the protected good that is endangered by the offence and is realized *through the payment* should be more important than the one that is violated *by the criminal*. However, it can be argued on whether the protected interests sacrificed by the victim would outweigh the interests endangered by the attack. This assessment ultimately requires a balancing of interests in any given case.

It must be noted that even if art. 17 CrimC is not applicable, art. 18 could still be relevant. According to the latter, the victim's payment could be justified if the person involved could not have been reasonably expected to abandon the endangered interest (art. 18 para. 2 CrimC). And if the interest was of high value but could reasonably have been sacrificed, the victim could still benefit from a reduced liability (art. 18 para. 1 CrimC).

In cases of ransomware payments, this would mean that art. 17 CrimC could only apply if the legally protected goods of the victim are predominant to the protected good by, for instance, art. 260ter CrimC. This requires a balancing of the affected interests which, on the one hand, can be the entrepreneurial freedom of the victim and his/her goods or assets that the criminal organization targets.[68] As ransomware attacks mainly target and block a company's data, depending on the organization's activities and the data it depends on in a given case, there might be different interests and operations that can be affected through the blocking of such data. On the other hand, art. 260ter CrimC primarily protects public security as it follows the logic of felonies and misdemeanors against public order. One could argue that for a critical infrastructure, such as a hospital, the protected interests that the victim tries to save could not be reasonably sacrificed, e.g., if patients' lives are endangered. Consequently, art. 17 CrimC could potentially come into play and justify a payment if such a payment can avert such damages. However, in cases that do not involve objectively «critical» interests, we think that it could become difficult to justify a payment that violates art. 260ter CrimC or other crimes that might be applicable. Similarly, art. 18 para. 2 CrimC seems difficult to apply in «general» cases as interests such as property or entrepreneurial freedom could, depending on the circumstances, possibly be expected to be (temporarily) sacrificed in order to protect public security. If, however, the interest of the victim was of high value according to art. 18 para. 1 CrimC, but could reasonably have been sacrificed, the victim might still benefit from a penalty reduction. However, in each case, the further conditions of art. 17 or 18 CrimC remain to be assessed; that is whether the commitment of an offence was appropriate, necessary, and proportionate to protect the endangered goods.[69] Both art. 17 and 18 CrimC are ultimately a question of balancing the involved interests and the situational circumstances.

Finally, it should be noted that even if a ransom-paying organization could be found guilty of supporting a criminal organization and art. 17 f. CrimC are not applic-

---

64 Message du 21 septembre 1998 concernant la modification du Code pénal suisse (dispositions générales, entrée en vigueur et application du Code pénal) et du Code pénal militaire ainsi qu'une loi fédérale régissant la condition pénale des mineurs, FF 1999 II 1787 ff., 1811.

65 PK StGB-Trechsel/Geth (n. 40), art. 17 N 10.

66 A criminal behind a ransomware attack who demands a ransom is committing extortion in the sense of art. 156 CrimC, see Benhamou/Wang (n. 2), 82. The provision protects the property and freedom, Teichmann/Gerber (n. 44), N 15.

67 NCSC (n. 12).

68 CR CP II-Livet/Dolivo-Bonvin (n. 25), art. 260ter N 3.

69 Benhamou/Wang also think that in other cases than a critical infrastructure like a hospital with patients who would be endangered where art. 18 para. 2 CrimC would be considered, art. 18 para. 1 CrimC could apply, see Benhamou/Wang (n. 2), 84.

able, the authority may still refrain from prosecuting it, bringing it to court, or punishing it (art. 54 CrimC).

