Vývoj právnej úpravy kybernetických zločinov v Európskej únii

Bicko, M.*

BICKO, M.: Vývoj právnej úpravy kybernetických zločinov v Európskej únii. Právny obzor, *108*, 2025, č. 4, s. 343 – 356. **https://doi.org/10.31577/pravnyobzor.2025.4.02**

Development of cybercrime legislation in the European Union. The article is divided into three chapters. The first two chapters analyze the development of cybersecurity in the sources of primary and secondary EU law. The third chapter also briefly introduces selected case law of the Court of Justice of the EU (CJEU) in the field of cybersecurity. The aim of the article is to analyze the development of cybersecurity legislation in the EU. I operate with the hypothesis that the development of cybersecurity was primarily influenced by the Lisbon Treaty of 2009, or rather the technological progress achieved in the last decade, while specific rules of cooperation or identification of cybercrimes are defined in secondary law documents. To achieve the aim of the article and verify the hypothesis, the methods of description, analysis, synthesis and deduction are used.

Key words: *cybercrime legislation, computer crime, EUROPOL, AML, NIS*

1. Východiskové postavenie kybernetickej kriminality v práve EÚ

Právo EÚ je možné rozdeliť na primárne a sekundárne právo. Primárne právo EÚ je tvorené zakladajúcimi zmluvami, ich prílohami a tiež zmluvami o pristúpení členských štátov, ktorými sa čiastočne obmedzila ich štátna suverenita v prospech práva EÚ. Prvotným dokumentom primárneho práva boli Rímske zmluvy, ktoré sa vyvinuli do Zmluvy o fungovaní Európskej únie a Zmluvy o Európskej únii. Primárne právo EÚ zahŕňa aj všeobecné právne zásady, základné ľudské práva a slobody (Tomášek a kol., 2021, s. 103). Hlavným zmyslom primárneho práva EÚ je rozdelenie kompetencií a povinností medzi EÚ (nadnárodnú úroveň) a členské štáty (národnú úroveň). Primárne právo zároveň zabezpečuje právny kontext, na ktorého základe inštitúcie EÚ formulujú a realizujú svoje politiky (Tichý a kol., 2014, s. 800).

Sekundárne právo EÚ je vymedzené v článku 288 Zmluvy o fungovaní EÚ. Konkrétne vymedzuje päť právnych aktov, ktoré je umožnené prijímať inštitúciám EÚ. Ide o nariadenia, smernice, rozhodnutia, odporúčania (legislatívne právne akty) a stanoviská (nelegislatívne a nezáväzné právne akty). Sekundárne právo EÚ zahŕňa aj atypické akty, ktoré môžu byť právne záväzné (interinštitucionálne dohody). Pri iných atypických aktoch, napríklad uzneseniach a záveroch, sa nepredpokladajú právne účinky (Tomášek a kol., 2021, s. 107 – 112). Sekundárne právo EÚ má nižšiu právnu silu a musí byť v súlade s primárnym právom.

Právny základ umožňujúci úpravu kybernetickej bezpečnosti zo strany inštitúcií EÚ je zakotvený v čl. 68 Zmluvy o fungovaní EÚ, v ktorého zmysle „*Európska rada vymedzuje strategické usmernenia pre legislatívne a operatívne plánovanie v rámci*

* JUDr. Martin Bicko, advokát, doktorand, Paneurópska vysoká škola v Bratislave, Fakulta práva, Katedra trestného práva.

priestoru slobody, bezpečnosti a spravodlivosti.“ Zásadné sú však aj ďalšie ustanovenia nachádzajúce sa v IV. kapitole (justičná spolupráca v trestných veciach) a tiež V. kapitole (policajná spolupráca). Článok 83 Zmluvy o fungovaní EÚ umožňuje Európskemu parlamentu a Rade stanovovať minimálne pravidlá týkajúce sa trestných činov a tiež sankcií za spáchanie trestných činov v oblasti vážnej trestnej činnosti, ktorá má cezhraničný rozmer. Jednou z oblastí vážnej trestnej činnosti je aj počítačová kriminalita, ktorá je v primárnom práve EÚ identická s úrovňou terorizmu, obchodovania s ľuďmi, nedovoleného obchodovania s drogami a so zbraňami, prania špinavých peňazí, korupciou či organizovanou trestnou činnosťou. Počítačová kriminalita tak z pohľadu justičnej spolupráce v trestných veciach patrí medzi najviac závažné trestné činy. EÚ s cieľom predchádzať, odhaľovať a vyšetrovať trestné činy rozvíja vzájomnú policajnú spoluprácu, do ktorej sa zapájajú príslušné orgány členských štátov vrátane polície a iných orgánov, ktoré presadzujú výkon práva. Na podporu a posilňovanie činnosti policajných a iných orgánov členských štátov EÚ bol zriadený EUROPOL (čl. 88 Zmluvy o fungovaní EÚ).

Činnosť EÚ sa v oblasti eliminácie páchania kybernetickej kriminality prejavuje na dvoch úrovniach, a to na nadnárodnej a národnej úrovni. Na nadnárodnej úrovni EÚ predstavuje aktéra vytvárajúceho strategické opatrenia, resp. kľúčové kroky a definuje ciele, ktoré je potrebné v tejto oblasti dosiahnuť. Na úrovni členských štátov zjednodušuje cezhraničnú výmenu informácií, realizáciu vyšetrovania, operatívnych akcií a tiež spoluprácu, čoho príkladom je EUROPOL. Hlavným zmyslom EÚ je na oboch úrovniach predchádzanie páchaniu trestnej činnosti, odhaľovanie a objasňovanie trestnej činnosti vzťahujúcej sa (nielen) ku kybernetickej kriminalite.

2. Genéza kybernetickej bezpečnosti v prameňoch primárneho a sekundárneho práva EÚ

Vývoj kybernetickej bezpečnosti v prameňoch práva EÚ je možné rozpracovať do dvoch období, a to do obdobia pred a po prijatí Lisabonskej zmluvy (2009). Predovšetkým po roku 2009 bolo prijatých viacero významných legislatívnych aktov vrátane vytvorenia dôležitých inštitúcií zameraných na boj proti páchaniu kybernetických zločinov. Súčasný vývoj legislatívy regulujúcej kybernetické prostredie je však predovšetkým v posledných rokoch úzko naviazaný na dynamický vývoj technológií, ktoré na jednej strane zjednodušujú život v spoločnosti a na strane druhej však ponúkajú stále nové možnosti rozvoja kybernetického zločinu.

