

<https://doi.org/10.5817/RPT2025-2-1>

# MALWARE JAKO AUTORSKÉ DÍLO: ANALÝZA OCHRANY A JEJÍCH LIMITŮ V EVROPSKÉM PRÁVU

GEORGIA HEJDUKOVÁ<sup>1</sup>

## ABSTRAKT

*Ačkoliv malware může teoreticky požívat formální autorskopravní ochrany, autor takového díla by při pokusu o její vymáhání čelil prakticky nepřekonatelným překážkám. Z procesního hlediska by se podáním žaloby doznal k trestné činnosti, zatímco z hmotněprávního hlediska by jakýkoli nárok paralyzovaly fundamentální právní principy, jako je zákaz zneužití práva či zásady nemo auditur. Současný právní rámec, opírající se o obecné zásady unijního i vnitrostátního práva, tak poskytuje dostatečnou ochranu činnosti antivirových společností a nevyžaduje zavedení nové, specifické legislativní úpravy.*

## KLÍČOVÁ SLOVA

*Malware; autorské právo; reverzní inženýrství; antivirové programy; zneužití práva; evropské právo; kybernetická bezpečnost*

## ABSTRACT

*Although malware may theoretically receive formal copyright protection, its author would face insurmountable obstacles in any attempt at enforcement. From a procedural standpoint, filing a claim would amount to a confession of criminal activity. From a substantive law perspective, any such claim would be neutral-*

---

<sup>1</sup> Georgia Hejduková je studentkou magisterského studijního programu na Právnické fakultě Univerzity Karlovy. Odborně se dlouhodobě zaměřuje na problematiku ochrany lidských práv a práv menšin v kontextu českého ústavního práva i práva mezinárodního. Kontakt: georgia.hejdukova140@student.cuni.cz

*ized by fundamental legal principles, such as the prohibition of the abuse of rights or the nemo auditur principle. Therefore, the existing legal framework, relying on the general principles of both EU and national law, provides sufficient protection for the activities of antivirus companies and does not necessitate the introduction of new, specific legislation.*

## KEYWORDS

*Malware; Copyright Law; Reverse Engineering; Antivirus Software; Abuse of Rights; European Law; Cybersecurity*

## 1. ÚVOD

Počítačová kriminalita představuje dlouhodobý fenomén, který časově předchází i samotnému vzniku internetu, jelikož podle některých autorů se první počítačový útok odehrál už v 70. letech,<sup>2</sup> kdy byl vytvořen jeden z prvních malwarů, který vznikl ještě na ARPANETu.<sup>3</sup> Od té doby se z něj stal celosvětový fenomén, proti němuž se společnost snaží bojovat právními prostředky, ať už formou zákonů, mezinárodních smluv, či zřízením specializovaných institucí. Malware je dnes natolik všudypřítomný, že se z vývoje antivirových programů stal multimilionový trh a některé operační systémy antivirové programy „předinstalovávají“.

Autorské právo v otázce ochrany počítačových programů nezůstalo pozadu a dnes jsou počítačové programy chráněny jako autorská díla ve vnitrostátní i evropské legislativě. Cílem tohoto článku bude zjistit, zda se ochrana autorského práva u počítačových programů vztahuje i na malware a zda mohou antivirové programy, jejichž cílem je tyto programy v počítačových systémech odhalovat a zneškodňovat, svým fungováním, zejména analýzou virů, porušovat majetková práva autorů virů.

Pokud dojde tento článek k závěru, že antivirové programy zasahují do majetkových práv autorů virů, bude předmětem následné analýzy otáz-

---

<sup>2</sup> HILL, Joshua B. – MARION, Nancy E. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. New York: Bloomsbury Publishing USA, 2016.

<sup>3</sup> ARPANET byl předchůdce internetu vyvinutý Ministerstvem obrany USA. Srov. ROSANNE WELCH a PEG A. LAMPHIER. *Technical Innovation in American History: An Encyclopedia of Science and Technology*. Santa Barbara: ABC-CLIO, 2019, s. 16.

ka, zda současný právní systém dokáže autorům antivirových programů poskytnout možnost, jak do práv autorů malwaru oprávněně zasáhnout a pokud současný právní systém záruky neposkytuje, jak by měla být legislativa upravena pro zajištění těchto záruk. Protože je autorské právo na úrovni Evropského hospodářského prostoru harmonizováno zejména pomocí směrnic, zaměří se analýza na tuto dimenzi.

Vzhledem k tomu, že evropské soudy zatím právní otázku ochrany autorských práv u malwaru neřešily, budou úvahy metodologicky vycházet především z heuristiky evropské legislativy, zejména směrnice upravující právní ochranu počítačových programů a dalších směrnic, včetně případné aplikace směrnice Evropské unie o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, tam, kde se výklad týká užití malwaru v Evropském hospodářském prostoru.<sup>4</sup>

## 2. DEFINICE MALWARU A ANTIVIROVÉHO PROGRAMU

Pojem malware etymologicky vychází z anglických slov „malicious“ (zlovolný) a „software“.<sup>5</sup> Označuje počítačový program, jehož primárním účelem je poškodit koncové zařízení uživatele nebo do něj získat neoprávněný přístup. Existuje celá řada typů malwaru, které se liší svými funkcemi a cíli, což se projevuje v různých důsledcích jejich činnosti v napadeném zařízení. Obecně lze však konstatovat, že cílem takového programu je provádět činnost, k níž by oprávněný uživatel neudělil souhlas. Tato definice našla svůj odraz v rozhodnutí Nejvyššího soudu<sup>6</sup> a je reflektována i v trestním zákoníku ve skutkových podstatách trestných činů.<sup>7</sup>

Úmluva o počítačové kriminalitě, známá též jako Budapeštská úmluva, představuje klíčový mezinárodní dokument v této oblasti.<sup>8</sup> Ukládá smluvním stranám povinnost kriminalizovat určené druhy jednání, jako je nezákonný přístup, nezákonný odposlech, zásah do dat, zásah do systému,

<sup>4</sup> Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

<sup>5</sup> AYCOCK, John. *Computer Viruses and Malware*. New York: Springer US, 2006.

