23. 9. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Regulace kybernetického prostoru a kybernetická bezpečnost

Kybernetický prostor – abstraktní poměrně obtížně představitelný prostor bez hranic, digitální prostředí, v němž se prolínají data, elektronická a komunikační systémy, procesy a sítě, které umožňuje využívat veškeré výdobytky soudobé informační společnosti. Vedle nesčetných přínosů však s sebou nese také řadu rizik.

Cílem tohoto článku je přiblížit základní právní mantinely fungování kybernetického prostoru – jeho regulaci, problematiku kybernetické bezpečnosti a odpovědnosti za protiprávní jednání.

Právní regulace kybernetického prostoru

Na první pohled by se mohlo zdát, že kybernetický prostor je zcela anonymním místem, kde panuje absolutní svoboda a nikdo nemá žádné povinnosti ani odpovědnost. Dnes je fungování kybernetického prostoru a veškeré jednání v něm regulováno právem jako ostatně téměř každá oblast lidské činnosti. Pravidla jsou stanovena jak na mezinárodní úrovni[1], na úrovni Evropském unie[2], tak i na úrovni národní.[3] Další specifická pravidla mohou stanovit rovněž subjekty, které spravují či provozují některé části digitální infrastruktury.

V České republice, stejně jako v jiných zemích, jsou základní aspekty fungování kybernetického prostoru upraveny právními předpisy zejména z perspektivy veřejného práva. Nejedná se o komplexní právní úpravu – řada otázek fungování kybernetického prostoru se řídí obecnou právní úpravou. Právní předpisy, které zmiňují kybernetický prostor se zaměřují zejména na subjekty, kterým je přisuzováno významné postavení, pro fungování kybernetického prostoru. Pro běžné uživatele kybernetického prostoru jsou stanovena zvláštní pravidla či povinnosti týkající se jednání v kybernetickém prostoru spíše výjimečně.

Kybernetická bezpečnost – důraz na prevenci

Tuzemské právní předpisy týkající se kybernetického prostoru se primárně zaměřují na zajištění bezpečnosti a stability jeho fungování a zejména na ochranu před různými hrozbami.

Základním předpisem v této oblasti je zákon o kybernetické bezpečnosti[4] ("ZKB"), který jednak vymezuje kybernetický prostor a kybernetickou bezpečnost, jednak stanoví povinnosti subjektům, které se podílejí na fungování kybernetického prostoru. ZKB rovněž upravuje dozor v oblasti kybernetické bezpečnosti, který vykonává Národní úřad pro kybernetickou bezpečnost („NÚKIB“), opatření k nápravě a příslušné sankce.[5]

ZKB specificky reguluje čtyři základní typy subjektů, správců a provozovatelů. Správcem se přitom rozumí subjekt (orgán nebo osoba), který určuje účel zpracování informací a podmínky provozování informačního systému, provozovatelem potom subjekt, jenž zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém. První skupinu regulovaných subjektů představují **správci a provozovatelé informačního nebo komunikačního systému kritické informační infrastruktury**. Jedná se o entity, které spravují či provozují některý prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, u nějž by narušení jeho

funkce mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu podle zákona o krizovém řízení.[6] Jedná se o subjekty určené nařízením vlády.[7]

Druhým typem regulovaných subjektů jsou **správci a provozovatelé významných informačních systémů**. Jedná se především o informační systémy spravované orgány veřejné moci, u nichž by zásah do bezpečnosti spravovaných informací mohl ohrozit výkon působnosti daného orgánu.

ZKB rovněž dopadá na **správce a provozovatele informačních systémů základních služeb,** tzn. služeb, jejichž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejichž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v energetice, dopravě, bankovnictví, infrastruktuře finančních trhů, zdravotnictví, vodním hospodářství, digitální infrastruktuře či chemickém průmyslu. Regulaci podle ZKB však podléhají pouze ty subjekty, které NÚKIB určí jako významné z hlediska odvětvových a dopadových kritérií.[8]

Vzhledem k významu těchto tří typů subjektů z hlediska zajištění kybernetické bezpečnosti jim ZKB ukládá řadu povinností – přijímat preventivní a reaktivní opatření a informační povinnosti vůči NÚKIB včetně hlášení kybernetických bezpečnostních incidentů, detekce kybernetických bezpečnostních událostí či stanovení specifických požadavků na dodavatele, které při své činnosti využívají.