2.1 Kybernetická bezpečnosť na úrovni EÚ do prijatia Lisabonskej zmluvy

Problematika kybernetickej bezpečnosti má v primárnom práve EÚ základ v trestnej oblasti. Zároveň ide o problematiku, ktorá sa postupne vyvíjala, a to tak v primárnych, ako aj v sekundárnych prameňoch práva. Vývoj kybernetickej bezpečnosti v prameňoch primárneho práva je spracovaný v tabuľke 1.

Tab. 1 Kybernetická kriminalita a pramene primárneho práva

Prameň práva	Význam pre kybernetickú bezpečnosť
Maastrichtská zmluva	Oblasť justície a vnútorných vecí primárne v kompetencii členských štátov EÚ. Neregulovaná oblasť práva.
Amsterdamská zmluva	Poukázanie na význam zbližovania legislatívy v oblasti vnútorných vecí, spolupráca EÚ a členských štátov pri vyšetrovaní závažných kriminálnych prípadov (EUROPOL).
Zmluva z Nice	Podpora činnosti EUROJUST, posilnenie užšej spolupráce medzi členskými štátmi EÚ.

Zdroj: vlastné spracovanie

Vývoj kybernetickej bezpečnosti (s ohľadom na kybernetickú kriminalitu) vo vybraných prameňoch sekundárneho práva v skúmanom období je spracovaný v tabuľke 2.

Tab. 2 Kybernetická kriminalita v prameňoch sekundárneho práva EÚ do prijatia Lisabonskej zmluvy

Prameň práva	Význam pre kybernetickú bezpečnosť
98/428/SVV	vytvorenie Európskej súdnej siete so zámerom spoločného vyšetrovania závažných kriminálnych prípadov (napríklad šírenie detskej pornografie)
98/699/SVV	riešenie problematiky prania špinavých peňazí
2001/413/SVV a 2001/500/SVV	boj proti praniu špinavých peňazí, podvodom a falšovaniu bezhotovostných platobných prostriedkov
2004/68/SVV	boj proti pohlavnému zneužívaniu detí a šíreniu detskej pornografie
2005/222/SVV	riešenie problematiky útokov na informačné systémy

Zdroj: vlastné spracovanie

V Maastrichtskej zmluve, ktorá položila základ vytvorenia EÚ (v roku 1992), bola táto problematika riešená v rámci tzv. III. piliera[1] zahŕňajúceho vzájomnú spoluprácu členských štátov EÚ v oblasti justície a vnútorných vecí. Cieľom tejto spolupráce boli zaistenie bezpečnosti a ochrany osôb, policajná a súdna spolupráca a tiež prevencia boja proti závažným formám medzinárodného zločinu (Tomášek a kol., 2021, s. 47 – 49). Za prevenciu a tiež boj proti medzinárodnému zločinu však boli zodpovedné aj členské štáty, v ktorých kompetencii zostávalo zaistenie vlastnej vnútornej bezpečnosti (Fiala, Krutílek, Pitrová, 2018, s. 131 – 132). Kybernetickej kriminalite v tomto období zatiaľ nebol v primárnom ani sekundárnom práve EÚ venovaný výraznejší priestor z dôvodu, že išlo o pomerne novú a zatiaľ neregulovanú oblasť práva.

Amsterdamská zmluva z roku 1997 v oblasti vnútornej bezpečnosti, resp. bezpečnostnej spolupráce členských štátov stanovovala nevyhnutnosť rozvoja spoločného po-

[1] Prvý pilier zahŕňal spoločné politiky Európskych spoločenstiev, napríklad poľnohospodárstvo, obchod, občianstvo, vedu a výskum, rybolov, sociálnu politiku a pod. Druhý pilier zahŕňal oblasť spoločnej zahraničnej a bezpečnostnej politiky. Do tretieho piliera boli zahrnuté oblasť justície a vnútornej bezpečnosti členských štátov. Medzi oblasti, ktoré sa riešili v rámci tzv. tretieho piliera, patrili napríklad organizovaný zločin, korupcia, obchod so zbraňami, obchodovanie s ľuďmi a pod. (Fiala, Krutílek, Pitrová, 2018, s. 131). Kybernetická kriminalita bola súčasťou III. piliera.

stupu členských štátov v oblasti policajnej a súdnej spolupráce. Významné pre oblasť riešenia kybernetických zločinov bolo najmä zbližovanie predpisov v oblasti trestného práva a tiež vznik Európskeho policajného úradu (EUROPOL) s cieľom výmeny informácií a koordinácie vyšetrovania zločinov presahujúcich národné hranice členských štátov (Tomášek a kol., 2021, s. 49 – 50). Prínosom pre oblasť vzájomnej spolupráce v oblasti justície a boja proti organizovanému zločinu bolo aj prijatie jednotnej akcie č. 98/428/SVV o vytvorení Európskej súdnej siete, ktoré bolo v roku 2008 nahradené Rozhodnutím Rady č. 2008/976/SVV. Aj napriek posilneniu vzájomnej spolupráce medzi členskými štátmi na nadnárodnej úrovni však išlo predovšetkým o rámcové rozhodnutia EÚ, pričom členské štáty si mohli zvoliť formu a tiež prostriedok na realizáciu konkrétnych rozhodnutí.