6. A Concrete Example: comparis.ch

As stated above (*supra* I.), Comparis.ch AG suffered a ransomware attack in 2021. The attack was later attributed to REvil, also known as Sodinokibi, a notorious organized criminal enterprise that was thought to be based outside Switzerland. The group demanded a payment of USD 400'000 for the decryption of the data.[70] Comparis refused to pay the ransom. However, if Comparis had decided to pay, it could have – quasi in a worst case scenario – been potentially liable for supporting a criminal organization, at least in terms of the objective elements of the offence. In fact, REvil can be described as a criminal organization in the sense of art. 260ter CrimC as it secures financial gains by criminal means and seems to reunite the other characteristics of a criminal organization (para. 1 let. a ch. 1 *in fine*). As such, it could theoretically be argued that offering them financial assets allows them to continue their illegal activities. Furthermore, it is very difficult to know where exactly the money obtained by such a group is reinvested, especially when the assets take the form of cryptocurrencies. It is entirely possible and realistic that these assets are used to finance the group's criminal activities such as weapon delivery or terrorism. Ultimately, it is not necessary to prove a causal contribution to a specific individual offence of the criminal group, but the support needs to relate to their overall criminal activity.

As for intention, Comparis would have had to be aware or at least have had reasonable cause to suspect that the payment would be made to a criminal organization and that it would support its illegal activities. If the responsible group behind the attack is known to the victim, one could argue that there could have been reasonable cause to suspect such a scenario. However, there need to be objective and clear grounds to suspect that the ransom payment would be used to support criminal activity. Furthermore, it has been said above that dolus eventualis could only have been negated if Comparis had been under absolute coercion. This would, however, probably have been unlikely since the requirements for absolute coercion are rather high.[71]

Ultimately, the assessment of criminal liability in any example depends on the extent to which a victim was coerced and compelled to pay the ransom as well as the extent to which other measures would have been possible to avert the danger (also in light of art. 17 and 18 CrimC). Hence, it might well be that art. 18 para. 1 CrimC would be left as the only provision conceivable to justify such a payment. However, it would depend on the appreciation of the facts by the court to finally decide this.

C. Legal Risks for a Third Party Paying a Ransom

1. Possible Third Parties

It can be the case that the entity paying a ransom is not the direct victim of the ransomware attack, but an entrusted third party that makes the payment on behalf of the victim. It also happens that a third party recommends or encourages the victim to pay or offers to cover the payment.

Usually, this can be the case when the victim has contracted a cyber insurance policy that covers damage that results from ransomware attacks, which could also include a ransom payment, or when the victim is a client of a private CSIRT, which is a team of IT experts that offers assistance in cyber incidents and cyberattacks.[72] According to the 2022 edition of the yearly study led by Sophos on the state of ransomware, insurance companies paid the actual ransom in 40 % of the examined cases.[73] Similarly, a CSIRT could also proceed to the payment itself as part of its assistance in dealing with the attack. Another possibility, should the victim report the attack to the prosecuting authorities, is that the police would pay a ransom on behalf of the victim. Consequently, in the following, this paper analyzes whether the offences dealt with here could also apply to such involved third parties.

2. A Third Party Proceeding to a Payment

As mentioned, there are three possible categories of involved third parties that may proceed to a ransomware payment: an insurer, a CSIRT, or possibly even the police. Although there are probably other possible third parties that could be involved in a ransomware payment and this list is not exhaustive, these three categories will be briefly discussed below for the purpose of illustration.

---

[70] Hans-Jürgen Maurus/Jürg Candrian, Comparis nach Hackerattacke wieder online, Tages-Anzeiger, 8.7.2021, Internet: https://www.tagesanzeiger.ch/hacker-greifen-comparis-an-495012049008 (accessed 20.2.2023).

[71] See *supra* II.B.1.

[72] Pauline Meyer/Sylvain Métille, Computer Security Incident Response Teams: Are they Legally Regulated? The Swiss Example, International Cybersecurity Law Review, 10.2022, 3 f.

[73] Sophos (n. 14), 10.

