Kyberkriminalita

Kyberkriminalita

Z hlediska práva lze tedy kyberkriminalitu zařadit do kategorie trestního práva, přičemž ji lze studovat z tří základních právních hledisek. Jednak z hlediska hmotněprávní úpravy, tedy z hlediska toho, co je za kyberkriminalitu považováno, jak jsou formulovány příslušné skutkové podstaty, na jaké aktivity se vztahují a jak jsou nastaveny trestní sazby. Z hlediska procesněprávního lze především posuzovat dostupnost a efektivitu procesních nástrojů, které trestněprocesní předpisy poskytují orgánům činným v trestním řízení k vyšetřování kyberkriminality, dopadení pachatele a zajišťování elektronických důkazů. A konečně z hlediska mezinárodního práva veřejného lze zkoumat limity mezinárodní justiční a policejní spolupráce při vyšetřování přeshraniční kyberkriminality a možnosti harmonizace právních úprav a implementace nových mechanismů pro mezinárodní součinnost a předávání důkazů.

Aktuální právní úprava kyberkriminality

Úmluva o počítačové kriminalitě představuje komplexní mezinárodní nástroj pro řešení problematiky kyberkriminality. Je rozdělena do čtyř kapitol, zahrnujících problematiku hmotného a procesního práva, stejně jako mezinárodní spolupráci.

Procesní část Úmluvy obsahuje úpravu procesních prostředků pro získávání a práci s elektronickými důkazy. Důvodem této harmonizace mimo jiné je, aby v rámci mezinárodní spolupráce měly signatářské státy jistotu, že dožadovaný stát bude disponovat vhodnými procesními prostředky pro realizaci vyžádaných úkonů. Tato část obsahuje nástroje jako:

– urychlené uchování uložených počítačových dat, neboli takzvaný freezing order, jímž mají být data u poskytovatelů služeb ochráněna před smazáním nebo změnou uživatelem, aby mohla být následně vyžádána jako důkazní prostředek;

– urychlené zachování a částečné zpřístupnění provozních dat, směřující ke stejnému cíli v případě provozních a lokalizačních údajů nezbytných pro identifikaci pachatele;

– příkaz k předložení, který orgánům činným v trestním řízení umožňuje požadovat od držitelů dat jejich poskytnutí pro potřeby trestního řízení;

– prohlídku a zajištění uložených počítačových dat, pro případ, kdy je nevhodné všechna data dožadovat a je efektivnější tato analyzovat přímo v zařízení nebo na datových nosičích poskytujících osob;

– shromažďování provozních dat v reálném čase, za účelem dohledání pachatele či důkazů o trestném činu; a

– odposlech obsahových dat prostřednictvím technických nástrojů umožňujících záznam obsahu elektronické komunikace.

■ porušení tajemství dopravovaných zpráv (§ 182 zákona č. 40/2009 Sb.

porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 zákona č. 40/2009 Sb.)

■ neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 zákona č. 40/2009 Sb.) ■ opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 zákona č. 40/2009 Sb.)

■ poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 zákona č. 40/2009 Sb.)

■ neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234)

■ výroba a držení padělatelského náčiní (§ 236

■ Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních

■ Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže

■ Balík zákonů upravující problematiku ochrany duševního vlastnictví

■ Zákon č. 127/2005 Sb., o elektronických komunikacích a jeho prováděcí vyhlášky

■ Zákon č. 480/2004 Sb., o některých službách informační společnosti

■ Nařízení EU č. 2016/679, obecné nařízení o ochraně osobních údajů

■ Zákony upravující právní povahu a nakládání s daty, elektronickými dokumenty, elektronickými podpisy apod.

Taxonomie kyberkriminality

Kyberkriminalita je z hlediska svých projevů velmi dynamickým fenoménem. Jak se rozvíjí informační komunikační technologie a vznikají nové způsoby jejich využívání a nové služby jejich prostřednictvím poskytované, vznikají také stále nové způsoby jejich zneužívání. Katalog aktivit, které lze považovat za kyberkriminalitu, tak nebude nikdy konečný – některé přestávají být díky novým bezpečnostním technologiím nebo zastaralosti postupů atraktivní, zatímco jiné vznikají a mechanismus jejich fungování třeba není dokonale zmapován.

Stíhání kyberkriminality

Odhalování, prověřování a vyšetřování kyberkriminality má svá specifika, díky kterým je nutné, aby orgány činné v trestním řízení disponovaly dostatečně kvalifikovaným personálem, který dokáže po technické stránce porozumět příslušným technologiím a volit takové procesní prostředky, které na jednu stranu umožní efektivní dohledání pachatele a zmapování příslušné trestné činnosti a na druhou budou v souladu procesní úpravou trestního řízení. Následující podkapitoly proto pojednávají o organizační připravenosti českých orgánů činných v trestním řízení pro řešení problematiky kyberkriminality a specificích trestního stíhání kyberkriminality z hlediska využitých procesních nástrojů a postupů.