V oblasti kybernetickej kriminality, resp. v oblasti spravodlivosti a vnútorných vecí boli v tomto období prijaté viaceré významné legislatívne návrhy, ktoré sa vzťahovali aj na oblasť kybernetickej bezpečnosti a páchania kybernetickej kriminality. Jedným z prvých dokumentov sekundárneho práva bola Jednotná akcia 98/699/SVV o praní špinavých peňazí, identifikácii, vyhľadávaní, zmrazení, zhabaní a konfiškácii prostriedkov a ziskov z trestnej činnosti, ktorej väčšina ustanovení bola nahradená Rámcovým rozhodnutím Rady č. 2001/500/SVV z 26. júna 2001 o praní špinavých peňazí, identifikácii, vyhľadávaní, zmrazení a konfiškácii prostriedkov a príjmov z trestnej činnosti. V tomto rámcovom rozhodnutí Európska rada vyslovila záver, že „*pranie špinavých peňazí je jadrom organizovaného zločinu a treba ho vykoreniť všade, kde sa vyskytne*“. Zároveň sa vyslovila za prijatie konkrétnych krokov s cieľom vyhľadať, zmraziť a zaistiť príjmy z trestnej činnosti. Rámcové rozhodnutie bolo nahradené smernicou Európskeho parlamentu a Rady 2014/42/EÚ z 3. apríla 2014 o zaistení a konfiškácii prostriedkov a príjmov z trestnej činnosti v Európskej únii.

V roku 2001 bola prijatá Zmluva z Nice, ktorá však ako prameň primárneho práva nepriniesla výraznejšie zmeny v oblasti postihovania kybernetickej kriminality. Významné však bolo prijatie viacerých rámcových rozhodnutí Rady, predovšetkým č. 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov, č. 2004/68/SVV o boji proti pohlavnému zneužívaniu detí a detskej pornografii a č. 2005/222/SVV o útokoch na informačné systémy.

Mimoriadny význam v otázke riešenia kybernetickej kriminality malo prijatie rámcového rozhodnutia Rady z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov (2001/413/SVV), v ktorom Rada zdôraznila nárast vybraných foriem podvodov páchaných v medzinárodnom meradle, pričom eliminácia týchto podvodov si vyžadovala realizáciu komplexných riešení na nadnárodnej úrovni. V čl. 3 boli upravené trestné činy týkajúce sa počítačov a v čl. 4 trestné činy týkajúce sa zvláštne upravených zariadení. Ako trestný čin bolo v kontexte kybernetickej kriminality definované „*vykonanie alebo navádzanie na prevod peňazí alebo peňažnej hodnoty a tým spôsobenie neoprávnenej straty na majetku inej osoby s úmyslom nadobudnúť neoprávnenú výhodu pre osobu páchajúcu trestný čin alebo tretiu stranu prostredníctvom neoprávneného vkladania, pozmeňovania, vymazávania alebo odstraňovania úda-*

jov, najmä identifikačných, alebo neoprávneného zasahovania do fungovania počítačového programu alebo systému". Konanie bolo považované za trestný čin v prípade, že bolo spáchané úmyselne. Za trestný čin bolo v súlade s čl. 4 rámcového rozhodnutia aj „*podvodné vyrábanie, prijatie, získanie, predaj alebo poskytovanie inej osobe alebo vlastníctvo nástrojov, článkov, počítačových programov a akýchkoľvek ďalších prostriedkov prispôsobených na spáchanie trestného činu napodobovania alebo falšovania platobného nástroja s cieľom použiť ho na účely podvodu.*" Trestným činom bolo podvodné vyrábanie, prijatie, získanie, predaj alebo poskytovanie inej osobe alebo vlastníctvo počítačových programov na účely spáchania trestných činov uvedených v čl. 3 rámcového rozhodnutia.

Rámcové rozhodnutie Rady 2004/68/SVV z 22. decembra 2003 o boji proti pohlavnému zneužívaniu detí a detskej pornografii revidovalo predchádzajúce právne akty týkajúce sa problematiky obchodovania s ľuďmi a pohlavného zneužívania detí, napríklad jednotnú akciu Rady č. 97/154/SVV či rozhodnutie Rady č. 2000/375/SVV o boji proti detskej pornografii na internete. Rámcové rozhodnutie 2004/68/SVV bolo revidované v roku 2011.

Od 1. júla 2004 nadobudol v členských štátoch EÚ[2] platnosť aj tzv. Budapeštiansky dohovor o počítačovej kriminalite, ktorý bol členskými štátmi Rady Európy odsúhlasený v novembri 2001 v Budapešti. Dohovor upravuje konanie, ktoré je považované za kriminálne (t. j. nezákonný prístup k dátam, zasahovanie do údajov/systémov, počítačové podvody, zneužívanie detí/detská pornografia a pod.), procesné právomoci týkajúce sa počítačovej kriminality, zaistenie elektronických dôkazov spáchaného trestného činu a tiež medzinárodnú spoluprácu zmluvných strán, ktoré sú členmi Výboru pre Dohovor o počítačovej kriminalite. Hlavným zmyslom Budapeštianskeho dohovoru o počítačovej kriminalite bolo pomôcť zmluvným stranám protokolu v boji proti trestným činom, ktoré je možné spáchať výhradne s využitím vybraných technológií. Dodatkový protokol z marca 2006 rozšíril rozsah pôsobnosti aj na rasistickú a xenofóbnu propagandu, ktorú je potenciálne možné šíriť v kybernetickom priestore. Druhý dodatok, ktorý však nenadobudol platnosť, bol zameraný na posilnenie medzinárodnej spolupráce a zároveň riešil problematiku elektronických dôkazov spojených s páchaním počítačovej kriminality a tiež iných trestných činov, pričom tieto dôkazy sú v držbe poskytovateľov služieb sídliacich v zahraničných jurisdikciách. Dodatkový protokol č. 2 by tak v prípade nadobudnutia platnosti poskytol zmluvným stranám protokolu novú právnu platformu, na ktorej základe majú možnosť požiadať registrátora v inej jurisdikcii o informácie, ktoré sa týkajú registrácie názvu domény, získanie informácií o predplatiteľoch, informácie o účastníkoch a o prevádzkových dátach. Druhý dodatok k Dohovoru o počítačovej kriminalite by zároveň umožnil urýchlenú spoluprácu v núdzových situáciách, a to vrátane možnosti využívania spoločných vyšetrovaní a vytvárania spoločných vyšetrovacích tímov (European Union, 2023).

[2] V tomto prípade ide výhradne o členské štáty EÚ, a nie o EÚ na inštitucionálnej úrovni. Dôvodom je skutočnosť, že EÚ nie je členom Rady Európy. Členmi Rady Európy sú jednotlivé štáty Európy (Fiala, Krutílek, Pitrová, 2018, s. 41).