<sup>6</sup> Rozsudek Nejvyššího soudu ze dne 27.01.2011, sp. zn. 4 Tz 79/2010.

<sup>7</sup> § 230 až § 232 zákona č. 40/2009 Sb., trestní zákoník.

<sup>8</sup> Smlouva č. 104/2013 Sb. m. s Úmluva o počítačové kriminalitě.

zneužití zařízení, počítačové padělání či počítačový podvod.<sup>9</sup> Samotná Úmluva však neobsahuje legální definici pojmu malware. Pro jeho vymezení je proto nutné vycházet z odborné literatury či z navazující judikatury. Odborná literatura malware definuje například jako počítačový program, který zasahuje do jiného počítačového programu a způsobuje, že se jeho zamýšlená funkce odlišuje od té, která je skutečně vykonána.<sup>10</sup>

Oproti tomu antivirový software je určen k ochraně koncového zařízení před napadením malwarem.<sup>11</sup> Širším a v současnosti přesnějším termínem je antimalware,<sup>12</sup> který označuje software aktivně analyzující soubory v zařízení. Za využití metod, jako je reverzní inženýrství, analyzuje strukturu a fungování škodlivého kódu. Získané informace a signatury následně uchovává ve svých databázích, aby byl schopen malware efektivně detekovat.<sup>13</sup> Tento proces umožňuje neustálé zdokonalování ochrany a zajištění vyšší úrovně bezpečnosti pro uživatele.

### 3. LIMITY AUTORSKOPRÁVNÍ OCHRANY MALWARU

#### 3.1 OBECNÁ VÝCHODISKA OCHRANY PRO POČÍTAČOVÉ PROGRAMY

Ačkoliv je účelem malwaru zpravidla protiprávní činnost, z hlediska autorského práva se může jednat o standardní počítačový program. Pokud takový program splňuje obecné pojmové znaky autorského díla, požívá právní ochrany jak v České republice, tak v celém Evropském hospodářském prostoru. Tuto ochranu harmonizuje směrnice o právní ochraně počí-

---

<sup>9</sup> GŘIVNA, Tomáš, DVOŘÁK, Marek. § 230 In: ŠÁMAL, Pavel a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 2949.

<sup>10</sup> KRAMER, Simon – BRADFIELD, Julian C. A general definition of malware. *Journal in Computer Virology*. 2010, roč. 6, č. 2., ISSN s. 105.

<sup>11</sup> NAYAK, Umeha. Malicious Software and Anti-Virus Software. In: *The InfoSec Handbook*. Apress, 2014. ISBN 9781430263838. Dostupné z: [https://doi.org/10.1007/978-1-4302-6383-8\\_7](https://doi.org/10.1007/978-1-4302-6383-8_7) s. 156.

<sup>12</sup> ROSENCRANCE, Linda. What is antimalware? *TechTarget* [online] [cit. 2024-03-28]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/antimalware>.

<sup>13</sup> LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS: Establishing Protection for Authors Irrespective of the Merits of Their Creation*. 2010, Diplomová práce, University of Oslo s. 40.

tačových programů.<sup>14</sup> Uvedená směrnice vymezuje podmínky ochrany, stanovuje dovozené způsoby zásahu do autorských práv tvůrců a definuje mechanismy pro zajištění této ochrany v rámci EHP<sup>15</sup>.

## 3.2 LIMITY OBECNÝCH VÝCHODISEK PRO ANTIVIROVÉ PROGRAMY

### 3.2.1 ZÁKONNÉ LICENCE A JEJICH APLIKACE NA MALWARE

Vycházíme-li z premisy, že i malware jako počítačový program požívá autorskoprávní ochrany,<sup>16</sup> vyvstává zásadní otázka, zda by tato ochrana neměla být limitována s ohledem na jeho protiprávní účel. Tuto kolizi mezi individuálním autorským právem a veřejným zájmem lze posuzovat optikou již existujících omezení autorského práva. Prvním příkladem takových omezení jsou zákonné licence, které autorský zákon výslovně upravuje.

Mezi zákonné licence patří například licence pro citační účely, pro využití díla ve prospěch osob se zdravotním postižením nebo pro účely vyučování a vědeckého výzkumu. Zásadní je rovněž licence umožňující užití díla v zájmu veřejné bezpečnosti. Pro další analýzu jsou relevantní pouze licence pro vyučování, vědecký výzkum a veřejnou bezpečnost, neboť ostatní zákonné licence nejsou pro posouzení autorskoprávní ochrany malwaru aplikovatelné.<sup>17</sup>

Uplatnění výjimky pro vědecký výzkum a výuku je limitováno požadavkem, aby daná činnost nesledovala přímý ani nepřímý hospodářský prospěch.<sup>18</sup> Tato restrikce sice umožňuje analýzu malwaru v akademickém

---

<sup>14</sup> Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

<sup>15</sup> Evropský hospodářský prostor.

