Úmluva o kybernetické kriminalitě (soulad české právní úpravy s ustanoveními Úmluvy)

JUDr. Tomáš Gřivna, Ph.D.

Obsah

- Úvodem
  - Proč Úmluva vznikla
  - Jak Úmluva vznikla
  - Struktura Úmluvy
  - Používané pojmy
- Závazky hmotněprávní povahy (povinnost kriminalizace některých jednání)
- Závazky procesněprávního charakteru (povinnost umožnit některá procesní opatření)
- Závazky v oblasti mezinárodní spolupráce
- Závěrem

Proč Úmluva vznikla

- Rozvoj informačních a telekomunikačních technologií – připojením na komunikační a informační služby vytváří uživatelé určitý druh společného prostoru = kyberprostor
- Vedlejší produkt = prostor pro společensky nebezpečné aktivity nového typu
- Právní ochrana tradičními instituty nepostačuje
  - nové jevy nejsou postižitelné starými normami
  - působnost trestních norem je omezena (trestní právo je projevem státní suverenity, neexistuje nadnárodní trestní právo)
  - překrývání jurisdikcí
- Snaha o efektivní postih (je-li zločin v kyberprostoru bez hranic, musí být i postih bez hranic nebo alespoň s co nejmenšími překážkami)
- Různorodost a odlišnost národních úprav – problém shodnout se na závazném minimu; je-li konsensu dosaženo – relativizace připuštěním výhrad či odchylných ujednání

Jak Úmluva vznikla, stav ratifikací

- 4 roky práce expertů RE, USA, Kanady, Japonska
- schválena Výborem ministrů Rady Evropy na jejím 109. zasedání 8. listopadu 2001
- Otevřena k podpisu byla v Budapešti dne 23. listopadu 2001. V platnost vstoupila dne 1. července 2004 (5 ratifikací).
- Úmluvu podepsalo 44 států, z nichž jí však ratifikovalo jen pouhých 50 %. Z nečlenských států podepsaly a zároveň ratifikovaly jen USA.
- Česká republika podepsala Úmluvu dne 9.2.2005. K její ratifikaci prozatím nedošlo,
- Slovenská republika - Úmluvu podepsala dne 4.2.2005, ratifikovala 8.1.2008, v platnost vstoupila dnem 1.5.2008.
- K Úmluvě byl přijat Dodatkový protokol (kriminalizace činů rasistické a xenofobní povahy spáchané prostřednictvím počítačového sytému) - otevřen k podpisu 28.1.2003, vstoupil v platnost 1.3.2005, podepsalo jej 33 států, z toho ratifikovalo jen 12 (stav k 8.5.2008).

Struktura Úmluvy

- 48 článků
- preambule + 4 kapitoly
  - Kapitola I. - používání pojmů
  - Kapitola II. - opatření přijímaná na národní úrovni:
    - upravuje závazky států v oblasti trestního práva hmotného (oddíl 1)
    - i procesního (oddíl 2)
    - včetně ustanovení o působnosti vnitrostátních norem (oddíl 3).
  - Kapitola III. - závazky na poli mezinárodní spolupráce
  - Kapitola IV. - závěrečná ustanovení

Používané pojmy

- **Počítačovým systém** = jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat.
- **Počítačová data** = jakékoli vyjádření skutečností, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu vhodného k zajištění, aby počítačový systém vykonával určitou funkci.

Používané pojmy

- **Poskytovatelem služeb** se podle Úmluvy rozumí:
  - a) jakýkoli veřejný nebo soukromý subjekt, který poskytuje uživatelům služby možnost komunikovat prostřednictvím počítačového systému, a
  - b) jakýkoli jiný subjekt, který zpracovává nebo ukládá počítačová data pro tuto komunikační službu nebo uživatele této služby.
  - poznámky:
    - pojem zahrnuje soukromé i veřejné subjekty;
    - je nerozhodné, zda uživatelé služeb tvoří uzavřenou skupinu (např. zaměstnanci jedné společnosti) či je služba poskytována veřejně;
    - není rozhodující, zda je služba poskytována za úplatu anebo zdarma.
    - podle bodu b. bude poskytovatelem služby i ten, kdo poskytuje vyrovnávací paměť pro internetové stránky (caching), zajišťuje provoz aplikace třetí osoby na vlastním technickém a programovém vybavení (hosting), tak služby, které poskytují připojení k síti;
    - definice nezahrnuje pouhé poskytovatele obsahu, pokud takový obsah nenabízí také komunikaci nebo související služby zpracování dat.