In principle, the above-mentioned criminal offences according to the CrimC apply to any natural (or even legal) person. Therefore, if third parties like insurers or CSIRTs pay a ransom themselves, they could theoretically also commit such a crime. Hence, if applicable, they could be considered to be supporting a criminal organization in virtue of art. 260ter CrimC if the requirements examined above are met. Thereby, not only the objective and subjective elements of the crime itself, but also the reasons for a possible legal justification according to art. 17 and 18 CrimC follow the same logic as if the direct victim had paid.[74] However, it is to be noted that certain actors such as insurers (or banks) – other than CSIRTs or other actors that are not specifically regulated – have additional obligations to observe that might arise from their financial intermediary position.[75] Such rules often state that an intermediary must be able to verify the information of its account holders or economic beneficiaries, which is the so-called «know your customer» principle that stems from anti-money laundering laws.

As for a possible involvement of the police, it can be a helpful measure to include them in an ongoing ransomware attack. In this regard, it could even be a feasible alternative to paying a ransom. Police can advise and support an affected company on how to proceed, especially regarding the communication with the perpetrators, and on how to behave towards them as they frequently have relevant experience with such incidents. Notifying the police could also reduce risks of incompliance stemming from a possible payment and can be considered an often reasonable and appropriate alternative to wanting to resolve such an incident alone. Furthermore, the police work in a special environment that is usually part of concrete preliminary investigations of a case that are subject to strict rules according to the Swiss Criminal Procedure Code (CrimPC). Therefore, if the police are involved in an incident, they can take further measures to resolve and investigate the incident while, of course, having to keep the victim's information confidential. As this can be helpful for a victim, it is also advised by the NCSC to file criminal charges in any case.[76] This, however, means that if criminal charges are filed, the cantonal police, who are competent in this matter, would have the necessary information and tools to pay a ransom. In practice, it could even be a way to set a trap as part of the police's strategy to prosecute criminals, to attribute and secure relevant traces or assets. If the police therefore act in the context of preliminary investigations and paying a ransom becomes necessary to that end, their actions would be justified because there is a public interest in dealing with such attacks. In particularly serious crimes, the police might even legally conduct a process to pay a ransom for a victim in the course of a covered operation (see art. 285a or 298a CrimPC) in order to establish contact with the criminal and to solve such crimes. If the legal conditions are met (see art. 286 or 298b CrimPC), the police would not be committing an offence.

3. A Third Party Encouraging or Covering a Payment

Once a ransomware attack occurs, the question arises on how to limit or stop the damage it causes. In this regard, for insurers, art. 38a of the Insurance Contract Act (Loi sur le contrat d'assurance, Versicherungsvertragsgesetz) can become relevant for the decision of whether its client should pay or not pay a ransom. According to art. 38a of the Insurance Contract Act, the beneficiary of an insurance must do everything possible to limit damage.[77] Unless in immediate danger, this requires that the beneficiary asks the insurer for instructions on which measures to take to mitigate the damages; instructions that he must consequently follow.[78] Within such instructions it is conceivable that the insurer recommends the payment of a ransomware to avoid (further) damage. This could be stated – implicitly or explicitly – through a general policy or also ad hoc during an ongoing case. It cannot be fully excluded that an insurer advises to pay a ransom as it could consider it economically cheaper than restructuring the whole IT infrastructure of an insured company. According to the above-mentioned 2022 study led by Sophos, 89% of the companies hit by ransomware had an insurance covering the financial risks posed by ransomware.[79] In most cases, this policy covered «clean-up costs», i.e., the costs necessary to get the company back on its feet.[80] And as mentioned before, actual ransom payments were covered in 40% of the examined cases.

---

74 See *supra* II.B.1.

75 For more information on this subject, cf. Benhamou/Wang (n. 2), 85 f.

76 NCSC (n. 13).

77 BGE 128 III 34 c. 3b, JdT 2022 I, 629 ff.

78 Jean-Maurice Frésard, art. 38a N 60, in: Vincent Brulhart/Ghislaine Frésard-Fellay/Olivier Subilia (editors), Loi sur le contrat d'assurance, Commentaire romand, Basel 2022; Thierry Luterbacher, Ausgewählte Aspekte im Umgang mit Rechtsschutzversicherungen, in: Stephan Fuhrer/Ueli Kieser/Stephan Weber (editors), Mehrspuriger Schadenausgleich/Des différentes voies menant à la réparation du dommage, Zurich 2022, 775 ff., 790.

