

Ransomvér a úhrada výkupného v kontexte trestného práva*

Ransomware and Ransom Payments in the Context of Criminal Law

Jozef Čentés**, Michal Rampášek***

Abstrakt

Článok poskytuje systematický prehľad kľúčových právnych aspektov úhrad výkupného pri ransomvérových útokoch z pohľadu českého a slovenského trestného práva. Po úvode, sa v druhej kapitole sumarizuje doterajší výskum v tejto oblasti. Následne tretia kapitola približuje fenomén ransomvéru, so zameraním na model Ransomware-as-a-Service (RaaS) a jeho technicko-ekonomické pozadie. Štvrtá kapitola analyzuje mechanizmy legalizácie výkupného, najmä prostredníctvom kryptomien a anonymizačných nástrojov. Piata kapitola sa venuje právnym dôsledkom úhrady výkupného, vrátane možného porušenia sankčných režimov EÚ a trestnoprávných rizík, ako je legalizácia výnosov z trestnej činnosti či financovanie terorizmu. Na záver sú rozobrané ďalšie riziká spojené s platbami výkupného a rámec pre rozhodovací proces poškodených s dôrazom na compliance a riadenie rizík.

Kľúčová slova

Ransomvér; výkupné; trestné právo; legalizácia výnosov; sankcie; financovanie terorizmu; compliance a riadenie rizík.

Abstract

This article provides a structured overview of the key legal aspects of ransom payments in the context of ransomware attacks from the Czech and Slovak criminal law perspective. After introduction, the second section summarizes existing and recent research on the topic. The third section introduces the concept of ransomware, with a special focus on the Ransomware-as-a-Service (RaaS) model, and explores its technical and economic underpinnings. The fourth section analyses the laundering of ransom proceeds, particularly via cryptocurrencies and anonymization tools. The fifth section

* Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00002 (Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality).

** Prof. JUDr. Jozef Čentés, DrSc., Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta, Univerzita Komenského v Bratislave, Slovenská republika / Department of Criminal Law, Criminology and Criminalistics, Faculty of Law, Comenius University in Bratislava, Slovak Republic / E-mail: jozef.centes@flaw.uniba.sk / ORCID: 0000-0003-3397-746X / Scopus ID: 57205550015

*** JUDr. Michal Rampášek, doktorand, Katedra trestného práva, kriminológie a kriminalistiky, Právnická fakulta, Univerzita Komenského v Bratislave, Slovenská republika; advokát / PhD. student, Department of Criminal Law, Criminology and Criminalistics, Faculty of Law, Comenius University in Bratislava, Slovak Republic; Attorney / E-mail: rampasek1@uniba.sk / ORCID: 0009-0006-6997-0250 / Scopus ID: 59404668600

examines the legal implications of ransom payments, including potential violations of EU sanctions regimes and the risk of committing money laundering or terrorism financing offences under criminal law. Finally, the article discusses other risks associated with ransom payments and a formal decision-making framework for victims, emphasizing compliance duties and risk management procedures.

Keywords

Ransomware; Ransom Payment; Criminal Law; Money Laundering; Sanctions; Terrorist Financing; Compliance and Risk Management.

Úvod

Právne aspekty platieb výkupného (v anglickom originály „ransom“) pri ransomvérových útokoch zostávajú zložitou a spornou témou, v ktorej sa prelínajú regulačné, etické a právne aspekty. Hoci sa platenie výkupného vo všeobecnosti neodporúča, nie je *per se* trestným činom. Naša analýza relevantných ustanovení slovenského Trestného zákona¹ a českého trestního zákoníka² však poukazuje na možné právne riziká spojené s úhradou výkupného z hľadiska porušenia sankcií v oblasti kybernetických útokov v EÚ, ako aj vybraných trestných činov – legalizácie výnosov z trestnej činnosti a trestného činu financovania terorizmu.

S cieľom poskytnúť komplexný prehľad je tento článok štruktúrovaný do šiestich kapitol, ktoré sa zaoberajú kľúčovými prvkami tejto naliehavej problematiky. Po prvej úvodnej kapitole, sa v druhej kapitole venujeme doterajším a najnovším článkom v oblasti posudzovania platieb výkupného pri ransomvérovom útoku v oblasti trestného práva. V tretej kapitole predstavujeme pojem ransomware (v slovenskom tvare „ransomvér“) s osobitným dôrazom na model ransomvér ako služba (*Ransomware-as-a-Service* – RaaS). Štvrtá kapitola sa zameriava na zložitosti platieb ransomu a metódy používané na pranie týchto platieb, najmä v kontexte kryptomien. Uhradiť či neuhradiť? Alebo vyjednávať? To sú otázky na ktoré sa pokúsime zodpovedať v rámci kľúčovej piatej kapitoly, kde sa venujeme právnym aspektom úhrady výkupného. V závere sa pozornosť presúva na rozhodovací proces, ktorý by mali poškodení ransomvérovým útokom dodržiavať pri zvažovaní platieb výkupného, pričom zdôrazňujeme povinnosti dodržiavania predpisov (compliance) a postupy riadenia rizík.

Kybernetický bezpečnostný incident (ďalej „incident“) spôsobený ransomvérovým útokom môže pre zasiahnutú právnickú osobu znamenať nemalé náklady. Spoločnosť IBM poukazuje na úspory nákladov pre poškodených pri zapojení orgánov činných v trestnom konaní po ransomvérových útokoch.³ Obete ransomvéru, ktoré zapojili orgány činné v trestnom konaní, celovo znížili náklady za narušenie v priemere o takmer 1 milión USD, a to bez nákladov na zaplatenie výkupného. Zapojenie týchto orgánov tiež pomohlo skrátiť čas potrebný na identifikáciu a zvládnutie narušenia z 297 dní na 281 dní. Priemerné náklady

¹ Zákon č. 300/2005 Z.z. Trestný zákon v znení neskorších predpisov.

² Zákon č. 40/2009 Zb. v znení pozdějších predpisů.

³ Cost of a Data Breach Report 2024. IBM [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>

na incident sa pohybovali od 4,38 milióna USD so zapojením orgánov činných v trestnom konaní, do 5,37 milióna USD bez zapojenia orgánov činných v trestnom konaní, čo predstavuje rozdiel v nákladoch viac ako 20 %. Tieto údaje o nákladoch nezahŕňajú platby samotného výkupného. Podľa dostupných informácií 52 % obetí šifrovania nahlásilo incident orgánom činným v trestnom konaní a 63 % z nich nezaplatilo výkupné. Údaje spoločnosti IBM sú presvedčivým argumentom v prospech zapojenia orgánov činných v trestnom konaní po ransomvérovom útoku. Je to aj tým, že orgány činné v trestnom konaní vyvinuli nástroje na dešifrovanie, ktoré pomáhajú poškodeným obnoviť ich zašifrované súbory, a zároveň majú prístup k odborným znalostiam a zdrojom v procese obnovy.⁴

Podľa analýzy spoločnosti Chainalysis došlo v roku 2024 k poklesu platieb výkupného za ransomvér o 35 % v porovnaní s rokom 2023, ktorý bol rekordný. Hoci prvá polovica roka 2024 naznačovala, že objem platieb prekročí úroveň z predchádzajúceho roka⁵, v druhej polovici došlo k výraznému poklesu. Zníženie platieb súviselo s úspešnými zásahmi orgánov činných v trestnom konaní a rastúcou neochotou poškodených platiť výkupné. Celkové príjmy z ransomvéru klesli na približne 813,55 milióna USD, čo je o 35 % menej oproti 1,25 miliardy USD v roku 2023, pričom ide o prvý pokles od roku 2022.⁶

1 Doterajšie vedecké spracovanie platby výkupného

V rámci systematického prehľadu literatúry sa zameriavame na priblíženie fenoménu ransomvéru a platby výkupného v kontexte trestného práva, súvisiaceho regulačného rámca, identifikáciu problémov, medzier a výskumných príležitostí v tejto oblasti, ako aj na vytvorenie výskumného rámca, ktorý môže podporiť budúce skúmanie v danej oblasti. Vzhľadom na nerozpracovanosť zvolenej témy v domácej odbornej literatúre, sme vykonali analýzu predovšetkým zahraničnej odbornej literatúry (meta analýzu) prostredníctvom troch primárnych zdrojov, a to v časovo neohraňčenom období. Primárne zdroje tvorila databáza SCOPUS, ISI (Web of Science), a arXiv. Prehľad sa zameriava na problematiku osobitostí ransomvéru, faktorov vedúcich k (ne)uhradeniu výkupného, vrátane mechanizmov úhrady, dôsledkov pre poškodeného, ako aj celkového dopadu na ekosystém kybernetickej bezpečnosti. Osobitne nás zaujímala literatúra súvisiaca so zameraním na to, ako sa plnenie povinností v oblasti regulácie kybernetickej bezpečnosti (najmä prevencia a hlásenie kybernetických bezpečnostných incidentov) zohľadňuje zo strany orgánov činných v trestnom konaní, príp. iného štátneho orgánu, pri prípadnej úhrade vykúpeného poškodeným. Hlavnou použitou metódou výskumu je analytická metóda, prostredníctvom ktorej identifikujeme

⁴ Napr. COKER, J. Law Enforcement Confirms BlackCat Take Down, Decryption Key Offered to Victims. *Infosecurity Magazine* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.infosecurity-magazine.com/news/law-enforcement-blackcat-decryption/>

⁵ Najmä v dôsledku rekordnej platby výkupného vo výške 75 miliónov USD, pozri WINDER, D. Record-Breaking \$75 Million Ransom Paid To Dark Angels Gang. *Forbes* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.forbes.com/sites/daveywinder/2024/07/31/record-breaking-75-million-ransom-paid-to-dark-angels-gang/>

⁶ Chainalysis Report: 35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments. *Chainalysis* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/>

kľúčové ustanovenia a právne pojmy, porovnávame podobnosti, rozdiely a medzery medzi jednotlivými nástrojmi v boji proti ransomvéru a prostredníctvom analýzy dospievame ku konceptuálnemu uchopeniu súčasného právneho prostredia.

Meurs et al. považujú zákaz platieb výkupného, pokiaľ zvyšuje náklady na právne služby a pokuty, za prospešný, pretože znižuje zisk útočníkov. Zákonný zákaz by však mohol znížiť platby výkupného pod úroveň a znížiť náklady na právne služby pretože poškodení už nebudú vyhľadávať rady právnikov a vyjednávačov. Skúmanie efektu utajeného platenia výkupného na sociálny blahobyt by mohlo byť podľa týchto autorov cenným smerom budúceho výskumu. Zvýšenie nákladov na právne služby, ktoré by mohlo zahŕňať nielen náklady na právne služby, ale aj náklady na odborníkov na vyjednávanie a psychológiu, teda znižuje výšku výkupného. Vysoké náklady narušajú zisk útočníkov. Neprinášajú však prospech poškodenému, pretože znamenajú len to, že platí náklady namiesto výkupného. Jedným zo spôsobov, ako o tom uvažovať zo spoločenského hľadiska, je regulácia (okrem zákazu platieb). Vyššia úroveň regulácie (napr. starostlivo presadzované sankčné zoznamy alebo požiadavky na oznamovanie útokov orgánom činným v trestnom konaní) by mala za následok zvýšenie nákladov na právne služby. Ideálnym riešením by bolo znížiť platby výkupného bez toho, aby platby výkupného boli realizované neoficiálnymi, skrytými spôsobmi.⁷ Inak povedané, poškodení ransomvérovými útokmi by nemali byť motivovaní obchádzať oficiálne alebo legálne postupy pri riešení týchto incidentov.