<sup>16</sup> Obecně, pokud malware naplní znaky počítačového programu podle § 2. odst. 2 autorského zákona chráněn spíše je, nicméně autor nebude z důvodu aplikace § 6 občanského zákoníku (OZ) moci z této ochrany těžit. Viz HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525. Praha: Wolters Kluwer Česká republika, 2019.

<sup>17</sup> Čl. 5 odst. 3 Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

<sup>18</sup> LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 49.

prostředí, avšak výrazně omezuje její aplikační potenciál v praxi. Představuje totiž bariéru pro komerční subjekty, které hrají klíčovou roli v detekci a analýze kybernetických hrozeb.

Alternativním právním titulem by mohla být tzv. úřední licence, jež v rovině unijního práva zahrnuje i užití pro účely veřejné bezpečnosti.<sup>19</sup> V podmínkách českého právního řádu je však subsumpce analýzy malwaru pod toto ustanovení vyloučena. Rozsah § 34 autorského zákona totiž nekryje veřejný zájem v jeho obecné rovině. Odborná literatura konzistentně dovozuje, že tuto zákonnou licenci lze aplikovat pouze na základě specifického zákonného zmocnění pro úřední účely.<sup>20</sup> Teleologickým východiskem této licence není ochrana veřejné bezpečnosti *per se*, nýbrž zajištění výkonu pravomocí orgánů veřejné moci.<sup>21</sup> Z tohoto důvodu nelze úřední licenci pro účely reverzního inženýrství využít.

### 3.2.2 NELEGÁLNÍ JEDNÁNÍ AUTORŮ MALWARU JAKO DŮVOD PRO ODEPŘENÍ OCHRANY AUTORSKÝM PRÁVEM

Klíčový argument pro odepření autorskoprávní ochrany malwaru spočívá v rozporu s dobrými mravy a veřejným pořádkem. Tato fundamentální soukromoprávní zásada brání tomu, aby výkon subjektivního práva vedl k následkům, které jsou v příkrém rozporu se společensky uznávanými hodnotami. Poskytnutí soudní ochrany dílu, jehož primárním účelem je páchání protiprávní činnosti, by naplňovalo znaky zneužití práva (§ 8 občanského zákoníku). Právní řád nemůže legitimovat nástroje určené k jeho vlastnímu porušování, neboť by tím popřel svůj základní smysl a dostal se do neřešitelného vnitřního rozporu.

Opozici vůči morálnímu korektivu tvoří objektivní charakter autorskoprávní ochrany. Mezinárodní smluvní rámec (Bernská úmluva,

<sup>19</sup> Viz § 34 autorského zákona či čl. 5 odst. 3 písm. e) směrnice o Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

<sup>20</sup> CHALOUPKOVÁ, Helena, HOLÝ, Petr. *Autorský zákon*. 6. vydání. Praha: C. H. Beck, 2023, s. 105. Srov. HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů)*: komentář, s. 339–353.

<sup>21</sup> TELEC, Ivo, TŮMA, Pavel. *Autorský zákon*. 2. vydání. Praha: C. H. Beck, 2019, s. 413.

Smlouva WIPO),<sup>22</sup> neumožňuje odepřít ochranu dílu pouze na základě jeho protiprávního původu či účelu. Moderní autorské právo je ovládáno zásadou, že ochrana svědčí každému dílu *ex lege*, nehledě na jeho estetickou či morální kvalitu.<sup>23</sup> Tento doktrinální rozpor lze demonstrovat na příkladu street artu. I v případech, kdy vznik díla naplňuje skutkovou podstatu trestného činu (např. sprejerství), zůstává autorskoprávní status nedotčen. Právní teorie důsledně odděluje vlastnické právo k hmotnému nosiči a nehmotný statek. Splňuje-li výtvar generální klauzuli autorského díla, požívá ochrany bez ohledu na protiprávnost jednání, které vedlo k jeho vzniku.<sup>24</sup>

Princip ochrany dobrých mravů se promítl například do amerického případu *Villa v. Pearson Education*, který relativizoval neomezenou ochranu děl street artu. Ačkoliv soud v dané fázi řízení nerozhodl ve věci samé, připustil možnost, že autorům graffiti nemusí být autorskoprávní ochrana přiznána právě pro rozpor se zásadou zákazu těžit z vlastní nepoctivosti (*nemo auditur*).<sup>25</sup> V českém právním řádu plní obdobnou funkci generální klauzule obsažená v občanském zákoníku. Zejména § 6 odst. 2 OZ stanoví, že nikdo nesmí těžit z vlastního protiprávního činu.<sup>26</sup> Dle rozhodnutí Nejvyššího soudu se lze těchto obecných principů, jako je zásada poctivosti, dovolat vždy jako korektivu i tam, kde to zákon výslovně neuvádí.<sup>27</sup> Na úrovni Evropského hospodářského prostoru však podobné ustanovení nenajdeme. Lze tedy konstatovat, že z celoevropského hlediska neexistuje jednotná úprava.<sup>28</sup>

Nicméně je nutné dodat, že využití malwaru nemusí být pouze protiprávní. Malware může být vyráběn například i pro vědecké účely či pro

<sup>22</sup> LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 50.

<sup>23</sup> LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 50.

<sup>24</sup> ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*. 7. American Bar Association, 2015. ISSN 1942-7239, s. 48.

<sup>25</sup> ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*, s. 49.