Významným předpokladem pro efektivní zvládání kyberkriminality na straně orgánů činných v trestním řízení je dobrá orientace nejen v samotných technologiích, které jsou při páchání využívány, proti kterým je tato trestná činnost namířena, nebo které mohou představovat vhodný zdroj operativního nebo důkazního materiálu, ale také znalost procesních nástrojů, prostřednictvím kterých je možné přístup k relevantním datům a informacím získat.

Jelikož nelze aktuální procesní úpravu trestního řízení považovat za dokonalou a pro potřeby trestního řízení v případech kyberkriminality přívětivou, je často nutné za účelem dosažení kýžených výsledků pracovat s dostupnými nástroji poněkud kreativně. V podstatě v každém stadiu trestního řízení se objevují v případě kyberkriminality specifické prvky, v dalším výkladu se proto na ty významné zaměříme.

V případech kyberkriminality se velice často vyskytuje mezinárodní prvek, kdy se například pachatel nachází v jednom státě, informační systém, na který útočí nebo využívá k útoku, je v druhém státě a škoda vzniká ve třetím státě. V takových případech se předpokládá úzká spolupráce na mezinárodní úrovni mezi policejními a justičními orgány, která by navíc měla probíhat efektivně vzhledem k volatilitě elektronických důkazů. Existující mechanismy mezinárodní spolupráce v trestních věcech však často nejsou dostatečně efektivní, aby umožňovaly včasnou reakci na přeshraniční požadavky na realizaci procesních úkonů. Jelikož si tento stav mezinárodní společenství uvědomuje, vznikají různé nástroje směřující ke zefektivnění postupů. Ty zasahují jak do práva hmotného, tak procesního.

Elektronické důkazy

Jelikož je trestní řád i přes velké množství jeho novelizací poněkud zastaralým právním předpisem, je často nutné elektronické důkazní prostředky zajišťovat prostřednictvím nepříliš vhodných procesních nástrojů, použitých kreativně tak, aby pokryly i případy elektronických důkazních prostředků trestním řádem původně nezamýšlené. Proto jsou často elektronické důkazy zajištěny postupem v praxi netestovaným a legislativně a judikatorně nezachyceným, což vyvolává riziko, že by se mohl jeho prostřednictvím získaný důkaz stát v trestním řízení nevyužitelný. Jasné limity stanovuje § 89 odst. 3 zákona č. 141/1961 Sb., který za absolutně nepřípustný považuje takový důkaz, který byl získán nezákonným donucením. Důkazy však mohou být v trestním řízení absolutně či relativně neúčinné i z jiných důvodů – například v případě, že je orgánem činným v

trestním řízení zvolen nevhodný procesní prostředek k jejich zajištění. Takový postup totiž může být vyhodnocen jako podstatná vada postupu způsobující absolutní či relativní (může-li být taková vada odstraněna) neúčinnost získaných důkazů.

Druhým způsobem, kterým lze získat elektronické důkazy, je prostřednictvím dat získaných ze vzdálených úložišť nebo služeb. To lze opět provést několika způsoby. Prvním a nejjednodušším způsobem je získání informací volně dostupných v síti. Není-li překonáváno žádné bezpečnostní opatření, lze v podstatě bez dalšího přistupovat k obsahu dostupnému v prostředí internetu a pořizovat z něj důkazní prostředky.

Data, která mohou být neocenitelným zdrojem důkazů v trestním řízení, mohou být získávána také přímo od poskytovatelů informačních služeb. Při volbě procesního nástroje, prostřednictvím kterého budou data zajišťována, je třeba z hlediska trestního procesu zohlednit dvě základní hlediska.

Prvním hlediskem je charakter poskytovatele, od kterého data žádáme. Poskytovatelé informačních služeb se totiž dají rozdělit na dvě základní skupiny.

Získání elektronických důkazních prostředků je teprve prvním krokem v procesu dokazování prostřednictvím elektronických dat. Data jako taková mají díky svému charakteru jen minimální vypovídací hodnotu. Teprve ve chvíli, kdy jsou interpretována na informace, je možné začít hovořit o důkazu. Vzhledem k vlastnostem dat a elektronických zařízení je, jak je naznačeno výše, poměrně technicky náročné nejen vyhodnocovat jejich informační obsah, ale mnohdy jej i v sumě dat identifikovat. K těmto úkonům lze nicméně využívat více či méně technicky sofistikované nástroje pro forenzní analýzu.

Revision #1
Created 2025-05-28 13:15:37 UTC by Magdalena Dobešová
Updated 2025-05-28 13:17:19 UTC by Magdalena Dobešová