Poslední skupinou subjektů podléhajících ZKB jsou **poskytovatelé digitálních služeb**, jimž ZKB stanoví relativně omezené povinnosti, zejm. infomačního charakteru.

Dozor nad plněním povinností podle ZKB vykonává NÚKIB, který přijímá opatření v oblasti kybernetické bezpečnosti a spolupracuje s ENISA[9] a zahraničními orgány kybernetické bezpečnosti.[10] Součástí úřadu je tzv. vládní CERT, který zejména analyzuje zranitelnost v oblasti kybernetické bezpečnosti a koordinuje řešení bezpečnostních incidentů v informačních a komunikačních systémech veřejné správy, kritické informační infrastruktury a ve významných informačních systémech.

ZKB dále vymezuje národní CERT,[11] který zajišťuje sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti a koordinaci řešení bezpečnostních incidentů mimo oblast veřejné správy a kritické infrastruktury.[12]

Vedle ZKB se kybernetické bezpečnosti dotýkají další právní předpisy např. zákon o zpracování osobních údajů, zákon o informačních systémech veřejné správy aj.,[13] které upravují zejména ochranu osobních údajů a bezpečnost infrastruktury zejm. ve vztahu k výkonu veřejné správy. I v těchto případech se však povinnosti ukládají primárně subjektům podílejícím se na fungování kybernetického prostoru, a nikoliv koncovým uživatelům.

Další požadavky a povinnosti, které se týkají některých aspektů kybernetické bezpečnosti, resp. řádného fungování kybernetického prostoru, stanoví další právní předpisy mj. v oblasti ochrany osobních údajů a obchodního tajemství, a obecné právní předpisy. Pro řadu subjektů stanoví speciální požadavky v oblasti kybernetické bezpečnosti sektorové právní předpisy, kupř. pro banky a další finanční instituce.[14]

Protiprávní jednání v kybernetickém prostoru

Tak jako ve světě reálném i v prostředí digitálním dochází k jednáním ohrožujícím právem chráněné zájmy či porušujícím právem stanovené povinnosti. I zde se uplatní standardní pohled na protiprávní

jednání z hlediska intenzity zásahu do právem chráněných zájmů a vedle deliktů civilních tak může jít o přestupky či trestné činy.

Obecná pravidla chování subjektů setkávajících se v kybernetickém prostoru (poskytovatelů služeb, správců a provozovatelů informačních a komunikačních systémů, uživatelů atp.) plynou z obecné právní úpravy v občanském zákoníku.[15] Tato pravidla mj. zahrnují obecnou povinnost počínat si tak, aby nedošlo k nedůvodné újmě jiného. S tím souvisí i následná obecná povinnost k náhradě újmy, resp. škody, způsobené jinému jednáním dané osoby, která se uplatní rovněž na jednání v kybernetickém prostoru. Kromě toho OZ upravuje například i ochranu osobnosti člověka a jeho soukromí či ochranu práv k obchodní firmě podnikatele. Uplatní se rovněž obecná úprava odpovědnosti v rámci pracovněprávních vztahů,[16] např. pokud zaměstnanec, který, byť řádně proškolen, poruší své povinnosti v oblasti kybernetické bezpečnosti vyplývající z interních předpisů, vzniká povinnost zaměstnance k náhradě škody, kterou zaměstnavateli způsobí.

V rámci veřejnoprávních předpisů je stanovena celá řada povinností týkající se kybernetického prostoru, resp. kybernetické bezpečnosti, zejm. správcům a provozovatelům kritických či jinak významných informačních a komunikačních systémů a pro případ porušení předmětných povinností jsou stanoveny skutkové podstaty přestupků a příslušné sankce.

Rovněž jednotliví uživatelé kybernetického prostoru podléhají správním sankcím za porušení právních povinností, resp. právem chráněného zájmu, v kybernetickém prostoru, které nedosáhne společenské závažnosti trestného činu či jej nelze podřadit pod skutkovou podstatu některého z trestných činů.

