11.
Jakými nástroji bude EU čelit kybernetické kriminalitě?

What Tools Will the EU Use to Fight Cyber Crime?

Tomáš Gřivna

Univerzita Karlova, vedoucí katedry trestního práva, advokát a společník Advokátní kanceláře Gřivna & Šmerda, s.r.o.

Charles University, Head of the Department of Criminal Law, defense lawyer and partner of the Law firm Gřivna & Šmerda, s.r.o.

Abstrakt: Příspěvek se zaměřuje na předestření a kritické zhodnocení navržených právních nástrojů, jimiž má EU čelit setrvale se vyskytující a na nebezpečnosti narůstající kybernetické kriminalitě. Pozornost je zaměřena například na otázky boje proti šíření protiprávního obsahu na internetu nebo na ryze aktuální aspekty související se zajišťováním elektronických důkazů. Autor rozebírá odpovědnost poskytovatelů zprostředkovatelských služeb za protiprávní obsah a povinnost poskytovatelů zprostředkovatelských služeb poskytnout součinnost donucovacím orgánům ve vztahu k protiprávnímu obsahu a k elektronickým důkazům.

Summary: The contribution focuses on the presentation and critical evaluation of the proposed legal instruments with which the EU is supposed to face the persistently occurring and increasingly dangerous cybercrime. Attention is focused, for example, on issues of combatting the spread of illegal content on the Internet or on profoundly topicl issues related to securing electronic evidence. The author discusses the responsibility of providers of intermediary services for illegal content and the obligation of providers of intermediary services to cooperate with law enforcement authorities in relation to illegal content and electronic evidence.

Psal se rok 1996 a John Perry Barlow vydal „Deklaraci nezávislosti kyberprostoru“.[180] Věřil, stejně jako řada dalších, že uživatelé kybernetického prostoru jsou schopni seberegulace a že jsou jako společenství schopni se sami vypořádat s těmi, kteří jejich společenství narušují. John P. Barlow zemřel a s ním i myšlenka o seberegulaci, neboť čas ukázal, že bez regulace se kybernetický prostor neobejde.

Stačí nahlédnout do statistik kriminality, aby bylo zřejmé, že trestná činnost spáchaná v on-line prostředí signifikantně roste. Uvedené platí o to více, že statistika zahrnuje pouze registrovanou kriminalitu. Neznámou zůstává míra latence kriminality na internetu. Z vlastní zkušenosti lze potvrdit, že denně je doručeno několik e-mailů, v nichž někdo nabízí peníze z dědictví, nebo upozorňuje, že vypršely přihlašovací údaje do internetového bankovnictví. Otázka zní, kolik osob, kterým jsou doručovány obdobné podvodné e-maily, je ohlašuje. Myslím, že málokdo. Kladu si tedy druhou otázku, proč neoznamujeme trestné činy, o jejichž spáchání se někdo pokouší. Důvodů bude vícero, jedním z nich je pocit zbytečnosti, že stejně k odhalení pachatele nedojde.

Mediálně známé případy v České republice jsou příkladem toho, že ani při závažném útoku k zjištění pachatele nedojde. Typickými útoky jsou stále útoky označované jako *Distributed denial of service (DDoS)*, což ukazují např. opakované útoky na stránky české vlády,[181] nebo ransomware, u kterého lze zmínit případy dvou známých nemocnic a Ředitelství silnic a dálnic.[182] Pachatelé těchto útoků nebyli

180 Srov. A Declaration of the Independence of Cyberspace. *Wikipedia.org.* Dostupné online na: https://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace [zobrazeno 25.10.2022].

181 Srov. např. Masivní hackerské útoky na české weby nekončí, napadený je i web vlády. *Seznamzpravy.cz*. Dostupné online na: https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-masivni-hackerske-utoky-na-ceske-weby-nekonci-napadeny-je-i-web-vlady-199082 [zobrazeno 17.10.2022].