S cieľom zlepšiť vzájomnú spoluprácu medzi súdnymi, policajnými a inými špecializovanými orgánmi členských štátov EÚ činných v trestnom konaní bolo prijaté rámcové rozhodnutie Rady 2005/222/SVV o útokoch na informačné systémy. Rada v rozhodnutí zdôraznila, že medzi členskými štátmi existovali významné rozdiely v právnych predpisoch, ktoré bránili efektívnemu boju proti organizovanému zločinu a terorizmu páchanému pomocou informačných systémov s nadnárodným a bezhraničným charakterom. Za trestný čin sa podľa rámcového rozhodnutia považoval protiprávny prístup k informačnému systému, protiprávny zásah do systému a protiprávny zásah do údajov informačného systému. Rámcové rozhodnutie bolo revidované v roku 2013 (smernicou č. 2013/40/EÚ), t. j. v období platnosti Lisabonskej zmluvy.

2.2 Kybernetická kriminalita v EÚ po prijatí Lisabonskej zmluvy

Lisabonská zmluva bola ako prameň primárneho práva EÚ prijatá členskými štátmi v roku 2009. Na rozvoj kybernetickej bezpečnosti mala zásadný vplyv. Dôvodom bolo zrušenie tzv. trojpilierovej štruktúry zavedenej Maastrichtskou zmluvou a posilnenie vzájomnej justičnej spolupráce v trestných veciach. Príkladom je stanovenie pravidiel týkajúcich sa prípustnosti dôkazov medzi členskými štátmi a pod. Užšia spolupráca v oblasti eliminácie páchania kybernetických zločinov mala zároveň za následok revidovanie viacerých smerníc a tiež vytvorenie inštitucionálneho rámca zameraného na oblasť kybernetickej bezpečnosti (tabuľka 3).

Tab. 3 Prehľad prameňov sekundárneho práva prijatých po roku 2009 a revidované/zrušené dokumenty

Prameň práva	Zmena
Smernica Európskeho parlamentu a Rady 2011/92/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii.	97/154/JHA 2000/375/SVV 2004/68/SVV
Smernica Európskeho parlamentu a Rady 2013/40/EÚ o útokoch na informačné systémy.	2005/222/SVV
Smernica Európskeho parlamentu a Rady 2014/42/EÚ o zaistení a konfiškácii prostriedkov a príjmov z trestnej činnosti v Európskej únii.	98/699/SVV 2001/500/SVV
Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu.	2001/413/SVV
Rozhodnutie Rady (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.	k 30. 06. 2024 10x doplnenie
Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti.	2016/1148 910/2014

Zdroj: vlastné spracovanie

Prvým významným rozhodnutím, ktoré bolo revidované po prijatí Lisabonskej zmluvy, bolo rámcové rozhodnutie Rady 2004/68/SVV z 22. decembra 2003 o boji proti pohlavné-

mu zneužívaniu detí a detskej pornografii. Rozhodnutie nahradila smernica Európskeho parlamentu a Rady 2011/92/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii. Smernica zdôraznila požiadavku komplexného riešenia prevencie a postihov závažných trestných činov, medzi ktoré patria detská pornografia a pohlavné vykorisťovanie detí. Kontakt detí na sexuálne účely na internete definovala ako zvláštnu hrozbu, vo vzťahu ktorej by mali byť prijaté opatrenia zamerané na sťaženie obsahu tohto typu na webové stránky, ktoré sú verejne dostupné. Ak sú servery spravované mimo územia EÚ, je potrebné, aby prístup k nim bol zablokovaný. Smernica zároveň definovala štyri oblasti trestných činov, a to trestné činy pohlavného zneužívania, pohlavného vykorisťovania, detskej pornografie a trestný čin kontaktovania detí (t. j. s osobami mladšími ako 18 rokov) na sexuálne účely. Z pohľadu skúmanej témy, t. j. páchania kybernetickej kriminality sú významné predovšetkým trestné činy detskej pornografie a trestný čin kontaktovania detí na sexuálne účely, ktoré sú realizované prostredníctvom informačných a komunikačných technológií. Za trestné sa nepovažuje výhradne spáchanie trestného činu, ale aj pokus, navádzanie, pomoc či účasť na trestnom čine.

Zásadným v smernici č. 2011/92/EÚ je čl. 25, ktorý definuje opatrenia proti internetovým stránkam, ktoré obsahujú, prípadne šíria detskú pornografiu. V zmysle uvedeného článku bolo potrebné, aby členské štáty prijali opatrenia smerujúce k zaisteniu odstránenia webových lokalít obsahujúcich alebo šíriacich detskú pornografiu v prípade, že sa tieto lokality nachádzajú na ich území. Zároveň boli členské štáty povinné snažiť sa o zabezpečenie odstránenia webových stránok nachádzajúcich sa mimo ich jurisdikcie. Členské štáty mali zároveň v zmysle čl. 25 ods. 2 právo prijať opatrenia, v ktorých zmysle by dosiahli zablokovanie webových lokalít obsahujúcich alebo šíriacich detskú pornografiu používateľom na ich území. Opatrenia je však potrebné realizovať transparentne, pričom je dôležité, aby obmedzenia mali primeraný a nevyhnutný dosah, pričom používatelia musia byť s dôvodom obmedzenia oboznámení.

Smernica Európskeho parlamentu a Rady 2013/40/EÚ o útokoch na informačné systémy nahradila rámcové rozhodnutie rady č. 2005/222/SVV a ukladala členským štátom EÚ povinnosť prijať legislatívu, ktorá zaistí trestnosť v prípade neoprávneného úmyselného prístupu do celého informačného systému alebo jeho časti, neoprávneného úmyselného závažného narušenia alebo prerušenia fungovania informačného systému, ktoré bolo spôsobené nakladaním s počítačovými dátami, úmyselného neoprávneného nakladania s počítačovými údajmi nachádzajúcimi sa v informačnom systéme (vrátane zneprístupnenia týchto údajov) a tiež v prípade výroby alebo iného nakladania s nástrojmi, ktoré sú určené na spáchanie trestného činu.