Používané pojmy

- **Provozními daty =** jakákoli počítačová data související s přenosem dat prostřednictvím počítačového systému, generovaná počítačovým systémem, který tvořil součást komunikačního řetězce, jež vyjadřují původ, cíl, trasu, dobu, objem, dobu trvání přenosu dat nebo druh použité služby.
  - provozními daty jsou tedy data, která slouží k nasměrování komunikace od místa původu do místa určení (od odesílatele k adresátovi);
  - ve vztahu ke komunikaci, která tvoří tzv. obsahová data, plní pouze pomocnou úlohu;
  - jejich zachycení nevede k odhalení obsahu sdělení;
  - jejich specifikem je též skutečnost, že mohou trvat pouze krátkou dobu. Z toho pak plyne požadavek jejich co nejrychlejšího zjištění a zajištění.
  - Úmluva sama specifikuje, co tvoří provozní data. Jsou to data o původu komunikace (tj. telefonní číslo, IP adresa nebo jiná identifikace komunikačního zařízení, jemuž poskytovatel služby poskytuje službu), určení komunikace (tedy telefonní číslo, IP adresa nebo jiná identifikace komunikačního zařízení, jemuž se příslušné komunikace, sdělení, zasílají), trasa, čas, délka, trvání a typ příslušné služby. Typem příslušné služby se rozumí typ (druh) služby používaný v síti, např. přenos souborů, elektronická pošta nebo okamžité posílání a příjem zpráv.

Závazky hmotněprávní povahy - obecně

- Úmluva obsahuje
  - znaky 9 trestných činů, které dělí do 4 kategorií;
  - úpravu některých otázek základů trestní odpovědnosti (trestnost účastenství, pokusu trestného činu; zavedení alespoň tzv. nepravé trestní odpovědnost právnických osob);
  - požadavky na sankce - účinné, přiměřené a odstrašující;
  - problém: odpovědnost právnických osob

Závazky hmotněprávní povahy – obecně ke všem jednáním, jejichž kriminalizace se požaduje

- výslovně je uveden znak **protiprávnosti** slovy „neoprávněně“, „protiprávně“
- ani jeden z definovaných činů **nelze spáchat z nedbalosti**
- u některých z činů se vyžaduje tzv. **druhý (specifický) úmysl**
- v řadě případů je umožněno omezení trestnosti jen na závažnější případy, tj. že smluvní stát bude k trestnosti vyžadovat naplnění tzv. **dodatečné náležitosti** (**další kvalifikační okolnosti**), např.
  - porušení bezpečnostních opatření,
  - nečestný úmysl pachatele,
  - čin je spáchán ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem,
  - jednání může vést ke vzniku závažnější škody,
  - držení je trestné jen při držení určitého počtu věcí.
- **možnost** smluvních států **učinit výhradu k aplikaci** některých taxativně vyjmenovaných článků

Neoprávněný přístup

- pouhé neoprávněné vniknutí, tj. „průnikaření“ („*hacking*“; „*cracking*“; „*computer trespass*“) by již v zásadě mělo být podle čl. 2 samo o sobě protiprávní.
- průnik do počítačového systému je často jen přípravou k závažnějšímu činu.
- **možnost dodatečných kvalifikačních okolností** (porušení bezpečnostních opatřením, úmysl získat počítačová data nebo jiný nečestný úmysl, nebo čin je proveden ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem)