79 Sophos (n. 14), 8.

80 *Idem*, 10.

Furthermore, an affected company may also ask or hire a CSIRT for guidance on technical and organizational measures once it is hit by a ransomware attack. Although a CSIRT would not in that sense cover the costs of the ransom payment, it could indeed encourage the victim to pay, based on its analysis of the estimated damages. Similar to the above-mentioned arguments, at first sight it could be considered more cost-effective, «easier», and more promising to pay a ransom rather than enduring the blockage of business operations and/or fixing and restoring a whole IT structure and data access.

However, if that payment turns out to constitute an offence, any third party actively recommending and encouraging a victim to pay a ransomware could potentially also become liable. In this sense, one could argue that a third party willfully inciting or assisting a victim to pay could be considered inciter or complicit in virtue of art. 24 or 25 CrimC if he or she knows or must reasonably assume that, for instance, a criminal organization in the sense of the CrimC is behind the attack.[81] This assumption could – at least theoretically – be reasonably expected before or while directly instructing a payment, and theoretically also if payments are *generally* recommended and covered.

Finally, however, it should be added that despite cyber insurance policies having long covered ransomware payment costs, in May 2021 the global insurance company AXA publicly and explicitly stated that it would no longer be reimbursing customers for making payments to ransomware criminals.[82] Similarly, in its 2022 report, the Geneva Association of insurance companies also discourages insurers to pay ransomware demands.[83] Hence, it can be assumed (and hoped) that other insurers will effectively follow this tendency.[84]

D. Risks Beyond Swiss Criminal Law

First, besides key criminal provisions, victims paying a ransom could also be liable based on other legal grounds. There are a variety of civil and contractual provisions that might become relevant in a given case. For example, as for certain agreements with suppliers and customers, concrete contractual questions might arise that can also regard payments.[85] A ransom payer could further be liable in relation with his/her duties in dealing with customers' data, his/her contractual security obligations, and duty of care to reduce certain damages. One could either argue that the payment itself can constitute damage in legal terms or that paying a ransom may be seen as necessary to reduce further damage in certain cases. However, we think that seeing a payment as an actual obligation to minimize damage is going too far.[86] We consequently agree that any such (contractual) obligation should be interpreted and understood in the broader context of public recommendations not to pay the ransom.[87]

Second, like every kind of cyberattack, ransomware attacks can have transnational effects and consequences. It is important to understand that by paying ransoms, there are not only risks of violating Swiss laws, but potentially also internationally relevant or foreign regulations. In Switzerland, as in other countries, there are economic lists that prohibit the payment to certain people and organizations. In Switzerland, these prohibitions are included in the various ordinances providing Swiss economic sanctions.[88] Paying a criminal that is on such a list without having conducted reasonable due diligence might therefore become relevant for embargo provisions in Switzerland, but also for sanction lists abroad. Besides countries being listed on sanction lists, certain individuals can also be – and are – listed. In the case of cyberattacks specifically, certain attackers who are behind known ransomware

---

81 Benhamou/Wang (n. 2), 86.

82 Frank Bajak, Insurer AXA to Stop Paying for Ransomware Crime Payments in France, Insurance Journal, 9.5.2021, Internet: https://www.insurancejournal.com/news/international/2021/05/09/613255.htm (accessed 20.2.2023); Beck/Fleisher (n. 15). Zurich Insurance also thinks that cyberattacks are becoming difficult to cover, https://www.ictjournal.ch/news/2023-01-09/pour-le-patron-de-zurich-les-cyberattaques-ne-seront-bientot-plus-assurables (accessed 14.4.2023).