Podľa Agentúry Európskej únie pre kybernetickú bezpečnosť (*European Network and Information Security Agency – ENISA*), keď sa platby uskutočnia, často nedosahujú pôvodne požadované sumy, čo naznačuje, že poškodení použili úspešnú vyjednávaciu taktiku. K tomuto vývoju prispieva niekoľko faktorov. Zdokonalené opatrenia kybernetickej bezpečnosti vrátane stratégií zálohovania a obnovy umožnili právnickým osobám odolávať ransomvérovým útokom bez potreby uhradiť výkupné. Okrem toho zintenzívnené úsilie orgánov činných v trestnom konaní proti ransomvérovým skupinám vytvorilo pre kyberzločincov nepriateľskejšie prostredie. Keďže si poškodení viac uvedomujú potenciálne dôsledky platenia výkupného, ako je opätovná kompromitácia a financovanie nezákonných aktivít, čoraz častejšie sa rozhodujú pre alternatívne spôsoby obnovy. Hoci celkový obraz naznačuje rastúcu neochotu platiť výkupné, realita zostáva zložitá. Rozhodnutie zaplatiť alebo nezaplatiť je ovplyvnené rôznymi faktormi vrátane povahy činnosti, kritickosti zašifrovaných údajov a tolerancie právnickej osoby voči riziku.⁸

Connolly a Borrion vo svojej práci analyzovali rozhodovacie procesy poškodených počas štyridsaťjeden ransomvérových útokov pomocou kvalitatívnych údajov zozbieraných od právnických osôb a policajtov z jednotiek pre boj proti počítačovej kriminalite v Spojenom kráľovstve. Z ich zistení vyplýva, že existujú dôvody, prečo sa napadnuté právnické osoby môžu rozhodnúť zaplatiť výkupné, aj keď majú zálohy. Mnohé z týchto dôvodov sa dajú

⁷ MEURS, T. a kol. Deception in double extortion ransomware attacks: An analysis of profitability and credibility. *Computers & Security* [online]. 2024, roč. 138, č. 103670. ISSN 0167-4048 [cit. 9. 4. 2025]. Dostupné z: <https://doi.org/10.1016/j.cose.2023.103670>

⁸ Threat Landscape 2024 report. *ENISA* [online]. 2024, s. 53 [cit. 9. 4. 2025]. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

pochopiť prostredníctvom finančnej analýzy a súvisia s účinnosťou, rýchlosťou, náročnosťou a nákladmi na obnovu, ako aj s rizikom poškodenia dobrej povesti a možnými pokutami od regulačných orgánov. Zistenia tiež odhalili aj menej predvídateľné prvky, ktoré môžu zohrávať dôležitú úlohu pri rozhodovaní (ne)zaplatiť výkupné: nedostatok vedomostí, zlé poradenstvo, tajné dohody, morálka, pocit zodpovednosti, tlak, neistota a dôvera.⁹

Iná štúdia z Holandska uskutočnená medzi 445 majiteľmi a manažérmi holandských malých a stredných obchodných spoločností ukázala, že pravdepodobnosť zaplata výkupného je nízka. Hoci sa zdá, že cenová dostupnosť požiadavky na výkupné nesúvisí s pravdepodobnosťou zaplata výkupného, odporúčanie spoločnosti zaoberajúcej sa kybernetickou bezpečnosťou zaplatiť výkupné a neexistencia záloh výrazne zvyšuje pravdepodobnosť zaplata výkupného.¹⁰

Za podstatnú okolnosť považujeme riešiť príčinu problému a nielen jeho príznaky. Platenie výkupného nie je jediným problémom, a možno ani tým hlavným. Podľa autorov Robles-Carrillo et al. najväčší problém spočíva v tom, že mnohí z poškodených nevyužívajú existujúce právne prostriedky na nahlásenie útoku a sťažanie trestného činu. Okrem toho, okrem tendencie riešiť problém mimo zákona, sa ransomvér stal biznisom pre poisťovne. Uzatvorenie poisťovej zmluvy na prípadný ransomvér sa rovná poskytnutiu právnej záruky platby za spáchanie nezákonnej protiprávnej činnosti. Navyše je to dodatočná motivácia k páchaniu trestnej činnosti, pretože ak poškodený nemôže zaplatiť, poisťovňa zaplatí.¹¹

Abely tvrdí, že neexistencia všeobecného federálneho zákazu platieb výkupného narušá účel a účinnosť sankčného režimu USA. Program sankcií USA v oblasti kybernetických útokov trpí zásadným problémom načasovania: platby útočníkom sú často zakázané až po tom, ako boli títo zaradení na zoznam osobitne označených osôb a blokových osôb (*Specially Designated Nationals and Blocked Persons List* – SDN), ktorý vedie Úrad pre kontrolu zahraničných aktív (*Office of Foreign Assets Control* – OFAC) na ministerstve financií USA.¹² Okrem všeobecného zákazu úhrady výkupného boli navrhnuté aj iné riešenia. Westbrook napríklad navrhla podmienky beztrestnosti, tzv. bezpečný prístav (*safe harbor*) pre platby pri ransomvérových útokoch, ktorý by slúžil aj na prevenciu útokov a umožnil ich zastavenie.¹³

- ⁹ CONNOLLY, A. Y., BORRION, H. Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Computers & Security* [online]. 2022, roč. 119, č. 102760. ISSN 0167-4048 [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1016/j.cose.2022.102760>
- ¹⁰ MATTHIJSSE, S. R., MONEVA, A., VAN 'T HOFF-DE GOEDE, M. S., LEUKFELDT, E. R. Examining ransomware payment decision-making among small- and medium-sized enterprises. *European Journal of Criminology* [online]. 2024 [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1177/14773708241285671>
- ¹¹ ROBLES-CARRILLO, M., GARCÍA-TEODORO, P. Ransomware: An Interdisciplinary Technical and Legal Approach. *Security and Communication Networks* [online]. 2022, č. 2806605, 17 s. [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1155/2022/2806605>
- ¹² CHRISTINE, A. Ransomware, Cyber Sanctions, and the Problem of Timing. *Boston College Law Review* [online]. 2022, roč. 63, E. SUPP [cit. 9. 4. 2025]. Dostupné z: <https://bclawreview.bc.edu/articles/64>
- ¹³ WESTBROOK, A. A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security. *New York University Journal of Law and Business* [online]. 2022, roč. 18, č. 2 [cit. 9. 4. 2025]. DOI: <http://doi.org/10.2139/ssrn.3899370>

2 Ransomvér a obchodný model RaaS

Ransomvér je typ škodlivého softvéru (malvér), ktorý útočníci (páchatelia) vyvíjajú a/alebo používajú na zamedzenie prístupu k údajom, systémom alebo sieťam a požadujú zaň výkupné. Medzi bežné metódy útoku patrí šifrovanie údajov, exfiltrácia údajov a narušenie prevádzky obete. Útoky často zahŕňajú viac ako jednu metódu a môžu zahŕňať hrozbu zverejnenia údajov poškodeného.¹⁴

Útočníci sa často zameriavajú na právnické osoby s vysokou hodnotou alebo právnické osoby, o ktorých si myslia, že je pravdepodobnejšie, že zaplatia výkupné, aby obnovili obchodné operácie alebo sa vyhli kontrole. Selektívne sa zameriavajú aj na právnické osoby pôsobiace v dodávateľských reťazcoch typu just-in-time, u ktorých je pravdepodobnejšie, že budú mať vyššie náklady na výpadok, ako aj na kritickú infraštruktúru alebo na tie, ktoré majú citlivé alebo cenné informácie. Útočníci môžu vyhodnotiť, že tieto právnické osoby majú v porovnaní s ostatnými väčšiu tendenciu platiť výkupné.

Ransomvér ako služba (RaaS) označuje protiprávny obchodný model, v rámci ktorého útočníci poskytujú balíky ransomvérového softvéru na Dark webe alebo externe zabezpečujú prvky ransomvérových útokov vrátane distribúcie škodlivého softvéru, počiatočnej kompromitácie siete obete, exfiltrácie údajov alebo vyjednávania o výkupnom pre pridružené spoločnosti výmenou za poplatok a/alebo percento z výkupného. Páchatelia si môžu zakúpiť aj odcudzené údaje (credentials) na prístup k systémom poškodeného a ich zneužitie, čo umožní distribúciu ransomvéru, a môžu tiež získať spravodajské informácie týkajúce sa konkrétnych odvetví v konkrétnych jurisdikciách, aby sa mohli zamerať na svoje ciele a maximalizovať účinnosť svojho útoku. Model RaaS znížil náklady a potrebné technické znalosti na vykonávanie útokov, čím sa znížili bariéry vstupu a umožnilo sa menej sofistikovanejším zločincom vykonávať ransomvérové útoky.

V rámci postupu útočníkov po úspešnom prieniku do systému a siete obete sa vyvinulo niekoľko spôsobov či úrovní vydierania tejto obete.

Dvojité vydieranie (*double-extortion*) označuje postup, pri ktorom útočníci pred zašifrovaním údajov obete exfiltrujú údaje a potom hrozia zverejnením odcudzených údajov, ak nebudú splnené požiadavky na výkupné. Táto hrozba zverejnenia dopĺňa hrozbu týkajúcu sa napadnutého systému. Táto taktika môže na poškodených vyvinúť ďalší tlak, aby zaplatili požiadavky na výkupné, aj keď sa im podarí obnoviť prevádzku.

Trojité vydieranie (*triple-extortion*) sa vzťahuje na postup, pri ktorom útočníci požadujú peniaze nielen od poškodeného, ktorý bol prvým cieľom, ale aj od poškodených, ktorí by mohli byť ovplyvnení zverejnením údajov pôvodného (cieľového) poškodeného, ako sú citlivé zdravotné údaje, osobné údaje, údaje k účtu a duševné vlastníctvo.

Viacnásobné vydieranie (*multiple-extortion*) sa vzťahuje na postupy, ktoré zahŕňajú viac ako dva spôsoby vydierania. Vychádza z dvojitého vydierania pomocou šifrovania a exfiltrácie,

¹⁴ Report: Countering Ransomware Financing. *Financial Action Task Force (FATF)* [online]. Marec 2023 [cit. 9. 4. 2025]. Dostupné z: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf>

ale zahŕňa aj ďalšie nátlakové taktiky, ako je distribuované odmietnutie služby (DDoS), kontaktovanie zákazníkov poškodených a narušenie ich infraštruktúry.