182 Srov. např. útok na Nemocnici v Benešově. Viz Hacker způsobil benešovské nemocnici škodu 59 milionů, policie ho nedopadla. *Idnes.cz*. Dostupné online na: https://www.idnes.cz/praha/zpravy/kyberneticky-utok-policie-vysetrovani-benesovska-nemocnice.A200818_090949_praha-zpravy_pp. [zobrazeno 17.10.2022], nebo na Nemocnici v Brně Bohunicích. Viz Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty. *Idnes.cz*. Dostupné online na: https://www.idnes.cz/brno/zpravy/brno-nemocnice-fakultni-nemocnice-kyberneticky-utok.A200313_071531_brno-zpravy_bur. [zobrazeno 17.10.2022]. Dále srov. útok na Ředitelství silnic a dálnic. Viz Zálohy selhaly, data jsou nedostupná. ŘSD se po útoku hackerů vrátilo k papíru. Seznamzpravy.cz. Dostupné online na: https://www.seznamzpravy.cz/clanek/domaci-kauzy-rsd-po-utoku-hackeru-cast-lidi-nepracuje-vytahly-se-papirove-formulare-205888 [zobrazeno 18.10.2022].

odhaleni. Obdobné problémy vznikají také při odhalování pachatelů nenávistných projevů na internetu nebo pachatelů, kteří šíří dezinformace. Orgány činné v trestním řízení nejsou schopny najít důkazy proti konkrétním osobám. Důkazy o útoku, stopy trestného činu, zanechává samotný pachatel. Stopy podniknutého útoku lze získat též od poskytovatelů zprostředkovatelských služeb (dále také jen „PZS“). Evropská unie si je vědoma role PZS a postupně se je snaží přimět k aktivnějšímu jednání při eliminaci protiprávních projevů na internetu, jakož i k poskytování důkazů o protiprávní činnosti pachatelů.

1 Odpovědnost poskytovatelů zprostředkovatelských služeb za protiprávní obsah

Historicky lze připomenout Směrnici Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („Směrnice o elektronickém obchodu“), která upravuje, v jakých případech nejsou poskytovatelé zprostředkovatelských služeb odpovědní za jimi přenášený, resp. zprostředkovaný, obsah.[183] Podrobnosti upravují čl. 12 až 15 Směrnice o elektronickém obchodu. Zprostředkovatelé jsou rozděleni podle náplně jejich činnosti na ty, kteří zabezpečují prostý přenos (čl. 12) – *mere conduit*, *access provider*, ukládaní do vyrovnávací paměti (čl. 13) – *caching*, a na ty, kteří umožňují ukládání informací (čl. 14) – *host provider*. Za jakých podmínek ztrácí výhodu vyloučené odpovědnosti, tedy ve smyslu doktríny vyplutí z bezpečného přístavu, jsou nastaveny odlišně.[184] Žádný z poskytovatelů zprostředkovatelských služeb však nemá povinnost obecného dohledu nad jimi přenášenými informacemi. K uvedeným článkům existuje i poměrně bohatá judikatura Evropského soudního dvora, resp. Soudního dvora EU.[185]

183 V České republice došlo k implementaci Směrnice o elektronickém obchodu zákonem č. 480/2004 Sb., o některých službách informační společnosti.

184 Srov. např. GŘIVNA, T., ŠMERDA, R. Odpovědnost poskytovatelů služeb informační společnosti na internetu – současnost a perspektiva. In: PORADA, V., RAIS, K. a kol. Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti. Pocta Vladimíru Smejkalovi, Brno: Akademické nakladatelství CERM, 2021, s. 104–114.

185 Srov. C-360/10, C-70/10, spojené věci C-236/08 až C-238/08, C-324/09.

Změnu přinesla Směrnice Evropského parlamentu a Rady EU 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES ze 17. dubna 2019, která podle čl. 17 ukládá povinnost, aby poskytovatelé služeb pro sdílení obsahu online[186] získali od nositelů práv svolení ke sdělení nebo zpřístupnění děl nebo jiných předmětů ochrany veřejnosti, například uzavřením licenční smlouvy.[187] Na tyto poskytovatele se nevztahuje omezení odpovědnosti podle čl. 14 odst. 1 směrnice 2000/31/ES. Jinými slovy, takový poskytovatel nepožívá výhody bezpečného přístavu. Pokud totiž není svolení poskytnuto, odpovídá poskytovatel služeb pro sdílení obsahu online za neoprávněná sdělení nebo zpřístupnění děl chráněných autorským právem a jiných předmětů ochrany veřejnosti. Směrnice 2019/790 při takto přísném nastavení odpovědnosti přeci jen umožňuje poskytovateli zprostit se za určitých podmínek odpovědnosti. Poskytovatelé služeb pro sdílení obsahu online musí také zavést účinné a rychlé mechanismy pro stížnosti a nápravu, které uživatelé jejich služeb budou moci využívat v případě sporů týkajících se znemožnění přístupu k jimi nahraným dílům nebo jiným předmětům ochrany nebo jejich odstranění.