V roku 2016 bola prijatá smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (tzv. smernica NIS). Z pohľadu kybernetickej bezpečnosti išlo o prvú legislatívu na úrovni EÚ, ktorej cieľom malo byť zlepšenie spolupráce členských štátov v oblasti kybernetickej bezpečnosti. Smernica ukladala povinnosti v oblasti bezpečnosti pre prevádzkovateľov tzv. základných služieb (energetika, doprava, bankovníctvo/financie, zdravotníctvo) a tiež pre poskytovateľov digitálnych služieb, t. j. pre inter-

netové vyhľadávače, online trhoviská a tiež pre cloudové služby. Smernica bola v roku 2022 revidovaná a rozšírená smernicou NIS2.[3]

K zásadnému rozvoju kybernetickej bezpečnosti na úrovni EÚ došlo od roku 2019, a to z dôvodu zvýšenej intenzity páchania podvodov, kybernetických útokov a tiež zvyšujúceho sa počtu kybernetických hrozieb. Podľa štatistických dát Rady EÚ dochádza mesačne v členských štátoch EÚ k odcudzeniu viac než 10 TB dát, pričom náklady spojené s kybernetickou kriminalitou dosiahli v roku 2020 približne 5,5 bilióna eur. K zvýšenému počtu útokov a kybernetickej kriminalite dochádza na území EÚ od roku 2022, keď sa začala vojenská agresia Ruskej federácie voči Ukrajine. Medzi najviac závažné kybernetické hrozby v EÚ patria ransomware útoky, DDoS útoky (t. j. hrozby distribuovaného odmietnutia služby), šírenie malware, hrozby sociálneho inžinierstva, útoky s cieľom získania neoprávneného prístupu k dátam, internetové hrozby (t. j. útoky, ktoré majú dosah na dostupnosť internetu, napríklad krádeže BGP), vytváranie a šírenie dezinformácií, útoky cielené na dodávateľské reťazce (Európska rada, 2024).

Smernica Európskeho parlamentu a Rady (EÚ) č. 2019/713 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu nahradila rámcové rozhodnutie Rady 2001/413/SVV. Dôvodom revízie rozhodnutia Rady bola potreba rozšírenia ustanovení týkajúcich sa vybraných trestných činov súvisiacich s počítačmi a tiež trestov, prevencie, pomoci obetiam a cezhraničnej spolupráce. Európsky parlament a Rada zdôraznili, že práve podvody s bezhotovostnými platobnými prostriedkami vrátane ich falšovania majú zásadný cezhraničný rozmer, ktorý je zvýraznený práve zvyšujúcim sa digitálnym prvkom. Nedochádza výhradne k rastu digitálneho hospodárstva a šíreniu inovácií, ale aj k páchaniu podvodov. Smernica 2019/713 definovala v II. hlave nasledujúce trestné činy (Smejkal, 2022, s. 636):

1. Podvodné použitie bezhotovostných platobných nástrojov. Trestného činu sa dopustí osoba v prípade, že úmyselne podvodne použije odcudzený, resp. inak nezákonne prisvojený bezhotovostný platobný nástroj, prípadne bezhotovostný platobný nástroj sfalšuje, pozmení alebo napodobní.
2. Trestné činy súvisiace s podvodným použitím hmotných bezhotovostných platobných nástrojov. Ide o trestné činy:
   a) krádeže alebo prisvojenia si bezhotovostného platobného nástroja iným nezákonným spôsobom;
   b) falšovania, pozmeňovania alebo napodobňovania hmotného bezhotovostného platobného nástroja;
   c) prechovávania hmotného platobného nástroja (ktorý bol odcudzený alebo inak nezákonne získaný, prípadne sfalšovaný alebo napodobený) s účelom jeho podvodného použitia;
   d) obstaranie hmotného bezhotovostného platobného nástroja pre seba alebo inú osobu s cieľom jeho uvedenia do obehu a následného podvodného použitia.

[3] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa menia nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS2).

3. Trestné činy súvisiace s podvodným použitím nehmotných bezhotovostných platobných nástrojov, medzi ktoré patria nezákonné získanie takéhoto nástroja, podvodné falšovanie, pozmeňovanie alebo napodobovanie takéhoto nástroja, jeho držanie s cieľom podvodného použitia a tiež obstaranie nehmotného bezhotovostného platobného nástroja pre seba alebo inú osobu s cieľom jeho podvodného použitia.
4. Trestné činy podvodu súvisiaceho s informačnými technológiami, t. j. neoprávnené zamedzenie fungovaniu informačného systému, zasiahnutie do jeho fungovania alebo neoprávnené vloženie, pozmenenie, vymazanie, potlačenie alebo prenos počítačových údajov.

Za trestný čin v zmysle smernice 2019/713 sa považuje aj podnecovanie, napomáhanie, navádzanie na trestný čin a tiež pokus o spáchanie trestného činu. V závislosti od typu spáchania trestného činu sú v čl. 9 definované aj minimálne trestné sadzby, ktoré sa pohybujú v rozpätí od jedného roka do až troch rokov odňatia slobody, resp. 5 rokov v prípade, že trestný čin bol spáchaný v rámci zločineckej organizácie. Sankcie sú určené aj pre právnické osoby, pričom okrem peňažnej sankcie môžu zahŕňať napríklad aj nariadenie súdneho dohľadu, zrušenie právnickej osoby (na základe súdneho rozhodnutia), rozhodnutie o dočasnom alebo trvalom zatvorení prevádzok použitých na spáchanie trestného činu a podobne.

Významným pre oblasť kybernetickej bezpečnosti v EÚ bolo rozhodnutie Rady (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty. Rozhodnutie nadväzovalo na skôr prijaté dokumenty, napríklad na vykonávacie usmernenie k súboru nástrojov kybernetickej diplomacie prijaté Politickým a bezpečnostným výborom v októbri 2017, či na závery Rady zo 16. apríla 2018, ktoré boli zamerané na škodlivé kybernetické činnosti. Viaceré závery týkajúce sa kybernetickej bezpečnosti prijala v priebehu roka 2018 aj Európska rada. Rada (SZBP) na základe uvedených dokumentov vydala rozhodnutie 2019/797 vzťahujúce sa na kybernetické útoky so závažným vplyvom a tiež kybernetické útoky predstavujúce externú hrozbu pre EÚ s potenciálne závažným dosahom.