Čoraz viac prípadov, kde za ransomvérovým útokom je primárny dôvod nenápadná exfiltrácia dát. V týchto prípadoch je požiadavka na výkupné často úplne nepodstatná. Takéto krytie ransomvérom je využívané štátnymi hráčmi resp. skupinami sponzorovaným štátmi, či zločineckými skupinami zameranými na priemyselnú špionáž.¹⁵

Vznikajú tiež nové skupiny. Zo štatistik vyplýva, že v prvom polroku 2024 bolo v činnosti 73 ransomvérových skupín v porovnaní so 46 skupinami v prvom polroku 2023, čo predstavuje 56-percentný nárast počtu ransomvérových skupín. Hoci sa skupiny zmenili, trendy zostali rovnaké. Je pozoruhodné, že veľké skupiny¹⁶ vykonávajú operácie typu RaaS, čo znamená, že prenajímajú svoj ransomvér spolupracujúcim skupinám na vykonávanie útokov výmenou za percento z výnosov. Tento model je v súčasnosti v ekosystéme ransomvéru veľmi aplikovaný a medzi najaktívnejšími skupinami jednoznačne naďalej dominuje.¹⁷

3 Spôsoby platby výkupného a regulácia trhu s kryptoaktívami

V kontexte ransomvérových útokov a výkupného, platby často prebiehajú prostredníctvom anonymných alebo ťažko sledovateľných finančných technológií, najmä kryptomien. Táto anonymita a globalizácia platobných kanálov sťažujú tradičným orgánom činným v trestnom konaní ich detekciu a reguláciu. Z toho dôvodu je nutné analyzovať platby výkupného nielen z hľadiska ich bezprostredných následkov, ale aj ich možných dlhodobých dopadov na finančný systém, legislatívu a medzinárodnú bezpečnosť.

Legalizovanie ransomvérových platieb má predovšetkým nadnárodný charakter vzhľadom na cezhraničnú povahu virtuálnych aktív, v ktorých sa ransomvérové platby takmer vždy uskutočňujú.¹⁸ Používatelia virtuálnych aktív môžu uskutočňovať peer-to-peer transakcie priamo medzi sebou, pričom používajú len svoj súkromný kľúč a internetové pripojenie, bez ohľadu na geografické hranice a bez zapojenia inštitúcií s povinnosťami v oblasti boja proti legalizácii výnosov z trestnej činnosti a financovaniu terorizmu (AML/CFT). Útočníci môžu využívať tieto vlastnosti virtuálnych aktív na uľahčenie rozsiahlych, takmer okamžitých cezhraničných transakcií bez tradičných finančných sprostredkovateľov, ktorí majú programy AML/CFT. Majú tiež prístup k poskytovateľom služieb virtuálnych aktív so sídlom po celom svete v jurisdikciách so slabými alebo neexistujúcimi kontrolami AML/CFT, ktoré páchatelia využívajú na speňaženie svojich nezákonných príjmov vo fiat mene.¹⁹

¹⁵ CONNOLLY, L.Y., WALL, D.S., LANG, M., ODDSON, B. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1, tyaa023 [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1093/cybsec/tyaa023>

¹⁶ V prvej polovici roka 2024 bola činnosť skupiny LockBit vážne narušená v dôsledku rozsiahlej operácie orgánov činných v trestnom konaní pod názvom „Cronos.“ Medzi ďalšie skupiny patria RansomHub, 8Base, BlackBasta a Play.

¹⁷ Ransomware in H1 2024: Trends from the Dark web. *Searchlight Cyber* [online]. S. 4 a 7 [cit. 9. 4. 2025]. Dostupné z: <https://slyber.io/whitepapers-reports/ransomware-in-h1-2024-trends-from-the-dark-web/>

¹⁸ Countering Ransomware Financing. *FATF* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html>

¹⁹ Ibid.

Po prijatí požiadavky na výkupné poškodený alebo tretia strana konajúca v jeho mene zvyčajne pošle finančné prostriedky prostredníctvom bankového prevodu, automatizovaného zúčtovacieho strediska alebo platby kreditnou kartou poskytovateľovi služieb virtuálnych aktív na nákup typu a sumy virtuálneho aktíva určeného útočníkmi; je potrebné dodať v súvislosti s platobnými kartami, že v ostatnom období sa do popredia dostávajú taktiež zneužitia platobných kariet podporujúcich RFID technológie.²⁰ Medzi tretie strany, ktoré konajú v mene poškodeného ransomvérovým útokom, môžu patriť spoločnosti zaoberajúce sa reakciou na incidenty alebo kyberpoistením. Následne odošlú platbu výkupného, často z peňaženky umiestnenej v službe poskytovateľa služieb virtuálnych aktív, na adresu virtuálnych aktív páchatel'a. Zvyčajne ide o nehostovanú peňaženku (softvér alebo hardvér, ktorý umožňuje používateľom držať, uchovávať a prenášať virtuálne aktíva mimo tretej strany, napr. poskytovateľa služieb virtuálnych aktív; označuje sa aj ako nehostovaná peňaženka), ktorú kontroluje páchatel' alebo sprostredkovateľ, alebo o peňaženku hostovanú poskytovateľom služieb virtuálnych aktív, ktorá sa nachádza mimo jurisdikcie, kde došlo k útoku, a ktorá zvyčajne nespoločňuje so štátnymi orgánmi, teda najmä finančnými spravodajskými jednotkami.

MiCA²¹ významne ovplyvňuje platby výkupného pri ransomvérových útokoch tým, že ukladá prísne požiadavky na poskytovateľov služieb kryptoaktív (*Crypto-asset service provider, CASP*), čím obmedzuje anonymitu transakcií a znižuje atraktivitu kryptomien pre trestnú činnosť. Podľa nariadenia MiCA kryptoaktívum je digitálne vyjadrenie hodnoty alebo práva, ktoré možno prevádzať a elektronicky uchovávať použitím technológie distribuovanej databázy transakcií alebo podobnej technológie. Jedným z kľúčových opatrení MiCA je povinnosť vykonávať dôsledné overovanie klientov a monitorovanie transakcií. To znamená, že prevádzkovatelia búrz, peňažieniek a ďalších služieb musia identifikovať používateľov a sledovať podozrivé transakcie.²² Vďaka týmto mechanizmom je jednoduchšie sledovanie platieb výkupného a identifikovanie príjemcov, čo zvyšuje šance na ich odhalenie.

Ďalším dôležitým aspektom je pravidelné hlásenie o platbách súvisiacich s ransomvérom. MiCA vyžaduje, aby Európska komisia predložila správu o aplikácii MiCA, ktorá musí obsahovať údaje o počte a hodnote transakcií spojených s ransomvérovými útokmi.²³ Tento mechanizmus poskytuje cenné informácie pre orgány činné v trestnom konaní a regulátorov, čo umožňuje lepšie pochopenie trendov a vývoj stratégií na boj proti ransomvéru.

MiCA tiež zaväzuje poskytovateľov služieb kryptoaktív, ktorí držia kryptoaktíva svojich klientov, aby zabezpečili ich ochranu a zabránili ich zneužitiu. Poskytovatelia služieb kryptoaktív, ktorí poskytujú úschovu a správu kryptoaktív v mene klientov, by mali uzavrieť zmluvu so svojimi klientmi s určitými povinnými ustanoveniami a mali by zaviesť a vykonávať

²⁰ KLIMEK, L. Misuse of contactless payment cards with radio-frequency identification. *Masaryk University Journal of Law and Technology* [online]. 2020, roč. 14, č. 2, s. 259–274. DOI: <https://doi.org/10.5817/MUJLT2020-2-5>

²¹ Čl. 3 ods. 1 bod 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 2023/1114 o trhoch s kryptoaktívami (ďalej „MiCA“).

²² Článok 62 ods. 2 písm. (i), článok 76 ods. 1 písm. (a), ods. 7 písm. (h) MiCA.

²³ Článok 140 MiCA.

politiku úschovy.²⁴ Toto opatrenie sťažuje útočníkom prevod a konverziu získaných výkupných platieb na fiat meny, čím sa znižuje motivácia požadovať platby v kryptomenách.

4 Právne aspekty platenia výkupného

Hoci platba výkupného *per se* nie je nezákonná v kontexte Trestného zákona, resp. trestného zákoníku²⁵, v závislosti od toho, komu a za akých okolností sa peniaze vyplácajú, existuje riziko spáchania trestného činu legalizácie výnosu z trestnej činnosti alebo trestného činu financovania terorizmu. Navyiac je v kontexte ostatných zmien Trestného zákona potrebné venovať pozornosť trestnoprávnym aspektom porušenia medzinárodných či európskych sankcií.²⁶

Slovensko a tiež Česká republika sú členmi medzinárodnej iniciatívy proti ransomvéru (*Counter Ransomware Initiative* – CRI)²⁷, ktorá zohráva kľúčovú úlohu v celosvetovom boji proti ransomvéru. Prípojením sa k CRI oba štáty zvyšujú svoju kolektívnu odolnosť a profitujú z medzinárodnej spolupráce pri odhaľovaní, narúšaní a odrádzaní od aktivít ransomvéru. Toto členstvo zaväzuje právnické osoby a orgány verejnej moci dodržiavať osvedčené postupy a usmernenia CRI, ktoré kladú dôraz na posilnenie infraštruktúr kybernetickej bezpečnosti a podporu spoľahlivých mechanizmov výmeny informácií. Okrem toho sa oba štáty pripájajú k postoju CRI proti platbám výkupného a nabáda organizácie, aby uprednostnili obnovu údajov a integritu systému pred finančnými transakciami s kyberzločincami.²⁸

V tejto súvislosti nás zaujal návrh ministerstva vnútra Spojeného kráľovstva (the Home Office) z januára 2025, ktorým sa plánuje prijať právne predpisy na boj proti ransomvéru, s cieľom *inter alia* znížiť objem peňazí, ktoré prúdia k páchatelom ransomvéru zo Spojeného kráľovstva, a tým odradiť páchatelov od útokov na právnické osoby v Spojenom kráľovstve.²⁹ Ide o návrh cieleného zákazu platieb výkupného pre všetky orgány verejného sektora

²⁴ Recitál č. 83, článok 75 MiCA.

²⁵ Poukazujeme tiež na rozsudok anglického odvolacieho súdu (Court of Appeal) vo veci *Masefield AG proti Amlin Corporate Member Ltd* [2011] EWCA Civ 24 (v kontexte pirátstva) ktorý potvrdil, že zaplatenie výkupného nie je v rozpore s verejným poriadkom, a uviedol, že „*neexistuje žiadna všeobecne uznávaná zásada morálky, žiadny jasne identifikovaný verejný poriadok, žiadny v podstate nespochybniteľný verejný záujem, ktorý by mohol viesť súdy k tomu, aby za súčasného stavu vecí konštatovali, že zaplatenie výkupného by sa malo považovať za vec, ktorá stojí mimo rámca, bez akéhokoľvek legitímneho uznanja. Existujú len prvky protichodných verejných záujmov, ktoré sa presúvajú rôznymi smermi a ktoré ešte neboli vyriešené žiadnymi právnymi predpismi alebo medzinárodným konsenzom, pokiaľ ide o riešenie*“.