Do tohoto právního rámce nejnověji zasáhne návrh nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES.[188] Nařízení v principu přebírá režim bezpečných přístavů, je však mnohem podrobnější v mechanismech, které mají zabezpečit dodržování povinností poskytovatelů zprostředkovatelských služeb, především v případech hostingových služeb. Předchozí úprava byla příliš obecná, především ve vztahu k povinnosti *host providera* označované jako „*notice and take down*“, tedy neprodleně učinit veškeré kroky,

186 K definici poskytovatele služeb podle čl. 17 srov. Sliwka, R. Poskytovatelé služeb sdílení obsahu online dle Směrnice (EU) 790/2019. Revue pro právo a technologie. Ročník 11, 2020, č. 21, s. 91 až 128.

187 K implementaci Směrnice došlo přijetím novely autorského zákona (zákona č. 121/2000 Sb.), provedené zákonem č. 429/2022 Sb. K tomu srov. § 46 až § 52.

188 V době přednesení příspěvku probíhalo jednání Evropského parlamentu. Podrobnosti dostupné online zde: https://eur-lex.europa.eu/legal-content/CS/HIS/?uri=CELEX:52020PC0825 [zobrazeno 20.10.2022]. V době odevzdání příspěvku návrh nařízení prošel řádným legislativním procesem a nařízení bylo přijato dne 19. října 2022 jako nařízení Evropského parlamentu a Rady (EU) 2022/2065, o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách). Nařízení se jako celek použije ode dne 17. února 2024 s výjimkou některých článků, které se použijí od 16. listopadu 2022.

které lze po něm požadovat, k odstranění nebo znepřístupnění informací, když se prokazatelně dozvěděl o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele. Nařízení zavádí určitý mechanismus oznamování nezákonného obsahu a úpravu přijímání adekvátních opatření ze strany poskytovatelů hostingových služeb, včetně online platforem. Poskytovatelé hostingových služeb by měli, dle návrhu nařízení, zavést mechanismy, které umožní nejen fyzickým osobám, ale i jiným subjektům oznamovat výskyt nezákonného obsahu, a to podle jejich subjektivního vyhodnocení. Tento způsob oznámení musí být snadno dostupný a uživatelsky přístupný a musí být i možnost takové oznámení učinit elektronicky. Ze strany oznamovatelů se však bude muset jednat o oznámení dostatečně přesná, náležitě odůvodněná, tak aby mohl poskytovatel jednající s náležitou péčí takovou nezákonnost posoudit a určit. V případě, že oznámení obsahuje adresu oznamovatele, zašle poskytovatel hostingových služeb takové osobě obratem potvrzení o přijetí oznámení. Následně vyrozumí oznamovatele o svém rozhodnutí, jak s tímto podáním naložil (např. odstranění informace, znemožnění přístupu k ní apod.), a jak bude dále nakládat s označenými informacemi, včetně poučení o možných opravných prostředcích proti tomuto rozhodnutí. Poskytovatelé hostingových služeb jsou povinni vyřizovat všechna oznámení, která obdrží, a která splňují výše uvedené parametry, včas, objektivně a s náležitou péčí. Pokud se dozví informace vedoucí k podezření, že došlo, dochází nebo pravděpodobně dojde k závažnému trestnému činu ohrožujícímu život či bezpečnost osob, neprodleně musí informovat donucovací či justiční orgány členského státu, popř. Europol. Článek 15 návrhu nařízení pak upravuje postup poskytovatele hostingových služeb v případě, že se rozhodne určité informace odstranit nebo k nim znemožnit přístup (bez ohledu na to, zda tak činí na základě oznámení nebo identifikace vlastní péčí), a zejména pak podmínky pro toto rozhodnutí z hlediska jeho obsahu a odůvodnění, včetně způsobu informování příjemce poskytované služby. Evropská komise by pak měla spravovat veřejně přístupnou databázi rozhodnutí a odůvodnění poskytovatelů hostingových služeb (nebude obsahovat osobní údaje). Příjemci poskytovaných služeb se mohou proti takovému rozhodnutí bránit formou stížnosti, která by měla být podrobena v první řadě internímu přezkumu u poskytovatele, a následně je možné celý spor řešit mimosoudně prostřednictvím certifikované autority pro řešení těchto sporů. Certifikaci pro status

nestranného „arbitra“ těchto sporů mezi poskytovateli a příjemci digitálních služeb by měl v členském státě vydávat příslušný národní koordinátor digitálních služeb. Veřejný seznam těchto certifikovaných subjektů povede Evropská komise. Národní koordinátor digitálních služeb bude mít oprávnění rovněž přiznat kterémukoliv subjektu, který si o to požádá, status důvěryhodného oznamovatele. Podmínkou pro přidělení takového statusu bude zvláštní odbornost a způsobilost, reprezentace kolektivního zájmu a nezávislost na kterékoliv online platformě. Oznámení ze strany takového důvěryhodného oznamovatele budou muset poskytovatelé vyřizovat neprodleně a přednostně. Status bude možné i odejmout, a to v případě neplnění podmínek.