<sup>26</sup> HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525.

<sup>27</sup> Rozsudek Nejvyššího soudu ze dne 18. 3. 2019, sp. zn. 26 Cdo 1984/2018.

<sup>28</sup> Směrnice Evropského parlamentu a Rady 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu, Úř. věst. OJ L 130.

účely testování antimalware programů. Tyto situace lze však označit za vysoce specifické. V takovém případě by ochrana na principu zneužití práva a dobrých mravů nemohla obstát a autor by se mohl své autorskoprávní ochrany domáhat standardním způsobem.<sup>29</sup> Takový scénář je však vysoce nepravděpodobný, jelikož vývoj tohoto softwaru se zpravidla odehrává interně v rámci jedné společnosti a kód není určen pro veřejnost. Dojde-li k úniku, bude se primárně řešit porušení obchodního tajemství, nikoliv otázka autorství.

### 3.3 OCHRANA ZÁKLADNÍCH PRÁV JAKO ODŮVODNĚNÍ MOŽNOSTI ZÁSAHU

#### 3.3.1 OBECNÁ VÝCHODISKA VEŘEJNÉHO ZÁJMU V AUTORSKÉM PRÁVU

Východiskem celé analýzy je střet dvou protichůdných principů. Na jedné straně stojí formální autorskoprávní ochrana malwaru jako počítačového programu. Na straně druhé je činnost antivirových společností, která do tohoto práva z podstaty věci zasahuje reverzním inženýrstvím a dalšími analytickými metodami. Aby tato činnost, která je nezbytná pro ochranu společnosti, mohla být považována za legální, je nutné dospět k závěru, že výkon autorských práv tvůrce malwaru je v tomto specifickém případě omezen vyšším veřejným zájmem na kybernetické bezpečnosti.

Ochrana autorského práva je nedílnou součástí práva na ochranu majetku. Toto základní právo je zakotveno jak v čl. 11 Listiny, tak v čl. 1 Dodatkového protokolu k Evropské úmluvě o lidských právech (EÚLP).<sup>30</sup> Rozhodnutí Evropského soudu pro lidská práva (ESLP) připouští zásah do vlastnického práva, pokud je takový zásah v souladu se zákonem, sleduje legitimní cíl ve veřejném zájmu a je přiměřený sledovanému cíli.<sup>31</sup>

Právě judikatura ESLP představuje vhodný rámec pro analýzu této problematiky v kontextu Evropského hospodářského prostoru. Všechny

<sup>29</sup> Děkuji anonymnímu recenzentovi za upozornění na tuto situaci.

<sup>30</sup> Rozsudek velkého senátu ESLP ze dne 11.1.2007, *Anheuser-Busch Inc. proti Portugalsku*, č. 73049/01, § 63.

<sup>31</sup> Rozsudek velkého senátu ESLP ze dne 13.12.2016, *Bélané Nagy proti Maďarsku*, č. 53080/13, § 71.

členské státy EU jsou totiž zároveň smluvními stranami EÚLP a judikatura ESLP k ochraně majetku je podstatně rozvinutější než judikatura Soudního dvora EU. Proto bude soulad zásahu do práv tvůrců malwaru posuzován optikou testu proporcionality, jak jej aplikuje ESLP.

### 3.3.2 ZÁSAH DO VLASTNICKÝCH PRÁV AUTORŮ MALWARU VE VEŘEJNÉM ZÁJMU

Judikatura ESLP uznává širokou škálu legitimních veřejných zájmů, které mohou odůvodnit omezení vlastnického práva. Od sociální spravedlnosti přes hospodářskou regulaci až po prevenci daňových úniků.<sup>32</sup> Ačkoliv ESLP dosud výslovně neřešil otázku omezení autorských práv u děl vytvořených za účelem poškodit třetí stranu (jako je malware), argument pro takové omezení lze dovést z jeho stávající judikaturní linie. Takový argument lze postavit nejen na analogii z konkrétních rozhodnutí, kde Soud připustil omezení práv v zájmu ochrany společnosti před jinými druhy hrozeb, ale i na aplikaci obecných principů, kterými ESLP vymezuje a limituje pojem „veřejný zájem“.

Z judikatury ESLP lze dovést obecný princip, že ochranu majetku je možné omezit za účelem prevence trestné činnosti. Například v případě Butler proti Spojenému království Soud akceptoval zabavení peněz, které mohly sloužit k pašování drog,<sup>33</sup> a v případě *Hentrich proti Francii* shledal legitimním obdobný zásah v zájmu prevence daňových úniků.<sup>34</sup>

Mezi těmito případy a problematikou malwaru nicméně existuje zásadní rozdíl. V citovaných kauzách se jednalo o dočasné omezení práv k legitimnímu majetku (penězům), který mohl být ke spáchání trestného činu teprve použit. Oproti tomu malware je nástroj, jehož samotná podstata a účel jsou protiprávní. Nejde zde tedy o dočasnou prevenci, ale o trvalou

<sup>32</sup> Například eliminace sociální nerovnosti Srov. Rozsudek pléna ESLP ze dne 21.2.1986 *James a ostatní proti Spojenému království*, č. 8793/79, nacionalizace specifických průmyslů Srov. Rozsudek pléna ESLP ze dne 8.7.1986 *Lithgow a ostatní proti Spojenému království* č. 9006/80, 9262/8, 9263/81, 9265/81, 9266/81, 9313/81, 9405/81, nebo třeba prevence daňových úniků Srov. Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88.