Neoprávněný přístup - česká právní úprava

- **Podle trestního zákona** (§ 257a TZ – poškození a zneužití záznamu na nosiči informací) je trestné získání přístupu k nosiči informací, pokud jsou kumulativně splněny dvě podmínky:
  - pachatel tak činí v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, což by ještě bylo v souladu s Úmluvou pokryto možností aplikovat dodatečné okolnosti, a
  - pachatel se dopustí některého z alternativně uvedených jednání: a) takových informací neoprávněně užije; b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými; nebo c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení. Tyto zužující podmínky však již nejsou v souladu s Úmluvou.
- **Návrh trestního zákoníku** upravuje v § 228 trestný čin **Neoprávněný přístup k počítačovému systému a nosiči informací**.
  - V odstavci 1 je trestné, jestliže někdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části.
  - překonání bezpečnostních opatření - nutnost učinit prohlášení podle čl. 40 Úmluvy.

Neoprávněné zachycení informací

- ochrana práva na soukromí datové komunikace; „odposlech“;
- všechny formy přenosu elektronických dat (např. telefonem, faxem, elektronickou poštou, přenosem souborů);
- není však zamýšlena kriminalizace používání běžných praktik jako jsou „cookies“.
- **jednání** spočívá v zachycení neveřejných přenosů počítačových dat pomocí technických prostředků, a to z nebo v rámci počítačového systému, včetně zachycení elektromagnetických emisí z počítačového systému, obsahující taková počítačová data.
  - veřejně dostupná informace může být mezi účastníky přenášena důvěrně (neveřejně)
  - problém komunikace zaměstnanců (§ 316 ZP)
- **dodatečné kvalifikační okolnost** - nečestný úmysl nebo je-li čin proveden ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem

Neoprávněné zachycení informací –česká úprava

- § 239 a 240 - trestný čin porušování tajemství dopravovaných zpráv.
  - podle § 239 odst. 1 písm. b) se dopustí tohoto trestného činu, kdo úmyslně poruší tajemství zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením.
  - přenos počítačových dat nemusí být patrně vždy „zprávou“ ve smyslu § 239 TZ.
  - odposlech elektromagnetických emisí z počítačového systému?
- **Návrh trestního zákoníku** - § 180 odst. 1 písm. c): TČ se dopustí, kdo úmyslně poruší tajemství neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování počítačového systému, přenášejícího taková počítačová data.

Zásah do dat

- **Objektivní stránka** spočívá v poškození, vymazání, zhoršení kvality, změně nebo potlačení počítačových dat.
  - Potlačením dat = zabránění jejich upotřebitelnosti. Pod toto ustanovení lze subsumovat činnost „zákeřných programů“ jako jsou viry a trojské koně.
  - **oprávněná** (nikoliv protiprávní) **činnost** - testování ochrany bezpečnosti počítačového systému schválené vlastníkem nebo operátorem, anebo rekonfigurace operačního systému počítače, která probíhá v případech, kdy operátor systému získá nové programové vybavení (například software umožňující přístup k Internetu a vyřazující z činnosti podobné, dříve instalované programy).
  - modifikace provozních dat za účelem usnadnění anonymních komunikací (například činnost systémů pro anonymní (pře)posílání emailové pošty – „*anonymous remailer systems*“) anebo modifikace dat za účelem zabezpečení komunikací (například zašifrování) by se v zásadě měly považovat za legitimní ochranu soukromí, a tedy za úkony provedené oprávněně. Smluvní strany však mohou kriminalizovat určitá zneužití týkající se anonymních komunikací, jako například změnu informace v záhlavích paketů („*packet header information*“), aby se skryla totožnost pachatele trestného činu.

Zásah do dat – česká právní úprava

- Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch informace zničí, poškodí, změní nebo učiní neupotřebitelnými (**poškození a zneužití záznamu na nosiči informací podle § 257a odst. 1 písm. b) TZ);**
- **§ 228 odst. 2 písm. b) Návrhu:** za trestný čin prohlašuje jednání, kterým někdo získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými.