2 Povinnost poskytovatelů zprostředkovatelských služeb poskytnout součinnost donucovacím orgánům ve vztahu k protiprávnímu obsahu a k elektronickým důkazům

Návrh nařízení o digitálních službách upravuje specificky dva příkazy. V čl. 9 jsou to příkazy k přijetí opatření proti nezákonnému obsahu, který mohou vydat vnitrostátní justiční nebo správní orgány. Přikázaným opatřením může být např. povinnost odstranit protiprávní obsah. Druhým typem příkazu je příkaz k poskytnutí informace podle čl. 10 návrhu. Typickou požadovanou informací může být informace o objednateli služby.

Poskytovatelé zprostředkovatelských služeb určí jednotné kontaktní místo, aby jim umožnilo přímo komunikovat elektronickými prostředky s orgány členských států, Komisí a Evropským sborem pro digitální služby, a to za účelem uplatňování tohoto nařízení.

Poskytovatelé zprostředkovatelských služeb, kteří nemají v Unii provozovnu, ale nabízejí v Unii služby, ustanoví písemně určitou právnickou nebo fyzickou osobu, aby jednala jako jejich právní zástupce v jednom z členských států, v nichž poskytovatel své služby nabízí. Ustanoveného právního zástupce lze činit odpovědným za neplnění povinností vyplývajících z tohoto nařízení, aniž je tím dotčena odpovědnost poskytovatele zprostředkovatelských služeb, stejně jako právní řízení, která by proti němu mohla být zahájena.

Tímto nařízením by však nemělo být dotčeno právo Unie v oblasti justiční spolupráce v občanských nebo trestních věcech, včetně nařízení (EU) č. 1215/2012 a připravovaného nařízení o evropských

předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, ani vnitrostátní trestní nebo občanské procesní právo. Pokud tedy tyto právní předpisy v rámci trestního nebo občanského řízení stanoví podmínky, jež jsou dodatečné k podmínkám stanoveným v tomto nařízení nebo jsou s nimi neslučitelné, pokud jde o příkazy k přijetí opatření proti nezákonnému obsahu nebo k poskytnutí informací, podmínky stanovené v tomto nařízení by se nemusely použít nebo by mohly být upraveny.

V souvislosti se zmíněným evropským předávacím a uchovávacím příkazem je vhodné zmínit dva návrhy Evropské komise, které již byly předloženy Evropskému parlamentu. Jeden z nich má formu nařízení, tzn. přímo aplikovatelného předpisu.[189] Nařízení se vztahuje na přeshraniční situace, kdy je PZS usazen nebo zastoupen v jiném členském státě, než je stát, který příkaz vydá. Příkazem se obrací justiční orgán jednoho členského státu přímo na PZS v jiném členském státě. Možnost vydání příkazu je vázána na vedení konkrétního trestního řízení, příkaz nelze použít preventivně. Navrhované nařízení zavádí dva typy příkazů: předávací a uchovávací. Již z názvu těchto příkazů vyplývá, k čemu slouží. Účelem uchovávacího příkazu je uchování údajů, tedy prevence před ztrátou zájmových údajů. Na jeho základě nedochází k předání údajů. Není ho možné použít pro přístup k údajům v budoucnu vzniklým, tedy na odposlech telekomunikačního provozu v reálném čase. Předávací příkaz je určen k získání údajů o účastníkovi, přístupu, obsahu či transakcích. Často v případech, kdy předtím již bude vydán uchovávací příkaz.