<sup>33</sup> Rozhodnutí ESLP ze dne 27.6.2002, *Butler proti Spojenému království*, č. 41661/98.

<sup>34</sup> Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88, § 39.

potřebu společnosti bránit se nástroji určenému ke škodlivé činnosti. Nicméně i přesto, že se tyto případy liší, lze prevenci kriminality označit za legitimní veřejný zájem.

### 3.3.3 ZÁKONNOST ZÁSAHU DO PRÁV AUTORŮ MALWARU

Druhou podmínkou pro jakýkoli zásah do vlastnického práva je, že musí být v souladu se zákonem.<sup>35</sup> To znamená, že omezení práva musí mít oporu v platném právním předpise.

Na úrovni Evropského hospodářského prostoru sice neexistuje specifický zákon, který by tuto problematiku řešil, avšak dostatečný právní základ poskytují obecné principy. Jak již bylo zmíněno, jedná se zejména o zákaz zneužití práva, zakotvený v čl. 54 Listiny základních práv EU, který funguje jako univerzální korektiv.

Pro účely testu ESLP je však existence těchto obecných a univerzálně aplikovatelných zásad, jako je zákaz zneužití práva, dostatečným zákonným základem pro omezení ochrany.

### 3.3.4 PROPORCIONALITA

Posledním krokem testu je posouzení, zda je zásah do práv tvůrce malwaru přiměřený (proporcionální). To vyžaduje poměření dvou konkurenčních zájmů: na jedné straně veřejného zájmu na zajištění kybernetické bezpečnosti a ochraně majetku a soukromí milionů uživatelů, a na straně druhé majetkového zájmu autora v díle, jehož jediným účelem je tato práva porušovat.

Při konečném poměrování je zřejmé, že zájem společnosti na ochraně před protiprávními útoky musí převážit. Zásah do autorských práv tvůrce malwaru, který umožňuje se těmto útokům bránit, tak nejenže splňuje test proporcionality, ale je i opatřením nezbytným v demokratické společnosti.<sup>36</sup>

Důvodem je, že malware nepředstavuje hrozbu jen pro osobní údaje jednotlivců, ale může způsobit i kolaps kritické infrastruktury, od nemocnic po energetické sítě, a to například prostřednictvím ransomwaru. Ochrana této infrastruktury je tak klíčovým bezpečnostním zájmem státu.

<sup>35</sup> Čl. 1 dodatkového protokolu č. 1 Úmluvy o ochraně lidských práva a základních svobod.

<sup>36</sup> Rozsudek velkého senátu ESLP ze dne 5.1.2000, *Beyeler proti Itálii*, č. 33202/96, § 107.

Tuto ochranu v praxi z velké části zajišťují soukromé společnosti (např. McAfee, Symantec), které investují značné prostředky do analýzy hrozeb.<sup>37</sup> Tyto společnosti sice z těchto komerčních aktivit mají nemalý zisk, lze ale argumentovat, že bez možnosti analyzovat malware pomocí reverzního inženýrství by jakákoliv iniciativa malware odhalovat a potlačovat, ať již státem organizovaná či soukromá, byla nemožná. Jejich činnost, ač komerční, je nepostradatelná. Bez možnosti analyzovat škodlivý kód pomocí reverzního inženýrství by byla jakákoliv efektivní obrana zcela iluzorní. Z tohoto důvodu je nepochybné, že veřejný zájem na kybernetické bezpečnosti musí mít přednost. Ochrana, kterou autorské právo formálně poskytuje tvůrcům malwaru, tak musí být prolomitelná, aby bylo možné zajistit funkčnost a bezpečnost digitální společnosti.

K bezpečnostnímu argumentu se navíc řadí i důvod ekonomický. Kyberkriminalita každoročně způsobuje globální ekonomice škody v řádech bilionů dolarů.<sup>38</sup> Pokud by antivirové společnosti nemohly malware efektivně analyzovat a neutralizovat, tyto již tak astronomické ztráty by dále exponenciálně rostly. Ochrana ekonomiky před těmito dopady je tak dalším pádným důvodem, proč musí veřejný zájem převážet nad formální autorskoprávní ochranou malwaru.

Součástí testu proporcionality je i posouzení, zda nelze sledovaného cíle dosáhnout méně invazivními prostředky.<sup>39</sup> V případě malwaru je toto kritérium splněno, neboť neexistuje jiný efektivní způsob jeho detekce než analýza jeho kódu a chování. Ačkoliv se plošné omezení autorského práva může jevit jako radikální, pro zajištění kybernetické bezpečnosti je nezbytné.

Je důležité zdůraznit, že autor malwaru neztrácí svá práva zcela. Omezení se vztahuje výhradně na úkony nezbytné pro analýzu a neutralizaci

---

<sup>37</sup> RODRIGUEZ, Miranda. All Your IP Are Belong to Us: An Analysis of Intellectual Property Rights as Applied to Malware. *Texas A&M Law Review*. 2016, roč. 3, č. 3. ISSN 2837-5165, s. 665.

<sup>38</sup> MORGAN, Steve. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. *Cybercrime Magazine* [online]. 8. 12. 2018 [cit. 2024-03-22]. Dostupné z: <https://cybersecurity-ventures.com/cybercrime-damages-6-trillion-by-2021/>.

<sup>39</sup> Rozsudek ESLP ze dne 11.2.2020, *Vaskrsić proti Slovinsku*, č. 31371/12, § 83.

hrozby. Jakékoli jiné užití díla (např. komerční reprodukce) by nadále vyžadovalo jeho svolení. Tvůrce softwaru určeného ke škodlivé činnosti však musí nést zvýšenou míru tolerance vůči zásahům, které slouží k ochraně společnosti.