Útoky predstavujúce externú hrozbu majú pôvod mimo EÚ (resp. sú vykonávané mimo členských štátov EÚ), využívajú infraštruktúru mimo EÚ a sú vykonávané aktérom (fyzickou alebo právnickou osobou, subjektom alebo orgánom) usadeným mimo EÚ. Kybernetický útok sa môže realizovať s podporou či vedením iného aktéra činného mimo EÚ. Kybernetický útok zároveň zahŕňa vybranú činnosť, ktorou môže byť prístup do informačných systémov, zásah do informačného systému, zásah do údajov alebo zachytávanie údajov, pričom tieto činnosti nie sú aktérovi, ktorý sa pokúša o ich realizáciu, povolené zo strany vlastníka systému alebo iného držiteľa práv k nim. Vždy tak ide o nepovolený prístup, zásah alebo zachytenie údajov. Rozhodnutie 2019/797 definovalo dva druhy kybernetických útokov, a to:

a) kybernetický útok alebo pokus o útok vedený voči EÚ;
b) kybernetický útok alebo pokus o útok, ktorý predstavuje hrozbu pre členské štáty.

Kybernetické útoky predstavujúce hrozbu pre členské štáty zahŕňajú útoky na informačné systémy kritickej infraštruktúry (vrátane predmetov vypustených do kozmického priesto-

ru a podmorské káble), útoky na služby nevyhnuté na zachovanie spoločenských alebo hospodárskych činností (útoky na energetickú infraštruktúru, dopravu, banky/finančný trh, zdravotnícke zariadenia a pod.), útoky na kritické funkcie štátu (napríklad v oblasti riadenia, na hospodárske inštitúcie štátu a pod.), útoky na informačné systémy uchovávajúce utajované skutočnosti a tiež útoky na informačné systémy tímov reagujúcich na núdzové situácie, pričom tieto tímy sú súčasťou verejnej správy. Kybernetické útoky predstavujúce hrozbu pre EÚ sú podľa rozhodnutia Rady 2019/797 útoky zamerané na inštitúcie, agentúry, orgány, osobitných zástupcov a tiež na delegácie nachádzajúce sa v tretích štátoch.

Závažnosť kybernetického útoku sa sleduje podľa viacerých faktorov. Ide napríklad o rozsah, dosah, mieru a tiež závažnosť spôsobeného narušenia činností alebo hospodárskych záujmov, počet aktérov dotknutých útokom, výšku straty spôsobenej útokom, získaný majetkový prospech, odcudzené údaje či povaha citlivých údajov, ku ktorým páchateľ získal v dôsledku kybernetického útoku prístup (Európska rada, 2024).

Rozhodnutie 2019/797 bolo k 30. júnu 2024 desaťkrát doplnené, napríklad rozhodnutím 2020/1127[4] či rozhodnutím č. 2022/754[5]. V rámci doplnení išlo najmä o rozširovanie zoznamu fyzických a právnických osôb, ktoré sa podieľali na kybernetických útokoch, boli spojené s osobami zodpovednými za kybernetické útoky alebo poskytli akúkoľvek pomoc na realizáciu alebo pokus o kybernetický útok. Osoby uvedené v zozname majú zabránený vstup na územie členského štátu a zároveň sú zmrazené všetky ich finančné prostriedky a hospodárske zdroje.

Akt o kybernetickej bezpečnosti, ktorý bol prijatý v júni 2019, zaviedol jednotný systém certifikácie zabezpečujúcej vysoké štandardy v oblasti IKT a zároveň posilnil aj mandát Agentúry EÚ pre kybernetickú bezpečnosť, ktorá vznikla ako nástupkyňa Agentúry EÚ pre bezpečnosť sietí a informácií (ENISA – Európska rada, 2023). Medzi súčasné kompetencie ENISA patrí napríklad vytváranie a udržiavanie certifikačného rámca kybernetickej bezpečnosti, realizácia technického základu konkrétnych certifikačných schém, informovanie verejnosti, pomoc členským štátom pri riešení bezpečnostných incidentov a tiež podpora a koordinácia EÚ v prípade vzniku závažných a rozsiahlych kybernetických útokov (European Commission, 2023).

Medzi významné akty zamerané na posilnenie kybernetickej bezpečnosti EÚ patrili aj Stratégia kybernetickej bezpečnosti EÚ (december 2020) definujúca viaceré návrhy na zavedenie nových investičných, regulačných a politických nástrojov. Rada prijala závery týkajúce sa kybernetickej bezpečnosti v marci 2021, pričom zdôraznila, že práve kybernetická bezpečnosť predstavuje determinujúci faktor pre budovanie zelenej a digitálnej Európy. Práve zachovanie kybernetickej bezpečnosti je zásadné pre upevnenie vedúceho postavenia EÚ v digitálnej oblasti (European Commission, 2023).

V decembri 2022 bola v EÚ prijatá smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bez-

[4] Rozhodnutie Rady (SZBP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.

[5] Rozhodnutie Rady (SZBP) 2022/754 zo 16. mája 2022, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.

pečnosti v Únii (smernica NIS2). Ide o revidovanú smernicu o kybernetickej bezpečnosti, resp. smernicu o bezpečnosti sietí a informácií č. 2016/1148. Cieľom prijatia novej smernice bolo zaistenie vysokej úrovne kybernetickej bezpečnosti na úrovni EÚ vrátane zohľadnenia digitálnej transformácie urýchlenej pandémiou COVID-19. Smernica aktualizovala zoznam odvetví a činností, ktoré podliehali povinnostiam v oblasti kybernetickej bezpečnosti, pričom tieto subjekty boli rozdelené na subjekty zásadného významu s vyššou dôležitosťou (energetika, doprava, bankovníctvo/finančný trh, zdravotníctvo, vodohospodárstvo, digitálna infraštruktúra, vesmírny priemysel a verejná správa) a subjekty dôležitého významu s nižšou dôležitosťou (odpadové hospodárstvo, poštové a kuriérske služby, potravinárstvo, výrobný priemysel a pod.). Organizačné zmeny zavedené smernicou sa týkali predovšetkým rizikového manažmentu, t. j. hodnotenia a riadenia rizík. Podmienkou bolo aj zavedenie komplexnej bezpečnostnej politiky a tiež zaškolenie zamestnancov. Jednou zo zmien bolo aj zaistenie bezpečnosti dodávateľského reťazca. Technické opatrenia sa týkali zaistenia IT infraštruktúry, medzi ktoré patrila napríklad kontrola prístupových oprávnení v organizácii, správa identít vrátane používateľov a dodávateľov nachádzajúcich sa v externom prostredí, ochrana sietí vrátane ochrany zariadení s prístupom do siete. Smernica nadobudla platnosť 16. januára 2023 a je súčasťou širšej legislatívy charakterizovanej v tabuľke 4.