Druhým návrhem Evropské komise je směrnice, která bude muset být do právních řádů členských států teprve implementována, a kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení.[190] Cílem směrnice je mimo jiné řešit situace, kdy PZS není v EU usazen, ale poskytuje na území některého z členských států služby. Taková situace je krajně nevýhodná pro donucovací orgán, neboť nemá k dispozici právní nástroj, jak přimět PZS ke spolupráci při vyhledávání a zajišťování důkazů. Členské státy mají podle návrhu směrnice povinnost zajistit, aby PZS, který není usazen v Unii a který nabízí služby na jejich území, jmenoval v EU nejméně jednoho právního

189 COM/2018/225 final, Celexové číslo: 52018PC0225, v době odevzdání příspěvku čekal na zařazení do prvního čtení v Evropském parlamentu.

190 COM/2018/226 final, Celexové číslo: 52018PC0226, v době odevzdání příspěvku čekal na zařazení do prvního čtení v Evropském parlamentu.

zástupce pro přijímání, dodržování a vymáhání rozhodnutí a příkazů vydaných příslušnými orgány členských států za účelem shromažďování důkazů v trestním řízení. Členské státy jsou také povinny zajistit, aby jmenovaný právní zástupce mohl nést odpovědnost za nesplnění povinnosti.

3 Úvahy nad navrženými právními nástroji

Z předchozí části by mělo být zřejmé, jakým směrem se Unie vydává, aby jednak zamezila šíření protiprávního obsahu na internetu, a jednak aby zvýšila šance na zajištění elektronických důkazů, které mohou vést k odhalení pachatelů protiprávního jednání. Předložené návrhy jsou z pohledu sledovaného cíle logické, ale přeci jen jsou s jejich prosazením spojena určitá nebezpečí. Pokusíme se nyní některá z nich nastínit.

Především je to otázka kontrolních mechanismů, což platí jak pro odstraňování údajně protiprávního obsahu na internetu, tak ve vztahu k uchovávacím a zajišťovacím příkazům. Zvážit je třeba i míru, v jaké lze zatížit PZS, kteří budou povinni příkazy provést patrně bezplatně. Na místě tak jsou obavy, že u menších PZS může náročnost vést k omezení funkčnosti či navyšování nákladů, které nebudou moct přenést na konečného uživatele bez toho, aniž by ztratili konkurenceschopnost. Do třetice lze zmínit problematiku nucení k doznání. Pokud totiž PZS sám porušil své povinnosti a založil vlastní odpovědnost za protiprávní jednání, pak má zřejmě právo odepřít i součinnost donucovacím orgánům s odkazem na zákaz nucení k doznání. Důkazem toho, že tyto (a další) otazníky uvedené návrhy vyvolávají, je i doba jejich projednávání. Ačkoliv návrh nařízení i směrnice jsou z roku 2018, stále čekají na první čtení v Evropském parlamentu, ačkoliv se jedná o problematiku vysoce aktuální.

Naléhavost přijetí řešení je zřejmá nejen z aktivit na úrovni Unie, ale také v rámci Rady Evropy. V květnu 2022 byl podepsán druhý dodatkový protokol k Úmluvě o počítačové kriminalitě. K září 2022 podepsalo dodatkový protokol 22 států, z nichž některé nejsou ani členskými státy Rady Evropy. Nebylo však dosaženo potřebného počtu ratifikací (tj. 5), aby druhý dodatkový protokol vstoupil v platnost. Zbývá též dodat, že Česká republika mezi signatáři není.[191]

191 Chart of signatures and ratifications of Treaty 224. Dostupné online na: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=224 [zobrazeno 18.10.2022].

Lze shrnout, že cesta odstraňování protiprávního obsahu a získávání důkazů skrze PZS je v principu správná, ale je zapotřebí pečlivě rozvážit konkrétní provedení, aby nedošlo k újmě na právech, a to jak PZS, tak uživatelů samotných.

Prof. JUDr. Bc. Tomáš Gřivna, Ph.D.
Univerzita Karlova
vedoucí katedry trestního práva
grivna@prf.cuni.cz

Zdroje a literatura

A Declaration of the Independence of Cyberspace. *Wikipedia.org.* Dostupné online na: https://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace.

GŘIVNA, Tomáš, ŠMERDA, Radek. Odpovědnost poskytovatelů služeb informační společnosti na Internetu – současnost a perspektiva. In: PORADA, Viktor, RAIS, Karel a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a* bezpečnosti. Pocta Vladimíru Smejkalovi. Brno: Akademické nakladatelství CERM, 2021, 468 s. ISBN: 978-80-7623-065-1.

SLIWKA, Rostislav. Poskytovatelé služeb sdílení obsahu online dle Směrnice (EU) 790/2019. *Revue pro právo a technologie.* Ročník 11, 2020, č. 21, s. 91 až 128.