Problematičtější se může jevit skutečnost, že toto omezení dopadá i na tvůrce legitimního softwaru. Antivirový program z podstaty své funkce musí analyzovat všechny programy, nikoli jen ty škodlivé. Tento plošný zásah je však odůvodněn povahou hrozby. Potenciálně nebezpečný může být jakýkoli kód. Jde tedy o široké, avšak s ohledem na neexistenci alternativ proporcionální omezení.

Při konečném poměřování je zřejmé, že veřejný zájem na fungující a bezpečné digitální infrastruktuře jednoznačně převažuje nad zájmem na absolutní ochraně autorských práv k softwaru. Autorskoprávní ochrana v důsledku činnosti antivirových programů nemizí, je pouze v nezbytně nutné míře omezena ve prospěch vyššího celospolečenského cíle.

#### 4. MALWARE A ANTIVIROVÉ PROGRAMY

Základní funkce antivirového softwaru spočívá v analýze malwaru. Tímto jednáním však nevyhnutelně dochází k užití cizího autorského díla ve smyslu § 12 a násl. autorského zákona. Pokud tedy přijmeme premisu, že malware je chráněným dílem, antivirové společnosti svou činností zasahují do majetkových práv jeho tvůrců.

Klíčovou metodou této analýzy je reverzní inženýrství,<sup>40</sup> definované jako proces dekonstrukce finálního produktu za účelem zjištění jeho vnitřního fungování. V kontextu softwaru to umožňuje odhalit charakteristiky a zamýšlené funkce škodlivého kódu.<sup>41</sup> Cílem je identifikovat jeho chování nebo nalézt zranitelnost, která umožní jeho neutralizaci. Uplatňují se přitom dvě základní techniky.

---

<sup>40</sup> Reverzní inženýrství bylo předmětem právního sporu v USA, kde získalo definici jako „proces, kdy začneme s finálním produktem a pracujeme tím, že ho rozmontujeme a zjišťujeme, jak funguje a jak byl vyroben“ Srov. *Secure Services Tech. v. Time and Space Processing*, 722 F. Supp. 1354 (E.D. Va. 1989).

<sup>41</sup> VIGNA Giovanni. *Static Disassembly and Code Analysis*, Christodorescu, Mihai. *Malware detection*. New York: Springer, 2006. ISBN 1-280-80436-X., s. 28.

První takovou technikou je dynamická analýza, která spočívá v monitorování běžícího programu a sledování příkazů, které zadává operačnímu systému a hardwaru. Druhou technikou je následně statická analýza, která představuje zkoumání samotného binárního kódu programu bez jeho spuštění.<sup>42</sup>

Směrnice o právní ochraně počítačových programů<sup>43</sup> skutečně stanovuje určité výjimky z výlučného práva autora. Klíčový je čl. 5, který oprávněnému nabyvateli licence umožňuje bez dalšího svolení zkoumat, studovat a zkoušet funkčnost programu za účelem zjištění jeho základních myšlenek a zásad.<sup>44</sup> Stejně tak smí provádět úpravy nezbytné pro zamýšlené užití programu, včetně opravy chyb. Tato ustanovení však nelze vykládat extenzivně – neopravňují například k dekompilaci za účelem vytvoření konkurenčního produktu.

Nabízí se tedy otázka, zda se antivirové společnosti mohou této výjimky dovolat. Takový výklad je však neudržitelný, a to ze dvou klíčových důvodů. Za prvé se vztahují pouze na oprávněného nabyvatele licence. Antivirová společnost analyzující malware, který se šíří protiprávně, nikdy není v pozici oprávněného nabyvatele, s výjimkou případů, kdyby si nechala od autora udělit licenci. Toto si sice lze těžko představit, ale je to teoreticky možné. Za druhé samotným cílem antivirové analýzy je malware neutralizovat a zničit, nikoliv ho užívat k zamýšlenému účelu či dosáhnout interoperability. Taková činnost jde zjevně nad rámec účelu, pro který směrnice výjimky stanovila.<sup>45</sup>

Pokud však odhlédneme od této formálněprávní roviny, je nepředstavitelné, že by se autor malwaru u soudu úspěšně domohl ochrany. Jeho případný nárok by byl vyloučen fundamentálními principy soukromého práva. Jakýkoli soud by takovou žalobu s největší pravděpodobností zamítl s odkazem na zákaz zneužití práva a obecnou zásadu, že nikdo nesmí těžit

<sup>42</sup> VIGNA Giovanni. *Static Disassembly and Code Analysis*, s. 29.

<sup>43</sup> Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

<sup>44</sup> Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

<sup>45</sup> LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 14.

z vlastního protiprávního činu. I přesto, že autor tak formálně svůj nárok neztrácí a teoreticky jej může licencovat, tak je takové právo jen těžko před orgány veřejné moci vymahatelné.

## 5. DOSTATEČNOST SOUČASNÉ LEGISLATIVNÍ ÚPRAVY A ÚVAHY DE LEGE FERENDA

Tato kapitola posuzuje, zda je současná unijní legislativa dostatečná pro omezení autorských práv tvůrců malwaru. Jak bylo ukázáno, evropské směrnice s existencí děl vytvořených za protiprávním účelem výslovně nepočítají, což ponechává řešení na aplikaci obecných právních principů, jako je zákaz zneužití práva.<sup>46</sup> Vystává proto otázka, zda by bylo vhodnější přijmout explicitní legislativní úpravu.