V rámci kybernetického prostoru se každý uživatel může dopustit např. přestupku proti občanskému soužití podle zákona o přestupcích,[17] který spočívá ve způsobení újmy jiné osobě pro její národnostní příslušnost, rasu, barvu pleti, pohlaví apod. Tohoto přestupku je možné se dopustit urážlivým, xenofobním a jiným hanlivým vyjadřováním na sociálních sítích a jiných platformách digitálního prostoru. Osobě, která se takového přestupku dopustí lze pak uložit pokutu či omezující opatření.

Vzhledem ke stále rostoucímu podílu lidských činností realizovaných elektronicky v kybernetickém prostoru se zásadním způsobem zvyšuje význam trestněprávní úpravy jednání v kyberprostoru. Trestné činy jako nejzásadnější případ porušení právní povinnosti v souvislosti s kybernetickým prostorem zaznamenaly v posledních letech významný nárůst a jejich obzvláštní závažnost je vnímána stále více jak odbornou, tak i laickou veřejností. Ve většině případů se nejedná o zcela nové typy trestných činů, které by nebyly známy dříve, spíše jde o využití možností, které kybernetický prostor k páchání trestné činnosti skýtá.

Trestní zákoník[18] vedle obvyklých skutkových podstat trestných činů vymezuje rovněž skutkové podstaty specificky se vážící k informačním a komunikačním systémům.[19] Úprava v TZ mj. postihuje jednání v případech kriminálního jednání směřující proti informačním či komunikačním systémům nebo tyto prostředky ke spáchání této trestné činnosti využívá.[20]

Nejčastější případy kybernetické kriminality představují podvodná jednání v podobě podvodných nabídek půjček, přivýdělku z domova atp.[21] Tyto mohou být rozšiřovány nejen prostřednictvím e-mailu, ale i v rámci sociálních sítí jako je Facebook či Instagram. Markantně rostoucím rizikem je hacking. Významný podíl na nárůstu počtu a závažnosti případů hackingu má snadný přístup k mnohým předpřipraveným kódům malwaru (škodlivého softwaru), které lze velmi snadno („jedním kliknutím“) rozeslat jednomu, tisícům či milionům dalších uživatelů, aniž by dotyčný pachatel nutně potřeboval expertní znalost informačních systémů či rozsáhlé „hackerské“ zkušenosti.

Další typ trestné činnosti představuje krádež identity a odcizení citlivých údajů, jakož i phishingové útoky za účelem získání podvodného přístupu na bankovní účty a odcizení peněžních prostředků.

V neposlední řadě kybernetická kriminalita zahrnuje mravnostní trestné činy, jako jsou šíření pornografie (zejména dětské) a ohrožování výchovy dítěte, a trestné činy podněcování nenávisti, vydírání, šíření poplašných zpráv a mnohé jiné.[22]

Závěr

V závěru lze shrnout, že právní předpisy ve vztahu ke kybernetickém prostoru primárně stanoví speciální povinnosti zejména subjektům majícím zvláštní význam pro fungování kybernetického prostoru zejm. jako správci a provozovatelé některých informačních a komunikačních systémů anebo poskytovatelé služby (veřejnoprávní i soukromoprávní subjekty). Nicméně, i pro běžné uživatele (fyzické a právnické osoby), stanovuje právní řád řadu norem chování pro pohyb v digitálním prostoru. I v případě porušení právních povinností v kybernetickém prostoru se uplatní standardní civilní, správní a trestní odpovědnost. Postupně se objevují nové skutkové podstaty kybernetických deliktů, které se týkají rovněž právnických osob. Kybernetická bezpečnost přináší řadu výzev jak pro obchodní korporace, tak i pro další instituce, rizika, která je nutno zohlednit nejen v interních předpisech a postupech pro obchodní a další činnost, ale též ve vnitřní kontrole a v compliance programech.

Mgr. Ing. et Ing. Zdeněk Husták, PhD.,
Partner, Regulation & Compliance

Mgr. Alžběta Bělova,
advokátní koncipient

BBH, advokátní kancelář, s. r. o.