²⁶ Zákonom č. 157/2025 Z.z. ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon, sa o.i. zavádza nový trestný čin Porušenie reštriktívneho opatrenia podľa § 417a

²⁷ Medzinárodná iniciatíva na boj proti ransomvéru. *SK-CERT* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.sk-cert.sk/sk/rady-a-navody/ransomware/medzinarodna-iniciativa-na-boj-proti-ransomveru/index.html>

²⁸ CRI joint statement on ransomware payments 2023. *GOV.UK* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.gov.uk/government/publications/cri-joint-statement-on-ransomware-payments>

²⁹ Open consultation Ransomware: proposals to increase incident reporting and reduce payments to criminals. *GOV.UK* [online]. 14. 1. 2025 [cit. 9. 4. 2025]. Dostupné z: <https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals>. Konzultácie preukázali silnú podporu cielenému zákazu platieb výkupného. Na základe stanoviska britskej vlády zo dňa 22. 7. 2025 bude vláda naďalej pracovať na tomto návrhu. Dostupné z: https://assets.publishing.service.gov.uk/media/6899a4ddad0cbc0e276431e3/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf [cit. 26. 9. 2025].

vrátane miestnej samosprávy a pre vlastníkov a prevádzkovateľov kritickej infraštruktúry. Ministerstvo vnútra však tiež skúma možnosti, či by sa mal tento zákaz vzťahovať aj na kľúčových dodávateľov pre tieto sektory. Tiež navrhuje zaviesť režim prevencie platieb, ktorý by vyžadoval, aby sa každý poškodený ransomvérovým útokom (právnická osoba a/alebo jednotlivci, na ktorých sa nevzťahuje navrhovaný zákaz uvedený v prvom opatrení) spojila s orgánmi verejnej moci a oznámila svoj úmysel vykonať platbu výkupného predtým, ako zaplatí akékoľvek peniaze zločincovi. Po nahlásení by potenciálny poškodený dostal podporu a usmernenie – vrátane diskusie o možnostiach riešenia neplatenia, a orgány by preskúmali navrhovanú platbu, aby zistili, či existuje dôvod, prečo ju treba zablokovať, napr. ak by mohla ísť zločincovi, na ktorých sa vzťahujú sankcie, alebo porušujú právne predpisy o financovaní terorizmu. Ak by navrhovaná platba nebola zablokovaná, bolo by na poškodenom, či bude pokračovať.³⁰ Britské ministerstvo vnútra tiež navrhuje zaviesť povinnosť obete oznámiť ransomvérový incident, pričom prvotné oznámenie by malo byť vykonané do 72 hodín od zistenia incidentu.³¹

V Európskom akčnom pláne pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti,³² Európska komisia požaduje po členských štátoch, aby od subjektov, na ktoré sa vzťahuje smernica NIS2, vrátane zdravotníckych organizácií, požadovali, aby spolu s ďalšími informáciami, ktoré poskytujú pri podávaní správ o závažných incidentoch, podávali správy o všetkých uskutočnených platbách výkupného a o platbách výkupného, ktoré plánujú uskutočniť. Takéto hlásenie má podľa Európskej komisie podporiť účinné vyšetrowanie incidentov s výkupným vrátane sledovania platieb na platformách výmeny kryptomien s cieľom identifikovať príjemcov.³³

Zvýrazňujeme, že ransomvérový útok môže predstavovať závažný incident³⁴, resp. incident s významným dopadom³⁵, najmä ak spôsobí vážne narušenie činnosti kritických služieb alebo významné škody tretím osobám, čím napĺňa znaky závažného incidentu resp. významného dopadu. Príkladom sú útoky na nemocnice, kde dôsledky môžu byť obzvlášť závažné, kde ransomvérový útok môže viesť k zablokovaniu prístupu k online službám³⁶, znemožniť objednávanie pacientov alebo dokonca znemožniť výkon operácií, čo priamo ohrozuje zdravie a životy pacientov.³⁷

³⁰ Open consultation Ransomware: proposals to increase incident reporting and reduce payments to criminals, op. cit., s. 19 (body 51 a 52).

³¹ Ibid., s. 22, 23.

³² Európsky akčný plán pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti. *Shaping Europe's digital future* [online]. 15. 1. 2025 [cit. 9. 4. 2025]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers>

³³ Ibid., s. 14.

³⁴ § 24 ods. 2 slovenského zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti v platnom znení (ďalej „SZoKB“).

³⁵ § 16 ods. 2 českého zákona č. 264/2025 Sb. o kybernetickej bezpečnosti (ďalej „ČZoKB“).

³⁶ Rumunské nemocnice napadnuté ransomvérom. *NBÚ* [online]. 13. 2. 2024 [cit. 9. 4. 2025]. Dostupné z: <https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom>

³⁷ KOBZOVÁ, L. Odkládání velkých operací, zpoždění zákroků, dokonce i úmrtí. Takové jsou dopady kyberútoků na nemocnice. *ZIVĚ.CZ* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.zive.cz/clanky/odkladani-velkych-operaci-zpozdeni-zakroku-dokonce-i-umrti-takove-jsou-dopady-kyberutoku-na-nemocnice/sc-3-a-228769/default.asp>

Prevádzkovateľ základnej služby i poskytovateľ regulovanej služby je povinný hlásiť incident³⁸ bez zbytočného odkladu, najneskôr však do 24 hodín od jeho zistenia formou včasného varovania, v ktorom sa uvádza aj to, či mohol byť incident spôsobený protiprávnym konaním. SZoKB zároveň výslovne ukladá povinnosť prevádzkovateľovi základnej služby oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosť, že bol spáchaný trestný čin, ktorého sa incident týka, ak sa o ňom hodnoverným spôsobom dozvie.

4.1 Porušenie sankcií

Hoci páchatelia sú zvyčajne anonymní, platby výkupného môžu porušovať režimy finančných sankcií. Uľahčenie platby výkupného, ktoré sa požaduje v dôsledku kybernetických útokov, môže umožniť páchatelom (s väzbou na sankcie) profitovať a presadzovať svoje nezákonné ciele. Napríklad platby vykonané sankcionovaným osobám alebo jurisdikciám, na ktoré sa vzťahujú komplexné sankcie, by sa mohli použiť na financovanie činností, ktoré sú v rozpore s cieľmi národnej bezpečnosti a zahraničnej politiky štátu. Takéto platby nielenže podporujú a obohacujú zlomyseľných aktérov, ale tiež udržiavajú a podnecujú ďalšie útoky. V Slovenskej republike ani v Českej republike nemôžu prípadné platby výkupného porušovať režimy finančných sankcií. Medzi príslušné režimy patria:

4.1.1 Sankčný režim Európskej únie (EÚ)

EÚ má zavedených viac ako štyridsať rôznych geografických a horizontálnych sankčných režimov. **Geografické sankčné režimy** sú zamerané na konkrétny štát, naopak **horizontálne režimy** sa týkajú tematických oblastí (napr. boj proti terorizmu, porušovanie ľudských práv, a pod.). Niektoré z nich schvaľuje Bezpečnostná rada Organizácie Spojených národov a sú transponované aj do legislatívy EÚ, zatiaľ čo iné prijíma EÚ autonómne.³⁹

Rozhodnutia a nariadenia Rady EÚ, ktorými sa ukladajú, upravujú alebo rušia reštriktívne opatrenia nadobúdajú platnosť spravidla dňom uverejnenia v Úradnom vestníku EÚ. Užitočným nástrojom na vyhľadávanie právnych aktov a na overenie informácie o zaradení jednotlivých osôb a entít na sankčné zoznamy je tzv. sankčná mapa EÚ, ktorú spravuje Európska komisia. Rozhodnutia a nariadenia Rady EÚ, ktoré sú zverejňované v Úradnom vestníku EÚ majú prednosť pred právnymi predpismi členských štátov.

Režim kybernetických sankcií EÚ je osobitne zameraný na osoby, subjekty a skupiny zodpovedné za kybernetické útoky vrátane ransomvéru, ktoré ohrozujú záujmy EÚ, alebo sa na nich podieľajú. Aktuálne sem sankcie proti ruským a severokórejským aktérom, ktorí

³⁸ Podľa § 24 ods.1 SZoKB prevádzkovateľ základnej služby je povinný hlásiť závažný kybernetický bezpečnostný incident, pričom závažnosť incidentu v prvom rade musím vyhodnotiť prevádzkovateľ základnej služby. Podľa § 16 ods. 1 ČZokB je každý poskytovateľ regulovanej služby povinný hlásiť každý kybernetický bezpečnostný incident, pričom podľa § 16 ods. 2 ČZokB NÚKIB oznámi poskytovateľovi regulovanej služby v režime vyšších povinností do 24 hodín od oznámenia incidentu, či má kybernetický bezpečnostný incident významný dopad na kybernetický priestor štátu.

³⁹ Mapa sankcií EÚ poskytuje vizuálny prehľad aktuálne platných sankčných režimov. *EU Sanctions Map* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.sanctionsmap.eu/#/main/details/47/lists>

sú spojené s vysokoprofilovými útokmi, ako sú NotPetya a WannaCry. Tento rok bolo pridaných na zoznam 6 osôb za útoky na členské štáty EÚ a Ukrajinu.⁴⁰

Právny základ režimu kybernetických sankcií v EÚ je tvorený **Rozhodnutím Rady č. 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty a Nariadením Rady (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty** (ďalej „nariadenie“), ktoré zavádzajú reštriktívne opatrenia proti kybernetickým útokom, ktoré ohrozujú EÚ alebo jej členské štáty. Tento sankčný režim bol zriadený v máji 2019 a je zameraný na škodlivé kybernetické aktivity pochádzajúce mimo územia EÚ, ktoré predstavujú hrozbu pre Úniu alebo jej členské štáty. Sankcie sa vzťahujú aj na škodlivé kybernetické útoky namierené proti tretím krajinám alebo medzinárodným organizáciám. Tieto sankcie sú neutrálne vo vzťahu ku konkrétnym krajinám a pokrývajú skutočné aj pokusy o kybernetické útoky, ktoré môžu mať významný dopad. Pri posudzovaní závažnosti sa berie do úvahy rozsah a dosah narušenia, počet postihnutých osôb, počet členských štátov, ktorých sa to týka, rozsah hospodárskych škôd alebo zisk páchatel'a, závažnosť narušenia údajov a strata komerčne citlivých informácií.

Reštriktívne opatrenia zahŕňajú zmrazenie aktív osôb, subjektov alebo orgánov uvedených v prílohe I nariadenia. Žiadne finančné prostriedky ani hospodárske zdroje nesmú byť priamo ani nepriamo prístupné týmto osobám ani v ich prospech. Zároveň je zakázané vedome a úmyselne sa zúčastňovať na činnostiach, ktorých cieľom alebo dôsledkom je obchádzanie týchto opatrení.⁴¹ Ak sa útok ransomvérom pripíše jednotlivcom alebo subjektom určeným podľa tohto nariadenia, akákoľvek platba týmto subjektom môže predstavovať porušenie. Nariadenie zakazuje priame alebo nepriame sprístupnenie finančných prostriedkov alebo hospodárskych zdrojov osobám uvedeným na sankčnom zozname.⁴²

Nariadenie vyžaduje priradenie kybernetického útoku konkrétnym aktérom. V praxi by sa na sankčné zoznamy EÚ mohli dostať právnické osoby alebo jednotlivci spojení s veľkými ransomvérovými operáciami. Platby týmto aktérom by potom boli v rozpore s nariadením hoci sa v nariadení výslovne nespomínajú „platby výkupného“. Opatrenia sú široké a vzťahujú sa na priamu aj nepriamu podporu, čo znamená, že aj platba výkupného prostredníctvom sprostredkovateľa by mohla byť potenciálnym porušením nariadenia, ak je konečným príjemcom sankcionovaná osoba. Tým sa platenie výkupného stáva právne rizikovým, najmä ak existuje vedomosť alebo odôvodnený predpoklad na strane obete ransomvérového útoku, že príjemca je sankcionovanou stranou.