83 The Geneva Association, Report on Ransomware: An Insurance Market Perspective, 7.2022, Internet: https://www.genevaassociation.org/sites/default/files/ransomware_report_online.pdf (accessed 14.4.2023).

84 See on this topic Tim Starks, Experts suggest French insurer AXA's plan to shun ransomware payouts will set a precedent, Cyberscoop, 10.5.2021, Internet: https://www.cyberscoop.com/axa-ransomware-cyber-insurance-policies/ (accessed 14.4.2023).

85 For instance, in connection with certain compliance measures that often include certain payments. See Gerrit Hötzel, Ransomware: Lösegeldzahlung kann rechtswidrig sein, Voelker Gruppe, October 2020, Internet: https://www.voelker-gruppe.com/stuttgart/ransomware_zahlung_rechtswidrig/ (accessed 20.2.2023).

86 Benhamou/Wang (n. 2), 84 f.

87 *Ibidem*.

88 See for example art. 3 para. 2 of the Ordinance imposing measures against persons and entities and entities associated with Osama bin Laden, or art. 15 para. 2 of the Ordinance imposing measures in connection with the situation in Ukraine. We cannot exclude that criminal and terrorist organizations behind ransomware attacks could be part of the organizations to which it is prohibited to proceed to a payment, which could lead, intentionally or through negligence, to a criminal sanction based on art. 9 of the Federal Act on the Implementation of International Sanctions (Embargo Act).

attacks were already listed by the EU, e.g.: WannaCry, CryptoLocker, BitPaymer, Dridex and SamSam.[89] More recently, the United States and the United Kingdom issued joint cyber sanctions by designating seven individuals of the cybercrime gang Trickbot.[90]

Some governments have even taken an official stand on not paying ransomware. For example, the U.S. Department of Treasury's Office of Foreign Assets Control and the Financial Crimes Enforcement Network state that many cases of paying a ransom can be illegal.[91] Hence, the U.S. government officially discourages companies and citizens from paying ransom demands and would likely even sanction them if that payment might breach a U.S. provision. Furthermore, the U.S. Office of Foreign Assets Control's sanctions regime can have extraterritorial reach and could possibly even lead to fines and penalties if a sanctioned entity or individual is being paid.[92] Hence, although the U.S. Treasury Department's ruling for its part primarily affects U.S. law, it *can* also have an impact on companies outside the U.S., for example in Switzerland or other overseas countries. This is also the case, for instance, if a Swiss company has a subsidiary or assets in the U.S., or if it is otherwise involved in the U.S. market, e.g., by using U.S. suppliers or service providers, or selling goods and services there.[93]

Third and finally, paying a ransom can mean paying a criminal who might be considered a member of a terrorist or a criminal group, not only under Swiss national law but possibly also under another State's law. As other countries have similar legal landscapes, their legal consequences might apply to a (Swiss) payment that has concrete links to their jurisdiction. If imprudent, a victim (or any third party involved in a payment) might therefore not only violate an embargo provision[94] but might also end up risking illegally financing or supporting criminal or terroristic groups according to foreign law. As an example in this regard, the EU and the United Kingdom's legal landscapes hold certain risks: Although there is no general ban on ransom payments, a person or company may yet risk violating existing provisions relating to terrorism, anti-money laundering, or to countering the financing of terrorism if he or she provides money and knows or has reasonable cause to suspect that it will or may be used for these purposes. Thereby, however, the specific preconditions for the offences vary from country to country,[95] and for the criminal liability of a Swiss national under foreign law, the condition of double criminal liability is required.

Consequently, the interwovenness of transnationally operating businesses and supply chains as well as a mere international payment might indeed become relevant for a broader range of (Swiss and foreign) provisions. Therefore, even if a small company decides to pay a ransom in a given case, it could lead to bigger (international) issues.