Klimentská 1207/10
110 00 Praha 1

Tel.: +420 234 091 355
Fax: +420 234 091 366
e-mail: legal@bbh.cz

---

[1] Především normy skupiny ISO 27000 vydávané Mezinárodní organizací pro normalizaci, či normy NIST publikované americkým Národním institutem pro normy a technologie, jakož i jednotlivé mezinárodní dohody či úmluvy směřující proti potírání kybernetické trestné činnosti.

[2] Úmluva Rady Evropy č. 185 o kybernetické kriminalitě, množství směrnic, nařízení a rámcových rozhodnutí Rady EU směřujících na ochranu počítačových programů, bezpečnost informačních systémů a potírání projevů kybernetické kriminality.

[3] Například zákon č. 181/2014 Sb., o kybernetické bezpečnosti, zákon č. 40/2009 Sb., trestní zákoník, zákon č. 127/2005 Sb., o elektronických komunikacích, zákon č. 365/2000 Sb., o informačních systémech veřejné správy, zákon č. 110/2019 Sb., zákon o zpracování osobních údajů, zákon č. 412/2005 Sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

[4] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů.

[5] Blíže např. k dispozici >>> zde.

[6] Zákon č. 240/2000 Sb., o krizovém řízení a změněn některých zákonů (krizový zákon) ve znění pozdějších předpisů („KZ“).

[7] Nařízení vlády 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury ve znění pozdějších předpisů. K tomu blíže např. k dispozici >>> zde.

[8] Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby („VKUPZS“).

[9] Evropský orgán pro kybernetickou bezpečnost (European Union Agency for Cybersecurity).

[10] Včetně národních bezpečnostních týmů CSIRT (Computer Security Incident Response Team).

[11] Na základě veřejnoprávní smlouvy s NÚKIB je dnes jeho provozovatelem sdružení právnických osob CZ.NIC.

[12] Další informace jsou dostupné např. k dispozici >>> zde.

[13] Zákon č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 365/2000 Sb., o informačních systémech veřejné správ ve znění pozdějších předpisů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů.

[14] Např. zákon č. 370/2018 Sb., o platebním styku ve znění pozdějších předpisů.

[15] Zákon č. 89/20112 Sb., občanský zákoník ve znění pozdějších předpisů („OZ“).

[16] Podle zákona č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů.

[17] Zákon č. 251/2016 Sb., o přestupcích ve znění pozdějších předpisů.

[18] Zákon č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů („TZ“).

[19] Jedná se například o trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§230), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231) či poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232). Relevantní jsou rovněž trestné činy neoprávněné nakládání s osobními údaji (§180), porušení tajemství dopravovaných zpráv (§182), šíření pornografie (§ 191) nebo výroba a jiné nakládání s dětskou pornografií (§ 192), porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270), hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355), pomluva (§ 184), vydírání (§ 175), šíření poplašné zprávy (§ 357).

[20] Kolouch, J. CyberCrime. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016, 522 s., s. 340-341.

[21] K tomu blíže zpráva o bezpečnostní situaci na území České republiky za rok 2018, str. 47 an., k dispozici >>> zde.

[22] Podrobné statistiky kybernetických trestných činů za roky 2011-2018 v České republice jsou k dispozici >>> zde.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Judikatura: smluvní sjednání prekluzivní lhůty je obecně platné (FIDIC)
- Civilněprávní prostředky ochrany při koupi falzifikátu
- Novela zákona o pyrotechnice: likvidace profesionálů namísto zmírnění negativních vlivů
- Konec zákonné koncentrace řízení? Návrh Nejvyššího soudu před Ústavním soudem
- Soudní poplatky v řízení o rozvodu manželství a úpravy poměrů k nezletilému dítěti po tzv. rozvodové novele
- Imise ve stavebním řízení aneb kde končí veřejný zájem a začíná soukromé právo?
- Užívání prostoru nad pozemkem třetí osobou
- Přístup k nemovitosti přes pozemek třetí osoby
- PŘEHLEDNĚ: Jak funguje předkládání plné moci? Postačí soudu jen její „fotokopie“? Aneb vývoj právní úpravy požadavků na plnou moc v našem právním systému.
- Využívání nástrojů umělé inteligence: proč je GDPR relevantní?
- Transfer Pricing: Na co si dát pozor s blížícím se koncem roku