⁴⁰ Cyber-attacks: six persons added to EU sanctions list for malicious cyber activities against EU member states and Ukraine. *Rada EÚ* [online]. 24. 6. 2024 [cit. 9. 4. 2025]. Dostupné z: <https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/cyber-attacks-six-persons-added-to-eu-sanctions-list-for-malicious-cyber-activities/cyberattacks-against-eu-member-states-and-ukraine/>

⁴¹ Články 3 a 9 nariadenia.

⁴² Článok 3 ods. 2 nariadenia.

4.1.2 Sankcie Organizácie Spojených národov (OSN)

Oba štáty uplatňujú sankcie OSN, ktoré sa často prekrývajú s opatreniami EÚ. Tieto sankcie sa zvyčajne týkajú globálnych hrozieb vrátane aktivít štátom podporovaných skupín zapojených do kybernetických útokov. Sankcie vydávané na základe rozhodnutia Bezpečnostnej rady OSN sú právne záväzné pre všetkých členov OSN a v súčasnosti sú na základe § 3 zákona č. 289/2016 Z. z. o vykonávaní medzinárodných sankcií v znení neskorších právnych predpisov (ďalej „slovenský sankčný zákon“) v Slovenskej republike a § 2 zákona č. 69/2006 Sb. o provádění mezinárodních sankcí v znení neskorších právnych predpisov (ďalej „český sankčný zákon“) v Českej republike priamo aplikovateľné (ďalej spolu „sankčné zákony“).

4.1.3 Sankčné zákony

Česká aj Slovenská republika má pre implementáciu medzinárodných sankcií platný *lex specialis*, ktorými sú sankčné zákony. Oba sankčné zákony stanovujú vykonávanie medzinárodných sankcií s cieľom zabezpečenia, udržania a obnovy medzinárodného mieru a bezpečnosti, ochrany základných ľudských práv, boja proti terorizmu a šíreniu zbraní hromadného ničenia a v záujme dosiahnutia cieľov spoločnej zahraničnej a bezpečnostnej politiky Európskej únie.

Český sankčný zákon definuje **medzinárodnú sankciu** ako „*příkaz, zákaz nebo omezení stanovené za účelem udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochrany lidských práv a svobod a podpory demokracie a právního státu*“, ktoré vyplývajú aj z priamo použiteľných predpisov Európskej únie.⁴³ Slovenský sankčný zákon definuje medzinárodnú sankciu ako „*obmedzenie, príkaz alebo zákaz v predpisoch o medzinárodnej sankcii*“, ktorými sú *inter alia* aj právne záväzný akt Európskej únie.⁴⁴

V Českej republike koordinuje vykonávanie medzinárodných sankcií na vnútroštátnej úrovni Finanční analytický úřad (FAÚ) a plní úlohu národného príslušného orgánu. V závislosti od povahy reštriktívnych opatrení sa na vykonávaní medzinárodných sankcií a kontrole ich dodržiavania podieľajú okrem FAÚ aj ďalšie ministerstvá a štátne orgány v rámci svojich kompetencií.

Ako problematickú vnímame aplikovateľnosť slovenského sankčného zákona v praxi.⁴⁵ Medzi nedostatky právnej úpravy zaraďujeme, že neexistuje jeden ústredný orgán verejnej moci (ústredný orgán štátnej správy), ktorý by bol zodpovedný za implementáciu medzinárodných sankcií. Aktuálne je celková aplikácia „rozdelená“ medzi viacero zodpovedných subjektov verejnej moci, čím prichádza k akejsi fragmentácii tejto zodpovednosti. Tento fakt možno pričítať okolnosti, že slovenská právna úprava ustanovuje iba všeobecne, že príslušným orgánom štátnej správy je orgán štátnej správy, ktorý je v rozsahu svojej pôsobnosti

⁴³ § 2 písm. c) českého sankčného zákona.

⁴⁴ § 2 písm. a) slovenského sankčného zákona.

⁴⁵ MATUŠKA, P. Sankčný mechanizmus v systéme práva Európskej únie. *Justičná revue*. 2022, roč. 74, č. 8–9, s. 901–916.

podľa osobitného predpisu príslušný a zodpovedný za zabezpečovanie vykonávania medzinárodných sankcií, vrátane príslušnosti na správne konanie, rozhodovanie a iný úradný postup vo veciach vykonávania medzinárodnej sankcie.

Medzinárodná sankcia v oblasti obchodu a nefinančných služieb je obmedzenie, príkaz alebo zákaz poskytovania akéhokoľvek iného plnenia českou, resp. slovenskou osobou v prospech sankcionovanej osoby na sankcionovanom území vrátane uzatvárania obchodov s nimi.⁴⁶ Preto je potrebné, aby si každý, kto udržiava alebo má v úmysle nadviazať akékoľvek obchodné alebo iné kontakty v „rizikových“ oblastiach alebo s „rizikovými“ osobami, vždy včas overil, či takýto subjekt nie je uvedený medzi osobami, s ktorými sú kontakty a obchodné vzťahy obmedzené alebo priamo zakázané.⁴⁷

Ak je príjemca výkupného na sankčnom zozname EÚ alebo OSN, platba by mohla predstavovať naplnenie správneho deliktu⁴⁸, ktorého sa dopustí ten kto poruší obmedzenie, príkaz alebo zákaz vyplývajúci z medzinárodnej sankcie. Za tento delikt možno podľa českého sankčného zákona uložiť pokutu až do 50 000 000 Kč, prípadne až do 10 % z ročného obratu podľa poslednej riadnej alebo konsolidovanej účtovnej závierky. Podľa slovenského sankčného zákona hrozí pokuta až do 1 659 700 €, najmä ak tým spôsobila obzvlášť závažný následok spočívajúci v ohrození alebo porušení dôležitého zahraničnopolitického alebo bezpečnostného záujmu štátu.

Inšpiráciou v prípade posudzovania sankcionovania za výkupné je prístup OFAC v USA. OFAC vydal usmernenie k potenciálnych sankčných rizikách pri platbách výkupného, v ktorom zvyrazňuje potrebu zavedenie compliance programu pre oblasť sankcií a opatrení odolnosti.⁴⁹ Podľa usmernenia OFAC je existencia, povaha a primeranosť programu dodržiavania sankcií faktorom, ktorý môže OFAC zvážiť pri určovaní primeranej reakcie na zjavné porušenie amerických sankčných zákonov alebo predpisov. O obdobnom prístupe či usmernení v Českej a Slovenskej republike nemáme vedomosť.

Compliance programy v oblasti sankcií týchto právnických osôb by mali zohľadňovať najmä riziko, že platba výkupného sa môže týkať sankcionovaných osôb, alebo jurisdikcie, na ktorú sa vzťahuje komplexné embargo. Právnické osoby zapojené do sprostredkovania platieb ransomvéru v mene poškodených by mali tiež zvážiť, či majú regulačné povinnosti. Významné kroky prijaté na zníženie rizika vydierania sankcionovaným subjektom prostredníctvom prijatia alebo zlepšenia postupov kybernetickej bezpečnosti (výslovne sa uvádza usmernenie *Ransomware Guide* od agentúry *Cybersecurity and Infrastructure Security Agency* – CISA zo septembra 2020), sa budú považovať za významný zmierňujúci faktor pri posudzovaní prípadu zo strany OFAC.

⁴⁶ § 5 ods. 2 písm. a) českého sankčného zákona, § 6 písm. e) slovenského sankčného zákona.

⁴⁷ Medzinárodní sankce v ČR. *Finanční analytický úřad* [online]. Dostupné z: <https://fau.gov.cz/mezinarodni-sankce-v-cr>

⁴⁸ Podľa § 19 ods. 1 písm. a) českého sankčného zákona, alebo podľa § 22 ods. 1 písm. a) slovenského sankčného zákona.

⁴⁹ Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. *Department of Treasury* [online]. 21. 9. 2021 [cit. 9. 4. 2025]. Dostupné z: <https://ofac.treasury.gov/media/912981/download?inline>

4.1.4 Trestnosť porušenia medzinárodných sankcií

Porušovanie medzinárodných sankcií je trestné, v prípade naplnenia skutkovej podstaty trestného činu porušenia reštriktívneho opatrenia podľa § 417a ods. 1 písm. a), písm. g), a písm. h) Trestného zákona „*keď poruší reštriktívne opatrenie v rozsahu najmenej 10 000 €, tým že*

- *sprístupní finančné prostriedky alebo hospodárske zdroje priamo alebo nepriamo označenej osobe alebo v jej prospech*
- *použije alebo prevedie tretej strane finančné prostriedky alebo hospodárske zdroje, ktoré priamo alebo nepriamo vlastní, má v držbe alebo pod kontrolou označená osoba, a ktoré majú byť zaistené podľa reštriktívneho opatrenia, alebo inak s nimi nakladá, s cieľom zatajiť tieto finančné prostriedky alebo hospodárske zdroje,*
- *poskytne nepravdivé alebo zavádzajúce informácie s cieľom zatajiť skutočnosť, že konečným vlastníkom alebo prijímateľom finančných prostriedkov alebo hospodárskych zdrojov, ktoré sa majú zaistiť podľa reštriktívneho opatrenia je označená osoba potrestá sa odňatím slobody až na tri roky.“*

Podľa § 137b ods. 1 Trestného zákona sa reštriktívnym opatrením rozumie „*prikaz, zákaz alebo obmedzenie vyplývajúce z medzinárodnej sankcie podľa predpisu o vykonávaní medzinárodných sankcií, prijaté právne záväzným aktom Európskej únie na základe čl. 29 Zmluvy o Európskej únii alebo čl. 215 Zmluvy o fungovaní Európskej únie.*“

Uvedené ustanovenia definície pojmov a novej skutkovej podstaty trestného činu porušenia reštriktívneho opatrenia boli doplnené do Trestného zákona s účinnosťou od 1. 8. 2025 ako súčasť transpozície **Smernice Európskeho parlamentu a Rady (EÚ) 2024/1226 z 24. apríla 2024 o vymedzení trestných činov a sankcií za porušenie reštriktívnych opatrení Únie a zmene smernice (EÚ) 2018/1673** (ďalej „smernica“).⁵⁰

Už v roku 2021 z analýzy Eurojust totiž vyplynulo, že v rámci porovnávaných 33 štátov nemalo priamy trestnoprávny postih porušovania alebo obchádzania medzinárodných sankcií iba Slovenská republika a Španielsko.⁵¹ V podmienkach Slovenskej republiky preto nebolo možné pred 1. 8. 2025 na základe účinnej právnej úpravy postihovať porušenia reštriktívnych opatrení normami trestného práva, s výnimkou tých, ktoré sa prekrývajú s inými trestnými činmi, ktoré pôvodne neboli cieleňé na túto oblasť. Na základe nových skutkových podstat trestného činu porušenia reštriktívneho opatrenia, bude možné postihovať takéto konanie normami trestného práva v súlade so smernicou. Okrem toho došlo k zavedeniu novej formy subjektívnej stránky trestného činu, t. j. konceptu hrubej nedbanlivosti vo vzťahu k zavineniu páchatel'a (trestný čin porušenia reštriktívneho opatrenia z hrubej nedbanlivosti podľa § 417b), vytvoreniu osobitnej úpravy hornej hranice peňažného

⁵⁰ Zákon č 157/2025 Z.z. ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

⁵¹ Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis. Eurojust [online]. [cit. 9. 4. 2025]. Dostupné z: https://www.eurojust.europa.eu/sites/default/files/assets/genocide_network_report_on_prosecution_of_sanctions_restrictive_measures_violations_23_11_2021.pdf

trestu, ktorý možno uložiť právnickej osobe v prípade takéhoto porušenia⁵², a v neposlednom rade došlo k nastaveniu koexistencie administratívnoprávnej a trestnoprávnej zodpovednosti v prípade porušenia reštriktívneho opatrenia.