III. Conclusion

As this article has shown, there are various problems stemming from ransomware that can potentially affect any natural or legal person alike. Thereby, apart from the vulnerability of organizations and companies to ransomware attacks in the first place, there are also certain risks when it comes to paying a ransom in the second place. Therefore, the respective *payments* of ransoms are a potentially far-reaching element that needs to be taken seriously. Given the severe consequences of ransomware (payments) for the broader economy, it is thus important to understand what (criminal) legal risks already exist. As Switzerland – alongside other governments – is currently in the process of evaluating how to best approach the ransomware problem,[96] it is also worth remembering that existing legal landscapes already provide relevant provisions in this context. Notwithstanding a specific ban, an organization paying a ransom hence already faces certain legal risks.

Although the legal situation regarding the risks for ransomware payments is not entirely clear, there *are*

---

89 As in the case of the EU, sanctions against eight people and four organizations involved in cyberattacks were extended, see Council of the EU, Press Release, 17.5.2021, Internet: https://www.consilium.europa.eu/de/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/ (accessed 10.7.2023).

90 U.S. Department of the Treasury, Press Release, 9.2.2023, Internet: https://home.treasury.gov/news/press-releases/jy1256 (accessed 14.4.2023).

91 See U.S. Department of the Treasury (n. 26); FinCEN, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, 8.11.2021, Internet: https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf (accessed 14.4.2023); Marañon/Wittes (n. 6).

92 See U.S. Department of the Treasury (n. 26).

93 Hötzel (n. 85), N 20.

94 *Ibidem*.

95 As opposed to the U.S., for instance, Swiss criminal law requires a certain degree of intention to commit an offence by paying a sanctioned actor. Furthermore, it is not always sure who the attacker is and to which country the payment is to be attributed according to the respective laws (if it is to a prohibited person in the U.S. or if it is to a criminal organization in Switzerland), U.S. Department of the Treasury (n. 26), 3; RANSOMWARE TASK FORCE (n. 10), 12.

96 See Postulate 21.4512 (n. 1).

legal – among other – risks that must be assessed when it comes to a ransomware payment. Depending on a given case, legal (and other) problems due to a ransomware payment may arise depending on who will be paid, by which means, through which party, and affecting which protected goods and interests. As the identity of a cybercriminal might not be ascertainable at the time of a payment, it is crucial to conduct diligent and forward-looking risk assessments that follow existing obligations.

As for the Swiss and the international legal context, there are not only contractual duties but also some key criminal legal provisions that need to be considered. Although unlikely, a payment could, at least in theory, violate Art. 260ter para. 1 lit. b CrimC if that payment is 1) made to a criminal organization which 2) the person paying the ransom must reasonably assume while 3) having no legal justification. This offence is relevant for both the victim and third parties that are involved in a payment. Also, as there are similar provisions in other countries, further risks stem from the international context.

Ultimately, when it comes to any decision about a ransomware payment, there is a whole number of existing risks that, of course, come on top of an already very sensitive and difficult situation. However, for the assessment of legal (contractual and criminal) risks, not only the respective international corporate structure and supply chain of the victim can become relevant, but also just a mere negligent *underestimation* of the possible consequences, even by a very small enterprise. As with many critical decisions, it is therefore very important to approach any such decision as to whether to pay or not to pay a ransom in a reasoned and informed manner.

All in all, however, the battle against ransomware will most likely not consist in trying to further punish an affected victim organization that desperately tries to save itself by paying a ransom. This article should have rather indicated and stressed the fact that such payments are part of a *bigger problem* that needs to be taken seriously in any decision-making process. Although there is no precedent yet, the imprudent handling of such risks could well be taken into consideration by prosecuting or supervisory authorities. Therefore, to avoid legal liabilities and before considering a ransomware payment to an (anonymous) cybercriminal, a diligent legal assessment and prior consultation with the responsible authorities may be indicated in any case.