První zvažovanou možností je rozšíření stávajících zákonných licencí, což by muselo být v souladu s tzv. třístupňovým testem Bernské úmluvy.<sup>47</sup> Konkrétně by šlo o extenzivní výklad úřední licence zakotvené v informační směrnici.

Tento přístup by nevyžadoval novelizaci směrnice, nýbrž změnu výkladu Soudního dvora EU. Soud by musel dovodit, že licenci mohou využít i soukromé subjekty (antivirové společnosti), pokud tím prokazatelně chrání veřejný zájem. Proti takovému výkladu však stojí značné riziko zneužití. Šlo by o široký průlom do systému licencí kvůli relativně úzkému problému, což by mohlo narušit právní jistotu a otevřít dveře pro nepředvídatelné aplikace v jiných oblastech.

Druhou teoretickou možností je zavedení nové generální klauzule, která by umožnila omezit autorskopravní ochranu v případě rozporu s veřejným zájmem. Klíčovou otázkou však zůstává, zda je taková legislativní změna nezbytná. V praxi neexistují případy, kdy by se autor malwaru úspěšně domáhal ochrany svých autorských práv proti antivirové společnosti. Historicky je sice znám pokus autorů Zetus Rootkitu zakázat reverzní inženýrství

---

<sup>46</sup> Konkrétně čl. 54 Listiny základních práv Evropské unie, který zakazuje zneužití práva.

<sup>47</sup> Třístupňový test Bernské úmluvy je test, který vychází z čl. 9 odst. 2 Bernské úmluvy a stanovuje limity na výjimky z ochrany majetkových práv autora k dílu.

a analýzu jejich kódu prostřednictvím licenčních podmínek (EULA),<sup>48</sup> avšak vymahatelnost takových podmínek je považována za čistě hypotetickou.<sup>49</sup> Autor malwaru by se navíc podáním žaloby fakticky sebeobvinil z trestné činnosti.

Především však platí, že nástroje pro řešení takové situace již existují, a to na národní i unijní úrovni. Jakýkoli pokus o zneužití autorského práva k ochraně malwaru by narazil na již zmiňovaný § 6 OZ,<sup>50</sup> a v právu Evropské unie na Listinu základních práv EU.<sup>51</sup> Z těchto důvodů lze konstatovat, že stávající právní rámec, opírající se o obecné právní zásady, je pro ochranu činnosti antivirových společností plně dostačující.

Ačkoliv se může zdát myšlenka žaloby podané tvůrcem malwaru absurdní, nelze ji zcela vyloučit. Spory vedené autory street artu ukazují, že i díla na hraně legality si mohou nárokovat ochranu. Přesto by takový pokus v případě malwaru narazil na dvě takřka nepřekonatelné překážky.

První je procesní povahy: žalobce by se podáním žaloby fakticky doznal k jednání, které je ve většině jurisdikcí klasifikováno jako trestný čin, a vystavil by se tak riziku trestního stíhání. Druhá překážka je hmotněprávní: i kdyby soud formální ochranu dílu přiznal, samotný výkon práva by byl znemožněn fundamentálními právními principy, jako jsou právě výše zmíněné zásady zákazu těžít z vlastní nepoctivosti (zásada *nemo auditur*), či zjevného zákazu zneužití práva.

Lze tedy shrnout, že ačkoliv specifické autorskoprávní směrnice EU postrádají výslovnou výjimku pro analýzu malwaru, současný právní rámec je plně dostačující. Ochranu antivirovým společnostem poskytují obecné zásady a korektivy obsažené jak v primárním právu EU, tak v národních občanských zákonících. Vzhledem k hypotetické povaze těchto sporů není

---

<sup>48</sup> RODRIGUEZ, Miranda. *All Your IP Are Belong to Us*. s. 665-666.

<sup>49</sup> DOCTOROW, Cory. *Malware gets a EULA. Boing Boing* [online]. 28. 4. 2008 [cit. 2024-03-27]. Dostupné z: <https://boingboing.net/2008/04/29/malware-gets-a-eula.html>. KDAWSON. *EULAs For Malware. Slashdot* [online]. 28. 4. 2008 [cit. 2024-03-27]. Dostupné z: <https://slashdot.org/story/08/04/29/0057236/eulas-for-malware>.

<sup>50</sup> Viz HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525.

<sup>51</sup> Listina základních práv Evropské unie ze dne 26.10.2012, Úř. věst. OJ C 202, 7.6.2016.

nutné přijímat novou legislativu; stávající právní řád si s tímto problémem dokáže efektivně poradit prostřednictvím soudního výkladu.

## 6. ZÁVĚR

Předkládaný článek analyzuje způsobilost malwaru být předmětem autorskoprávní ochrany a kolizi této ochrany s činností bezpečnostního softwaru (antimalware). Text konstatuje, že malware, jakožto počítačový program, naplňuje definiční znaky díla dle autorského zákona, a tudíž požívá ochrany bez ohledu na svou škodlivou povahu.

Autorka však zároveň dovozuje, že faktická vymahatelnost těchto subjektivních práv je nulová. Soudní vymáhání by nutně vedlo k sebeobvinění autora z trestné činnosti a nárok by byl s vysokou pravděpodobností zamítnut na základě zákazu zneužití práva či zásady *nemo auditur*.