Potrebu trestnoprávnej úpravy porušenia sankcií považujeme za odôvodnenú, nakoľko správne sankcie môžu byť málo odstrašujúce a v niektorých prípadoch aj nepostačujúce vzhľadom na rozsah a dôsledky porušenia sankcií (podpora ozbrojených konfliktov a tým spolupáchateľstvo na hlavných medzinárodných zločinoch). Okrem nižšieho odstrašujúceho účinku, spôsobuje absencia trestnoprávneho postihu aj neschopnosť poskytnúť justičnú spoluprácu iným členským štátom, či nemožnosť v odôvodnených prípadoch efektívne konfiškovať majetok podliehajúci medzinárodnej sankcii.

Uvedená skutková podstata trestného činu porušenia reštriktívneho opatrenia postihuje *inter alia* nasledovné porušenia reštriktívnych opatrení:

- a) sprístupnenie finančných prostriedkov alebo hospodárskych zdrojov priamo alebo nepriamo označenej osobe, subjektu alebo orgánu alebo v ich prospech v rozpore so zákazom, ktorý vyplýva z reštriktívneho opatrenia, ak sa toto konanie týka finančných prostriedkov alebo hospodárskych zdrojov v rozsahu najmenej 10 000 €; ale aj
- b) obchádzanie reštriktívneho opatrenia, ak sa toto konanie týka finančných prostriedkov alebo hospodárskych zdrojov v rozsahu najmenej 10 000 €
 - 1) použitím alebo prevodom tretej strane finančných prostriedkov alebo hospodárskych zdrojov, ktoré priamo alebo nepriamo vlastní, má v držbe alebo pod kontrolou označená osoba, subjekt alebo orgán a ktoré majú byť zaistené podľa reštriktívneho opatrenia Európskej únie, alebo iným nakladaním s nimi, s cieľom zatajiť tieto finančné prostriedky alebo hospodárske zdroje;
 - 2) poskytnutím nepravdivých alebo zavádzajúcich informácií s cieľom zatajiť skutočnosť, že konečným vlastníkom alebo prijímateľom finančných prostriedkov alebo hospodárskych zdrojov, ktoré sa majú zmraziť alebo zaistiť podľa reštriktívneho opatrenia Európskej únie, je označená osoba, subjekt alebo orgán.

Z hľadiska znakov skutkovej podstaty trestného činu ide o úmyselný trestný čin, ktorého páchatelom môže byť ktokoľvek (všeobecný subjekt), kto je trestne zodpovedný. Objektívna stránka trestného činu spočíva v porušení príkazu, zákazu alebo obmedzenia vyplývajúceho z reštriktívneho opatrenia.

Z vyššie uvedeného vyplýva, že poškodený ransomvérovým útokom, ktorý uhradí výkupné sankcionovanej osobe, subjektu alebo orgánu, by mohol naplniť skutkovú podstatu trestného činu porušenia reštriktívneho opatrenia podľa § 417a ods. 1 Trestného zákona, ak by boli splnené nasledujúce podmienky:

- a) **Uhradenie výkupného sankcionovanej osobe:** Ak poškodený zaplatí ako výkupné finančné prostriedky v hodnote najmenej 10 000 € a tieto finančné prostriedky sú sprístupnené priamo alebo nepriamo osobe, subjektu alebo orgánu uvedenému

⁵² Podľa § 15 ods. 2 zákona č. 91/2016 Z.z. o trestnoprávnej zodpovednosti právnických osôb v znení účinnom od 1. 8. 2025, môže súd uložiť právnickej osobe peňažný trest od 1 500 € do 40 000 000 €, ak odsudzuje právnickú osobu za trestný čin podľa § 417a, § 417b alebo § 417d Trestného zákona.

v reštriktívnych opatreniach EÚ, konanie by mohlo byť kvalifikované ako porušenie reštriktívneho opatrenia.

- b) **Vedomosť obete o reštriktívnom opatrení:** Na naplnenie subjektívnej stránky trestného činu by muselo byť preukázané, že poškodený si bol vedomý, aspoň na úrovni nepriameho úmyslu, že platba smeruje k sankcionovanej osobe, t.j. vedel, že k porušeniu reštriktívneho opatrenia môže dôjsť, a bol s tým uzročený.
- c) **Obchádzanie reštriktívnych opatrení:** Ak by platba bola sprostredkovaná cez tretie strany, ako sú niektorí poskytovatelia služieb virtuálnych aktív alebo anonymizačné technológie, a cieľom by bolo zatajiť skutočnosť, že prijímateľom je sankcionovaná osoba, mohlo by sa takéto konanie považovať za obchádzanie reštriktívneho opatrenia.

Tento trestný čin je konštruovaný ako výlučne úmyselný. Ak by poškodený ransomvérovým útokom konal bez úmyslu, že výkupné smeruje k sankcionovanej osobe (napr. na základe falošných alebo zavádzajúcich informácií od útočníkov), trestná zodpovednosť by nevznikla.

Na rozdiel od Slovenska, v českom trestnom zákoníku je už od prijatia českého sankčného zákona, upravený trestný čin porušenia medzinárodných sankcií, a to v § 410 českého trestného zákoníka. Objektívna stránka skutku spočíva v konaní páchatela, ktorý vo väčšom rozsahu poruší príkaz, zákaz alebo obmedzenie, ktorých dodržiavanie je Česká republika povinná zabezpečiť na základe svojho členstva v Organizácii Spojených národov alebo v Európskej únii. K dokonaniu trestného činu dochádza už tým, že páchatel poruší takýto príkaz, zákaz alebo obmedzenie a musí byť vykonané vo väčšom rozsahu a úmyselne, inak by išlo len o priestupok podľa českého sankčného zákona.⁵³

Pri posudzovaní väčšieho rozsahu sa nemožno opierať o výkladové ustanovenia § 138, ktoré definujú pojem väčšia škoda, prospech, náklady atď. Finančné hľadisko nemožno vôbec uplatniť, pretože ide o rozsah porušenia príkazu, zákazu alebo obmedzenia, a to z hľadiska frekvencie porušenia alebo závažnosti príkazu, zákazu alebo obmedzenia, prípadne škodlivosti alebo nebezpečnosti takéhoto porušenia a podobne.⁵⁴ Väčší rozsah môže byť naplnený viacerými spôsobmi, inter alia aj jednorazovým porušením jedného príkazu, zákazu alebo obmedzenia, ak ide o konanie, ktorého rozsah výrazne alebo podstatne presahuje bežné prípady porušenia takýchto opatrení.

Pri posudzovaní trestnoprávneho významu zaplatenia výkupného pri ransomvérovom útoku, ak existuje dôvodné podozrenie, že by mohlo dôjsť k prevodu majetku v prospech sankcionovaných osôb alebo subjektov, je dôležité analyzovať, či takéto konanie nenaplní znaky obchádzania medzinárodných sankcií vo „väčšom rozsahu“. Pri tejto analýze možno použiť pomocné kritériá.⁵⁵ Rozhodujúci môže byť spôsob vykonania platby (napr. konšpiratívne prevody, anonymizácia), povaha a cieľ transakcie (napr. podpora sankcionovaného subjektu), ako aj prípadná nadväznosť na trestnú činnosť (napr. financovanie

⁵³ ŠÁMAL, P., ŠÁMALOVÁ, M., BOHUSLAV, L.. § 410 [Porušení mezinárodních sankcí]. In: ŠÁMAL, P. a kol. *Trestní zákoník*. 3. vyd. Praha: C. H. Beck, 2023, s. 4819, marg. 3.

⁵⁴ Ibid. porov. mutatis mutandis bod 18 uznesenia Najvyššieho súdu z 28. 6. 2017, sp. zn. 5 Tdo 232/2017, publikované ako R 4/2018.

⁵⁵ Ibid., marg. 4.

terorizmu alebo legalizácia výnosov). Z uvedeného vyplýva, že zaplatenie výkupného pri ransomvérovom útoku, ak je preukázateľné alebo dôvodne predpokladateľné, že by mohlo ísť o podporu subjektov zaradených na sankčný zoznam, môže za určitých okolností naplňať skutkovú podstatu obchádzania medzinárodných sankcií vo väčšom rozsahu.

4.2 Legalizácia výnosu z trestnej činnosti

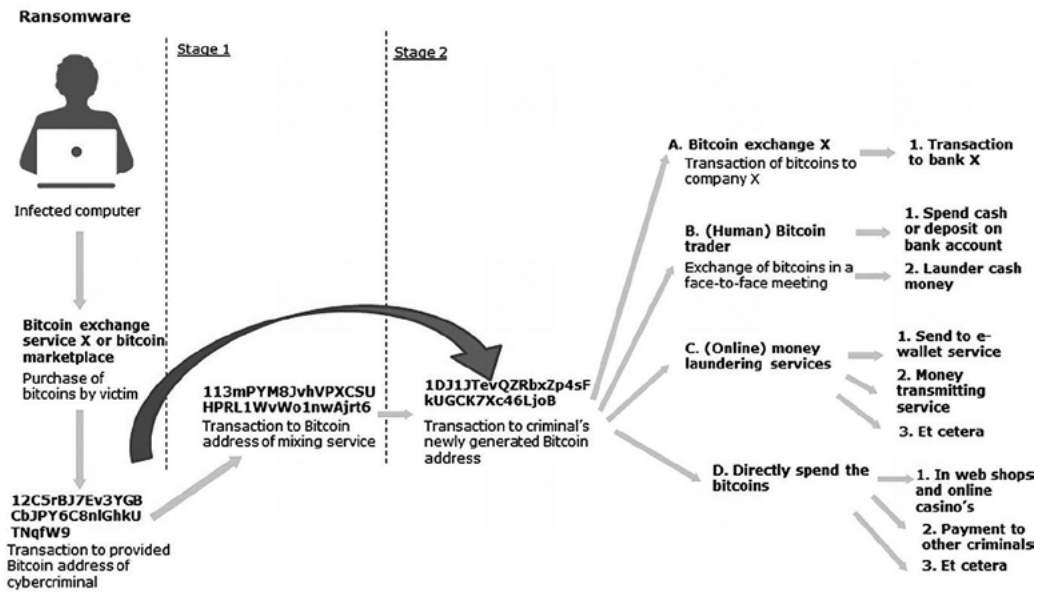
Vychádzajme z nasledovnej modelovej situácie, kde spoločnosť X je poškodeným ransomvérovým útokom. Útočníci zašifrujú jej citlivé dáta a požadujú výkupné vo výške 50 000 € v kryptomene Bitcoin, ktorá je potom smerovaná cez mixér kryptomien alebo premenená na privacy coins, napríklad Monero. Spoločnosť X, z dôvodu neexistencie záloh a obavy o stratu dôležitých údajov a finančných škôd, neoznámí incident na príslušnej jednotke CSIRT ani nepodá trestné oznámenie, výkupné zaplatí v kryptomene a spôsobom, ktorý žiadajú útočníci.