Tab. 4 Legislatíva EÚ upravujúca kybernetické prostredie

Legislatívny akt	Zámer legislatívneho aktu/nariadenia
Nariadenie o kybernetickej odolnosti	posilnenie pravidiel kybernetickej bezpečnosti v EÚ, zaistenie bezpečnejších a hardvérových a softvérových produktov
Nariadenie o kybernetickej bezpečnosti	posilnenie úlohy agentúry ENISA, posilnenie spolupráce a krízového riadenia v oblasti kybernetickej bezpečnosti
Nariadenie o kybernetickej solidarite	zlepšenie reakcie na kybernetické hrozby v EÚ, vytvorenie európskeho štítu kybernetickej bezpečnosti a núdzového mechanizmu kybernetickej obrany

Zdroj: vlastné spracovanie podľa úpravy Európskej komisie (2024)

Zatiaľ posledným nariadením, ktoré bolo prijaté na úrovni EÚ, bolo nariadenie Európskeho parlamentu a Rady o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami a o zmene nariadenia (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej bezpečnosti). Cieľom prijatia nariadenia bolo zaistiť používanie bezpečnejšieho softvéru a hardvéru na strane kupujúceho, resp. spotrebiteľov. Inštitúcie EÚ pri formulovaní nariadenia vychádzali z argumentu, že kybernetická bezpečnosť je v prípade mnohých produktov nedostatočná, resp. pre množstvo produktov vrátane softvéru nie sú zabezpečené dostatočné aktualizácie počas ich celej životnosti. Akt o kybernetickej bezpečnosti mal tak zaručiť harmonizáciu pravidiel týkajúcich sa uvádzania výrobkov s digitálnou zložkou alebo uvádzania

softvéru na trh. Okrem toho akt o kybernetickej bezpečnosti definoval rámec kybernetickobezpečnostných požiadaviek zameraných na plánovanie, návrhy, vývoj a údržbu softvéru alebo produktov s digitálnym prvkom. Spoločnosti, ktoré ponúkali na trh softvér alebo produkty s digitálnym prvkom, boli zároveň povinné poskytovať zákazníkovi (majiteľovi zariadenia) povinnú starostlivosť, napríklad aktualizácie, počas celého životného cyklu výrobku. Softvér a zariadenia pripojené na internet budú mať označenie CE, ktoré bude spotrebiteľov informovať o skutočnosti, že dané zariadenie bude spĺňať nové normy.

3. Judikatúra SDEÚ v oblasti kybernetickej kriminality

Judikatúra SDEÚ týkajúca sa zaistenia kybernetickej bezpečnosti, resp. páchania kybernetickej kriminality je pomerne skromná. Prvým dôvodom je skutočnosť, že aj napriek úprave kybernetickej bezpečnosti v sekundárnom práve EÚ sa konkrétne táto oblasť rozvíja predovšetkým v poslednej dekáde. Druhým dôvodom je pomerne komplikované vyšetrovanie kybernetických zločinov, resp. vyšetrovanie externých kybernetických hrozieb, čoho výsledkom je rozširovanie zoznamu fyzických a právnických osôb nachádzajúcich sa mimo členských štátov EÚ podieľajúcich sa na kybernetických útokoch (resp. osôb spojených so zodpovednosťou za kybernetické útoky alebo osôb, ktoré poskytli akúkoľvek pomoc na realizáciu alebo pokus o kybernetický útok).

SDEÚ sa v oblasti kybernetickej kriminality zaoberal napríklad legislatívnymi opatreniami, ktoré stanovujú urýchlené uchovanie lokalizačných a prevádzkových dát, a to s cieľom boja proti závažnej trestnej činnosti. SDEÚ sa v spojených veciach C-511/18, C-512/18 a C-520/18 vyjadril, že členské štáty majú povinnosť prijať na účely špecifického trestného vyšetrovania opatrenia, ktoré sa týkajú uchovávania prevádzkových dát. Štáty sú v uvedenom kontexte povinné prijať legislatívne opatrenia umožňujúce orgánom činným v trestnom konaní zaistiť prevádzkové dáta, ktoré sú uložené prostredníctvom prevádzkových systémov. Ide predovšetkým o prípady, keď existuje riziko straty či pozmenenia týchto údajov. Uvedený zásah však môže podľa SDEÚ predstavovať aj závažný zásah do základných práv človeka, a preto je dôležité, aby bolo zaistenie dát zdôvodnené výhradne bojom členského štátu proti závažnej trestnej činnosti, resp. zaistením národnej bezpečnosti. Uchovanie dát musí byť zároveň limitované výhradne na nevyhnutný čas, ktorý je možné predĺžiť iba v prípade odôvodnených okolností, resp. v prípade pretrvávajúcej hrozby.

Záver

V odbornom článku sme sa zaoberali vývojom právnej úpravy kybernetických zločinov na úrovni EÚ. Za cieľ sme si stanovili analyzovať vývoj právnej úpravy kybernetickej bezpečnosti EÚ, pričom sme pracoval s hypotézou, že na vývoj kybernetickej bezpečnosti mala zásadný vplyv predovšetkým Lisabonská zmluva a technologický progres dosiahnutý v poslednej dekáde. Zároveň sme predpokladali, že konkrétne pravidlá spo-

lupráce či identifikácia kybernetických zločinov sú vymedzené v dokumentoch sekundárneho práva EÚ. Stanovenú hypotézu sa nám podarilo potvrdiť ako pravdivú.