V kontextu antivirových programů článek potvrzuje, že dochází k užití cizího autorského díla, které nelze subsumovat pod stávající zákonné licence. Tento zásah je však legitimizován převažujícím veřejným zájmem na ochraně kybernetické infrastruktury. Závěrem je konstatováno, že ačkoliv jsou úvahy *de lege ferenda* možné, stávající judikатурní nástroje a obecné právní principy poskytují pro řešení těchto hypotetických sporů dostatečný rámec.

## 7. SEZNAM POUŽITÝCH ZDROJŮ

- [1] AYCOCK, John. *Computer Viruses and Malware*. New York, NY: Springer US, 2006. ISBN 1-280-71620-7. Dostupné z: <https://doi.org/10.1007/0-387-34188-9>.
- [2] DOCTOROW, Cory. *Malware gets a EULA*. *Boing Boing* [online]. 28. 4. 2008 [cit. 27.03.2024]. Dostupné z: <https://boingboing.net/2008/04/29/malware-gets-a-eula.html>.
- [3] MICROSOFT. *Does Windows 11 Need Antivirus on Laptops?* | Microsoft Surface. In: *Microsoft* [online] [cit. 2024-03-28]. Dostupné z: <https://www.microsoft.com/en-us/surface/do-more-with-surface/does-windows-11-need-antivirus-on-laptops> > .
- [4] ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*. 7. American Bar Association, 2015. ISSN 1942-7239.
- [5] GRÍVNA, Tomáš, DVOŘÁK, Marek. § 230. ŠÁMAL, Pavel a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023.
- [6] HILL, Joshua B. – MARION, Nancy E. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. New York: Bloomsbury Publishing USA, 2016 .

- [7] HOLCOVÁ, Irena; KŘEŠŤANOVÁ, Veronika; DOBŘICHOVSKÝ, Tomáš; CÍSAŘOVÁ, Zuzana; ŽIKOVSKÁ, Petra et al. Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář. Praha: Wolters Kluwer Česká republika, 2019. ISBN 978-80-7598-049-6.
- [8] CHALOUPKOVÁ, Helena, HOLÝ, Petr. *Autorský zákon*. 6. vydání. Praha: C. H. Beck, 2023.
- [9] KRAMER, Simon a Julian C. BRADFIELD. A general definition of malware. *Journal in Computer Virology*. 2010, roč. 6, č. 2. ISSN 1772-9890.
- [10] LUNDE, Jeremy S. *Copyright protection for virus authors*. Establishing Protection for Authors Irrespective of the Merits of Their Creation. Oslo, 1.12.2010, 65, Diplomová práce, University of Oslo.
- [11] MORGAN, Steve. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025 In: *Cybersecurity ventures* [online]. 2018 [cit. 22.03.2024]. Dostupné z: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
- [12] NAYAK, Umesha. Malicious Software and Anti-Virus Software. *The InfoSec Handbook*. Apress, 2014. ISBN 9781430263838.
- [13] RODRIGUEZ, Miranda. All Your IP Are Belong to Us: An Analysis of Intellectual Property Rights as Applied to Malware. *Texas A&M Law Review*. 2016, roč. 3, č. 3. DOI: 10.37419/LR.V3.13.7. ISSN 2837-5165
- [14] ROSENCRANCE, Linda. What is antimalware? In: *TechTarget* [online] [cit. 28.03.2024]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/antimalware>.
- [15] VIGNA Giovanni. Static Disassembly and Code Analysis CHRISTODORESCU, Mihai. *Malware detection*. New York: Springer, 2006. ISBN 1-280-80436-X.
- [16] Listina základních práv Evropské unie ze dne 26.10.2012, Úř. věst. OJ C 202, 7.6.2016.
- [17] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, Úř. věst. OJ L 167, 22.6.2001.
- [18] Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.
- [19] Smlouva č. 104/2013 Sb. m. s. Úmluva o počítačové kriminalitě.
- [20] Smlouva č. 209/1992 Sb. m. s. Úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 1, 2, 4, 6, 7.
- [21] Rozhodnutí ESLP ze dne 27.6.2002, *Butler proti Spojenému království*, č. 41661/98.
- [22] Rozsudek ESLP ze dne 11.2.2020, *Šeiko proti Litvě*, č. 82968/17, § 30.
- [23] Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88.
- [24] Rozsudek Nejvyššího soudu ze dne 18. 3. 2019, sp. zn. 26 Cdo 1984/2018.
- [25] Rozsudek Nejvyššího soudu ze dne 27.01.2011, sp. zn. 4 Tz 79/2010.

[26] Rozsudek pléna ESLP ze dne 21.2.1986, *James a ostatní proti Spojenému království*, č. 8793/79.

[27] Rozsudek pléna ESLP ze dne 8.7.1986, *Lithgow a ostatní proti Spojenému království*, č. 9006/80, 9262/8, 9263/81, 9265/81, 9266/81, 9313/81, 9405/81.

[28] Rozsudek velkého senátu ESLP ze dne 11.1.2007, *Anheuser-Busch Inc. proti Portugalsku*, č. 73049/01.

[29] Rozsudek velkého senátu ESLP ze dne 13.12.2016, *Bélané Nagy proti Maďarsku*, č. 53080/13.

[30] Rozsudek velkého senátu ESLP ze dne 5.1.2000, *Beyeler proti Itálii*, č. 33202/96.

[31] *Secure Services Tech. v. Time and Space Processing*, 722 F. Supp. 1354 (E.D. Va. 1989).

---

*Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).*

---