Výkupné požadované v niektorej z kryptomien, je teda súčasťou konania páchatel'a po neoprávnenom prieniku do systému spoločnosti napr. prostredníctvom phishingu, zraniteľnosti v softvéri alebo slabého zabezpečenia a následného zašifrovania dát (trestné činy podľa § 247 a § 247a Trestného zákona). Útočníci získavajú kryptomenu ako priamy výsledok trestného činu.

Aktuálnym trendom je žiadať o zaplatenie výkupného v niektorej z kryptomien. Kyberzločinci žiadajú o prevod bitcoinov na iné bitcoinové adresy alebo sériu bitcoinových adries. Po takomto prevode môže nasledovať vyplatenie peňazí, ale nie vždy. Tento model pozostáva z dvoch fáz a je znázornený na obrázku. V prvej fáze sa pôvod peňazí zakrýva pomocou tzv. mixovacích služieb, ktoré sa používajú na zakrytie nelegálneho pôvodu bitcoinov. Z právneho hľadiska je veľmi pravdepodobné, že využívanie služieb mixovania je už zakrývacím úkonom, ktorý sa kvalifikuje ako legalizácia výnosov z trestnej činnosti. V niektorých prípadoch sa prvá fáza vynecháva. V druhej fáze sa bitcoiny prevedú na bitcoinové adresy jedného alebo viacerých sprostredkovateľov, po čom skončia u kyberzločincov, ktorí s nimi ďalej nakladajú.⁵⁶

⁵⁶ CUSTERS, B., OERLEMANS, J., POOL, R. Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*. 2020, roč. 28, č. 2, s. 121–152 [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1163/15718174-02802002>

Obr. 1: Model legalizácie výnosov z trestnej činnosti z ransomvéru a kryptovéru prostredníctvom bitcoinov



Zdroj: CUSTERS, B., OERLEMANS, J., POOL, R. Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*. 2020, roč. 28, č. 2, s. 121–152 [cit. 9. 4. 2025]. DOI: <https://doi.org/10.1163/15718174-02802002>

Obdobne v prípade anonymných kryptomien, resp. kryptomien zameraných na ochranu osobných údajov (*privacy coins*), tieto zakrývajú tok peňazí. Hoci sa na tieto účely používali – a stále používajú – bežné kryptomeny, ako napríklad Bitcoin, sú pseudonymné a relatívne transparentné vďaka verejne prístupnej histórii transakcií v príslušných blockchainoch. Z tohto dôvodu *privacy coins*, ako sú Monero (XMR), Zcash (ZEC) a Dash (DASH), vynikajú svojimi vylepšenými funkciami anonymity, ktoré zahmlievajú transakcie, a preto sú preferovanou voľbou na nelegálnu činnosť.⁵⁷

Podľa ustanovenia § 233 ods. 2 Trestného zákona je trestné úmyselné konanie, ktorým sa zatajuje pôvod, existencia, umiestnenie, či vlastnícke práva k veci, ktorá je výnosom z trestnej činnosti. Ide najmä o situácie, keď páchatel zámerné umožní, aby výnosy z trestnej činnosti zostali neodhalené.

Z hľadiska objektívnej stránky takýto trestný čin zahŕňa ukrývanie výnosov z trestnej činnosti, ich zmenu (napr. zmenu vzhľadu alebo povahy veci), zatajenie ich existencie

⁵⁷ SCHARNOWSKI, S. Dark web traffic, privacy coins, and cryptocurrency trading activity. *Finance Research Letters* [online]. 2024, roč. 67, časť B, č. 105875. ISSN 1544-6123 [cit. 9. 4. 2025]. Dostupné z: <https://doi.org/10.1016/j.frl.2024.105875>

či znemožnenie, aby došlo k „vystopovaniu“ výnosu z trestnej činnosti.⁵⁸ Zo subjektívneho hľadiska sa vyžaduje úmysel, aby páchatel vedel o nezákonnom pôvode finančných prostriedkov a zámerne prispel k ich zatajeniu.

Z toho pohľadu vnímame preto ako rizikové, ak poškodený ransomvérovým útokom zaplatí výkupné porušujúc právne predpisy a najmä povinnosť odbornej starostlivosti tým, že neoznámí kybernetický bezpečnostný incident ani nepodá trestné oznámenie a zároveň vedome použije anonymizačné nástroje podľa pokynu útočníkov, smerujúce zjavne k zatajeniu pôvodu finančných prostriedkov – napríklad použitím technológií, ktoré sú určené na anonymizáciu transakcií (kryptomenové mixéry alebo privacy coins ako Monero). Tým umožňuje útočníkom zatajiť nezákonný pôvod výkupného. Uvedeným konaním by mohla byť za daných okolností naplnená skutková podstata trestného činu úmyselnej legalizácie podľa § 233 ods. 2 Trestného zákona, alternatívne v spojení § 21 ods. 1 písm. d) Trestného zákona (účastníctvo formou pomoci). Podotýkame, že v oboch prípadoch ide pri kvalifikácii podľa § 233 ods. 2 prípadne ods. 3 Trestného zákona stále o úmyselný prečin legalizácie.

V prípade nedostatku na strane subjektívnej stránke (úmyslu) je potrebné pripomenúť, že Trestný zákon samostatne postihuje aj trestný čin legalizácie z nedbanlivosti podľa § 233a ods. 2 Trestného zákona. Na rozdiel od úmyselného konania sa trestný čin z nedbanlivosti týka prípadov, keď niekto „z nedbanlivosti umožní zatajiť pôvod alebo zistenie pôvodu veci väčšej hodnoty, ktorá je výnosom z trestnej činnosti.“ Pre naplnenie skutkovej podstaty podľa § 233a ods. 2 Trestného zákona je potrebné naplniť tieto znaky:

- hodnota zatajených finančných prostriedkov prevyšuje 20 000 € (vec väčšej hodnoty)
- páchatel koná z nedbanlivosti, napríklad tým, že neoverí, či služby, ktoré používa na úhradu výkupného (napr. kryptomenové burzy alebo peňaženky), neumožňujú anonymizáciu transakcií alebo nevedome sleduje pokyny útočníkov bez zohľadnenia potenciálnych dôsledkov, prípadne že tieto služby sú známe nedodržívaním pravidiel.⁵⁹

Zatajenie skutočnej povahy veci, ktorá je výnosom z trestnej činnosti, jej umiestnenia, pohybu, nakladania s ňou, vlastníckeho alebo iného práva k nej, si nevyžaduje aktívne konanie v zmysle vytvorenia utajovanej informácie, ale v zásade postačuje aj pasívne konanie, ktoré vytvára dojem, že takáto vec má legálny pôvod, čím sťažuje alebo znemožňuje zistenie jej pôvodu ako veci, ktorá je v skutočnosti výnosom z trestnej činnosti.⁶⁰ Osobitnou otázkou, ktorá však prekračuje rámec rozberanej problematiky v tomto článku, ostáva

⁵⁸ ŠAMKO, P. Trestný čin legalizácie výnosu z trestnej činnosti a zdrojový trestný čin – základné východiská a praktické príklady. *Právne Listy* [online]. [cit. 9. 4. 2025]. Dostupné z: <https://www.pravnelisty.sk/clanky/a1267-trestny-cin-legalizacie-vynosu-z-trestnej-cinnosti-a-zdrojovy-trestny-cin-zakladne-vychodiska-a-prakticke-priklady>

⁵⁹ Napríklad Binance Holdings Limited (Binance), najväčšia burza kryptomien na svete, Binance.com, priznala, že „neudržiava účinný program proti praniu špinavých peňazí...“ a „úmyselné zlyhania umožnili tok peňazí teroristom, kyberzločincom“ viac Binance and CEO Plead Guilty to Federal Charges in § 4 B Resolut. U.S. Department of Justice [online]. 21. 11. 2023 [cit. 9. 4. 2025]. Dostupné z: <https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution>

⁶⁰ ŠÁMAL, P. a kol. § 216 [Legalizace výnosů z trestné činnosti]. In: ŠÁMAL, P. a kol. *Trestní zákoník*. 3. vyd. Praha: C. H. Beck, 2023, s. 2768, marg. 16.

aj skutočnosť, ako by bola úhrada výkupného vedená v účtovníctve subjektu a či by týmto konaním nedochádzalo aj poručovaniu daňových a účtovných právnych predpisov.

Trestné činy legalizácie výnosov z trestnej činnosti sú aj v § 216 a § 217 českom trestním zákoníku upravené v úmyselnom aj nedbanlivostnom variante a sa vždy skladajú z dvoch základných skutkových podstát.⁶¹ Z hľadiska predmetu tohto článku je relevantná objektívna stránka, ktorá spočíva predovšetkým v tom, že páchatel:

- 1) zatají pôvod majetku, ktorý je výnosom z trestnej činnosti, najmä tým, že zatají alebo zatají jeho skutočnú povahu, miesto, pohyb, nakladanie, vlastnícke alebo iné právo k nemu, alebo sa inak snaží podstatne sťažiť alebo znemožniť zistenie pôvodu tohto majetku (len v prípade úmyselnej formy podľa § 216 ods. 2) alebo
- 2) umožňuje inému zatajiť pôvod alebo zistenie pôvodu veci väčšej hodnoty (najmenej 100 000 Kč), ktorá je výnosom z trestnej činnosti (len v prípade nedbanlivostnej formy podľa § 217 ods. 1).

Zatajením skutočnej povahy výnosov z trestnej činnosti podľa § 216 ods. 2, ich umiestnenia, pohybu, nakladania s nimi, vlastníckeho alebo iného práva k nim postačuje aj pasívne konanie, typicky zasielanie finančných prostriedkov (peňazí), ktoré sú výnosmi z trestnej činnosti, vo virtuálnych menách (napr. bitcoinoch), kde hlavnou výhodou je sťažená identifikácia osôb, ktoré s nimi nakladajú.⁶²

Zatajenie podľa § 217 ods. 1 znamená, že informácie o pôvode veci sú zatajené alebo skreslené. K prostriedkom zatajenia pôvodu veci patrí prevod vlastníctva vecí, zatajenie jej skutočnej povahy, jej umiestnenia a pohybu, zatajenie dispozície (nakladania) s vecou a informácie o vlastníckych alebo iných právach k nej.⁶³

Trestnoprávna zodpovednosť môže vzniknúť až na základe následného spracovania alebo transferu finančných prostriedkov, ktoré priamo napomáhajú zatajeniu ich trestného pôvodu. Dôležitými faktormi sú:

- 1) použitie anonymizačných nástrojov alebo metód na utajenie transakcií,
- 2) neoznámenie ransomvérového útoku orgánom činným v trestnom konaní,
- 3) vedenie transakcií v účtovníctve bez zohľadnenia ich trestného pôvodu.

Aby sa predišlo potenciálnemu naplneniu skutkovej podstaty trestného činu, je dôležité, aby poškodený ransomvérov útokom:

- 1) vykonal náležitú starostlivosť (*due diligence*) pred realizáciou akejkoľvek platby,
- 2) oznámil ransomvérový útok príslušným orgánom a poskytol maximálnu súčinnosť pri vyšetrovaní,
- 3) vypracoval interné pravidlá pre riešenie ransomvérových útokov, vrátane mechanizmov na posúdenie právnych dôsledkov a compliance rizík spojených s úhradou výkupného.