Genézu právnej úpravy EÚ, ktorá sa týkala kybernetickej bezpečnosti, sme spracovali v dvoch obdobiach. Prvé obdobie trvalo od roku 1992 (t. j. od prijatia Amsterdamskej zmluvy a vzniku EÚ) do prijatia Lisabonskej zmluvy v roku 2009. Kybernetická bezpečnosť sa v tomto období zameriavala napríklad na boj proti praniu špinavých peňazí, podvodom, na boj proti pohlavnému zneužívaniu detí a proti šíreniu detskej pornografie či na riešenie problematiky útokov cielených na informačné (počítačové) systémy. V druhom období, ktoré sme identifikoval ako obdobie po prijatí Lisabonskej zmluvy, nastal významný technologický progres, ktorý sa ešte viac zintenzívnil v poslednej dekáde. Tieto skutočnosti mali za následok revidovanie dokumentov sekundárneho práva a tiež vydanie nových smerníc, rozhodnutí a nariadení. V legislatíve EÚ boli definované konkrétne trestné činy týkajúce sa kybernetického (počítačového) prostredia, napríklad falšovanie, pozmeňovanie hmotného bezhotovostného platobného nástroja, krádeže bezhotovostných platobných nástrojov, trestné činy podvodu, neoprávnené zamedzenie fungovaniu informačných systémov, neoprávnené zasiahnutie do fungovania počítačového (informačného) systému a pod. Legislatíva EÚ (sekundárne právo) definovala aj kybernetické útoky namierené proti členským štátom a útoky proti EÚ (jej inštitúciám, orgánom a pod.).

Súčasný legislatívny základ kybernetickej bezpečnosti a boja proti kybernetickým podvodom je okrem viacerých smerníc (predovšetkým NIS2, ktorá vstúpila do platnosti v roku 2023) a rozhodnutí tvorený aj viacerými nariadeniami (o kybernetickej odolnosti, kybernetickej bezpečnosti a kybernetickej solidarite). Zatiaľ posledným nariadením, ktoré bolo prijaté v októbri 2024, bol akt o kybernetickej bezpečnosti.

Vzhľadom na výrazný progres v oblasti kybernetiky, robotizácie či digitalizácie spoločnosti je možné aj v budúcnosti očakávať revidovanie legislatívnych dokumentov platných v súčasnosti a tiež vytváranie nových legislatívnych aktov regulujúcich prostredie a chrániacich bezpečnosť používateľov siete, softvéru, informačných a komunikačných prostriedkov.

Literatúra

EUROPEAN COMMISSION. 2023. *The EU Cybersecurity Act*. [online]. Brusel: Európska komisia, 18. 04. 2023. [cit. 10. 10. 2024]. Dostupné na: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

EUROPEAN UNION. 2023. *Dohovor o počítačovej kriminalite*. [online]. Európska únia, 28. 11. 2023. [cit. 10. 10. 2024]. Dostupné na: <https://eur-lex.europa.eu/SK/legal-content/summary/convention-on-cybercrime.html>

EURÓPSKA KOMISIA. 2024. *Politiky kybernetickej bezpečnosti*. [online]. Brusel: Európska komisia, 10. 10. 2024. [cit. 10. 10. 2024]. Dostupné na: <https://digital-strategy.ec.europa.eu/sk/policies/cybersecurity-policies>

EURÓPSKA RADA. 2024. *Kybernetická bezpečnosť: jak EÚ řeší kybernetické hrozby*. [online]. Európska únia, 10. 10. 2024. [cit. 10. 10. 2024]. Dostupné na: <https://www.consilium.europa.eu/cs/policies/cybersecurity/>.

FIALA, P., KRUTÍLEK, O., PITROVÁ, M. 2018. *Evropská unie*. 3. vyd. Brno : CDK, 2018. ISBN 978-80-7325-450-6
SMEJKAL, V. 2022. *Kybernetická kriminalita*. 3. vyd. Praha : Aleš Čeněk, 2022. ISBN 978-80-7380-849-5
TICHÝ, L. a kol. 2014. *Evropské právo*. 5. vyd. Praha : C. H. Beck, 2014. ISBN 978-80-7400-546-6
TOMÁŠEK, M. a kol. 2021. *Právo Evropské unie*. 3. aktualizované vyd. Praha : Leges, 2021, 512 s. ISBN 978-80-7502-491-6

Zoznam právnych aktov Európskej únie

Jednotná akcia 98/428/SVV z 29. júna 1998, ktorú prijala Rada na základe článku K.3 Zmluvy o Európskej únii o vytvorení Európskej súdnej siete
Jednotná akcia 98/699/SVV z 3. decembra 1998 o praní špinavých peňazí, identifikácii, vyhľadávaní, zmrazení, zhabaní a konfiškácii prostriedkov a ziskov z trestnej činnosti
Rámcové rozhodnutie Rady 2001/413/SVV z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov
Rámcové rozhodnutie Rady 2001/500/SVV z 26. júna 2001 o praní špinavých peňazí, identifikácii, vyhľadávaní, zmrazení a konfiškácii prostriedkov a príjmov z trestnej činnosti
Rámcové rozhodnutie Rady 2004/68/SVV z 22. decembra 2003 o boji proti pohlavnému zneužívaniu detí a detskej pornografii
Rámcové rozhodnutie Rady 2005/222/SVV z 24. februára 2005 o útokoch na informačné systémy
Smernica Európskeho parlamentu a Rady 2011/92/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV
Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV
Smernica Európskeho parlamentu a Rady 2014/42/EÚ z 3. apríla 2014 o zaistení a konfiškácii prostriedkov a príjmov z trestnej činnosti v Európskej únii
Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
Rozsudok Súdneho dvora. Spojené veci C-511/18, C-512/158 a C-520/18. [online]. [cit. 10. 10. 2024]. Dostupné online: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:62018CA0511&qid=1728843420751>
Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV
Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019, o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty
Rozhodnutie Rady (SZBP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty
Rozhodnutie Rady (SZBP) 2022/754 zo 16. mája 2022, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty
Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS2)
Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami a o zmene nariadenia (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)
Zmluva o fungovaní Európskej únie. Konsolidované znenie