⁶¹ ŠÁMAL kol., 2023, op. cit., s. 2759, marg. 1.

⁶² Ibid., s. 2768, marg. 16.

⁶³ Ibid., s. 2785, marg. 6.

Vzhľadom na takmer exkluzívne používanie kryptomien v prípadoch ransomvérových útokov je potrebná zvláštna obozretnosť pri transakciách, ktoré by mohli viesť k zatajeniu výnosov z trestnej činnosti.⁶⁴

4.3 Financovanie terorizmu

Podľa § 419c ods. 1 Trestného zákona „*kto sám alebo prostredníctvom iného zhromažďuje alebo poskytuje priamo alebo nepriamo veci, finančné prostriedky alebo iné prostriedky pre páchatela terorizmu, pre teroristickú skupinu, jej člena, alebo na spáchanie niektorého z trestných činov terorizmu, alebo zhromažďuje veci, finančné prostriedky alebo iné prostriedky v úmysle, aby ich bolo možné takto použiť, alebo s vedomím, že na taký účel môžu byť použité, potrestá sa odňatím slobody na päť rokov až pätnásť rokov.*“

Podľa § 312d českého trestného zákoníku „*kdo sám nebo prostřednictvím jiného finančně nebo materiálně podporuje teroristickou skupinu, jejího člena, teroristu nebo spáchání teroristického trestného činu, trestného činu podpory a propagace terorismu (§ 312e) nebo vyhržování teroristickým trestným činem (§ 312f) anebo shromažďuje finanční prostředky nebo jiné věci v úmyslu, aby jich bylo takto užito.*“

Financovanie terorizmu je samostatným trestným činom v českom aj slovenskom trestnom práve. Súčasne výraznou črtou českej aj slovenskej právnej úpravy je, že páchatel sa postihuje aj v prípade, ak zhromažďuje alebo poskytuje finančné alebo iné prostriedky jednotlivcovi, ktorý je označený ako „terorista“ resp. „páchatel terorizmu“, pretože nie každá osoba, ktorá pácha trestné činy, je členom teroristickej skupiny, rovnako ako nie každý člen teroristickej skupiny je nevyhnutne teroristom.⁶⁵ Uvedené je potrebné najmä na účely postihovania páchatel'ov, ktorí financujú tzv. osamelých bojovníkov, ktorí nepatria do žiadnej z teroristických skupín, resp. osôb, ktoré sú v teroristických zoznamoch OSN alebo EÚ.

K výkonu sankcie uloženej za trestné činy v oblasti terorizmu, ak sa osoba jej vyhýba, ako efektívny procesný nástroj môže byť použitý európsky zatýkací rozkaz⁶⁶, ktorý je plne udomácnенý v aplikačnej praxi.⁶⁷

Zastávame právny názor, že poškodený ransomvérovým útokom, ktorý uhradí výkupné v prospech páchatel'a, môže za určitých okolností spáchať tento trestný čin. Základným predpokladom je, či vedome (ne)poskytne finančné alebo iné prostriedky osobe, ktorá je označená ako „páchatel terorizmu“ alebo ktorá je evidovaná v teroristických zoznamoch OSN či EÚ, a to buď priamo, alebo sprostredkované.

Závažnou okolnosťou je však požiadavka subjektívnej stránky trestného činu – úmyslu. Ak poškodený vie alebo má dôvodné podozrenie, že výkupné môže byť použité na teroristické aktivity (napr. ak existuje preukázateľná väzba medzi útočníkmi a teroristickými organizáciami), môže byť jeho konanie právne kvalifikované ako financovanie terorizmu.

⁶⁴ CUSTERS, OERLEMANS, POOL, 2020, op. cit.

⁶⁵ ŠÁMAL, P., BOHUSLAV, L. § 312d [Financování terorismu]. In: ŠÁMAL kol., 2023, op. cit., s. 3976, marg. 2.

⁶⁶ KLIMEK, L. *European Arrest Warrant*. Cham: Springer, 2015, s. 98. DOI: <https://doi.org/10.1007/978-3-319-07338-5>

⁶⁷ KLIMEK, L. New Law on the European Arrest Warrant in the Slovak Republic: Does it Fulfil Standards at the Level of the EU? *European Journal of Crime, Criminal Law and Criminal Justice*. 2012, roč. 20, č. 2, s. 181–192. DOI: <https://doi.org/10.1163/092895612X13333546844473>

Trestný čin je pritom naplnený aj v prípade, ak poskytnuté prostriedky nie sú priamo použité na spáchanie teroristického činu, ale postačuje, že môžu byť takto použité.

V prípade, ak poškodený nemá vedomosť ani dôvodné podozrenie, že páchatel' ransomvérového útoku je zapojený do teroristických aktivít, jeho konanie spravidla nebude spĺňať znaky tohto trestného činu. V praxi však môže byť otázka vedomosti a jeho úmyslu predmetom rozsiahleho dokazovania, najmä ak sa výkupné realizuje prostredníctvom anonymných platobných systémov, ako sú kryptomeny, kde je identifikácia konečného príjemcu náročná. Aj v tomto prípade, obdobne ako v prípade sankcionovaných osôb, konštatovať, že pri úhrade výkupného ransomvérovému útočníkovi existuje riziko spáchania trestného činu financovania terorizmu, ak poškodený vedome poskytne prostriedky osobe alebo subjektu s preukázateľnými väzbami na teroristické aktivity. Z tohto dôvodu je pre poškodených kľúčové dôsledné posúdenie rizík spojených s platbou výkupného vrátane overenia dostupných teroristických zoznamov.

Záver

Vzhľadom na zvyšujúce sa riziko ransomvérových útokov a potrebu efektívnej reakcie je nevyhnutné, aby sa v rámci EÚ prijali opatrenia inšpirované britským prístupom, ktoré by nastavili jasné pravidlá pre reakciu na požiadavky o výkupné. Cieľom týchto opatrení by mala byť ochrana napadnutých subjektov, zvýšenie účinnosti vyšetrovania a obmedzenie toku financií k páchatel'om.

Jedným z kľúčových opatrení je povinnosť ohlasovania úmyslu zaplatiť výkupné a predbežné posúdenie platby. Všetky subjekty, ktoré nie sú viazané zákazom platieb, by mali mať povinnosť ohlásiť orgánom činným v trestnom konaní svoj úmysel zaplatiť výkupné ešte pred uskutočnením platby. Po prijatí oznámenia by tieto orgány mali poskytnúť poškodenému podporu, vrátane diskusie o možnostiach riešenia bez platenia výkupného. Súčasne by mali vykonať kontrolu legálnosti platby, najmä z hľadiska sankcií voči príjemcovi platby alebo porušenia právnych predpisov o financovaní terorizmu alebo legalizácie výnosov z trestnej činnosti. Ak by neexistovala zákonná prekážka, rozhodnutie o zaplatení by zostalo na poškodenom, pričom celý proces by bol dokumentovaný a monitorovaný.

Zároveň by sa mal zväziť zákaz platieb výkupného pre subjekty kritickej infraštruktúry a verejný sektor. Po vzore návrhu britského ministerstva vnútra by tento zákaz mal zahŕňať všetky orgány verejného sektora a kritické subjekty⁶⁸, ako aj ich významných dodávateľov. Takéto opatrenie by znížilo finančné stimuly pre ransomvérové skupiny, zabránilo páchatel'om financovať ďalšie útoky a ochránilo verejné zdroje pred plytvaním v dôsledku vydierania.

Osobitná pozornosť by sa mala venovať povinnosti včasného nahlásenia ransomvérových útokov a platieb výkupného. Zavedenie povinnosti nahlásenia ransomvérového incidentu do 72 hodín od jeho zistenia by malo byť plošné a nemalo by sa obmedzovať len na subjekty spadajúce pod reguláciu v oblasti kybernetickej bezpečnosti, kde už platí povinnosť

⁶⁸ § 2 písm. c) zákona č. 367/2024 Z.z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov.

hlásiť incidenty. Súčasťou hlásenia by mali byť údaje o uskutočnených alebo plánovaných platbách výkupného, ako aj popis incidentu a rozsah škôd.

Zároveň by sa mal klásť dôraz na budovanie prevencie a zvyšovanie odolnosti voči ransomvérovým útokom. Napadnuté subjekty (poškodení) by mali mať povinnosť prijať a pravidelne aktualizovať plány reakcie na incidenty, ktoré zahŕňajú postupy pri ransomvérových útokoch vrátane rozhodovania o zaplatení výkupného a povinností hlásenia.

Je potrebné zdôrazniť, že úhrada výkupného pri ransomvérovom útoku so sebou nesie významné riziká, ktoré presahujú samotnú stratu dát. Právnická osoba nemusí napriek zaplateniu výkupného dostať dešifrovací kľúč alebo môžu byť jej odcudzené údaje i tak zverejnené alebo predávané. Navyše, ochota platiť výkupné signalizuje útočníkom, že je subjekt zraniteľný a pripravený vyjednávať, čo ho môže vystaviť ďalším útokom.

Okrem toho, úhrada výkupného prináša reputačné, operačné a právne riziká, pričom v prípade regulovaných subjektov, ako sú banky alebo poisťovne, hrozia aj regulačné dôsledky. Logistika samotnej platby môže byť zložitá, keďže väčšina právnických osôb nedisponuje kryptomenovými peňaženkami ani prostriedkami v kryptomenách. Banky môžu odmietnuť realizovať takúto transakciu na základe mechanizmov na predchádzanie praniu špinavých peňazí, financovaniu terorizmu či porušeniu sankčných predpisov.

Vzhľadom na vyššie uvedené riziká je nevyhnutné, aby právnické osoby vypracovali svoj (formálny) rozhodovací proces týkajúci sa reakcie na ransomvérové útoky. Tento proces by mal byť vopred definovaný a schválený vedením právnickej osoby, pričom jeho súčasťou musí byť spravidla validácia právnym oddelením alebo advokátom. Formálny proces môže byť začlenený do širšej politiky organizácie zameranej na riešenie kybernetických incidentov.

Právnická osoba v rámci vnútorného systému compliance má vedieť preukázať aj primeranú na rizikách založenú úroveň kybernetickej bezpečnosti a zavedených bezpečnostných opatrení, predovšetkým v oblasti prevencie a riešenia incidentov. V tomto smere sa prikláňame k odporúčaniam amerického OFAC, ktorý aj v prípade porušenia predpisov úhradou výkupného môže zohľadniť mieru do akej poškodený bol organizačne a technicky pripravený čeliť ransomvérovým útokom. Proaktívne opatrenia, vrátane nastavenia postupov reakcie na kybernetické incidenty, môžu výrazne znížiť riziko porušenia sankcií.

Na overenie, či konkrétny subjekt alebo transakcia neporušujú sankčné pravidlá, by mali organizácie využívať príslušné aktuálne sankčné a teroristické zoznamy. Interný compliance program a rozhodovacie mechanizmy tak predstavujú nevyhnutný základ pre riadenie rizík spojených s ransomvérovými útokmi.

Príspevek je zverejnen pod mezinárodní verzí licence
Creative Commons 4.0 International (CC-BY-4.0).