Zásah do systému

- čin lze označit též za tzv. počítačovou sabotáž;
- objektivní stránka spočívá v závažném narušení fungování počítačového systému vložením, přenesením, poškozením, vymazáním, zhoršením kvality, změnou nebo potlačením počítačových dat.
  - přílišné kriminalizaci má zabránit požadavek, aby narušení fungování systému bylo *závažné*.
  - Sem patří též odesílání dat určitému systému v takové podobě, objemu nebo frekvenci, že to má za následek významný škodlivý vliv na schopnost vlastníka nebo operátora využívat systém nebo komunikovat s ostatními systémy, například prostřednictvím programů, které generují útoky typu odepření služby („*denial of service*“), škodlivé („*malicious*“) kódy jako jsou viry, které zabraňují chodu systému, nebo jej podstatně zpomalují, anebo programy, které odesílají velká množství elektronické pošty příjemci, aby zablokovaly komunikační funkce systému.
  - „spamming“ lze podle čl. 5 Úmluvy kriminalizovat pouze tehdy, je-li závažně omezena funkčnost komunikace.

Zásah do systému – česká právní úprava

- **§ 257a TZ** umožňuje kriminalizovat zásah do technického nebo programového vybavení počítače (nebo jiného telekomunikačního zařízení);
  - porovnáním obsahu obou pojmů „počítač“ (TZ) a „počítačový systém“ (Úmluva) zjistíme, že jsou v mnoha směrech shodné, pojem počítačový systém je bezpochyby širší;
  - trestní zákon navíc požaduje, aby tak pachatel učinil v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch - současný trestní zákon nechrání specificky narušení počítačového systému, jak vyžaduje Úmluva.
- **Návrh trestního zákoníku** stanoví jako okolnost podmiňující použití vyšší trestní sazby podle § 228 odst. 3 písm. b), jestliže pachatel spáchal trestný čin podle odst. 1 nebo 2 v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Jelikož odst. 1 kriminalizuje již pouhý neoprávněný přístup k počítačovému systému, a jelikož se nevyžaduje, aby došlo k omezení funkčnosti (postačí, že k tomu směřoval úmysl pachatele), jde navrhovaná úprava nad rámec závazku.

Zneužití zařízení

Objektivní stránka spočívá v

b) výrobě, prodeji, obstarání k užívání, dovozu, distribuci nebo jiném zpřístupnění:

i zařízení, včetně počítačového programu, určeného nebo přizpůsobeného **primárně** pro účely spáchání kteréhokoli trestného činu stanoveného v souladu s články 2 až 5;

ii počítačového hesla, přístupového kódu nebo podobného údaje, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

e) držbě jakékoli věci uvedené v písmenu a) bodech (i) a (ii).

- zpřístupnění nevyžaduje aktivní přístup pachatele (např. umístění hackerského programu na internet ke stažení; uvedení tzv. hyperlinku pro usnadnění přístupu k takovému nástroji);
- primárně = obvykle vyloučí zařízení s dvojím využitím (legálním i nelegálním);
- nevztahuje se na oprávněné testování ochrany počítačového systému;
- vyžaduje se specifický úmysl = využití zařízení pro účely spáchání kteréhokoli z TČ stanovených v Úmluvě;
- **dodatečnou kvalifikační okolností** v případě držení podle písm. b. - možnost určit minimální počet takových věcí;
- **výhrada:** neuplatňovat tento článek, pokud se taková výhrada netýká prodeje, distribuce nebo jiného zpřístupňování věcí uvedených v odstavci 1 písm. a) bodu (ii).

Zneužití zařízení – česká právní úprava

- **Český TZ** nemá skutkovou podstatu, která by kriminalizovala jednání vymezené v čl. 6 Úmluvy. Příprava k § 257a (poškození a zneužití záznamu na nosiči informací) není trestná; nejde o zvlášť závažný trestný čin.
- **Návrh trestního zákoníku:** § 229 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat).
  - návrh na rozdíl od Úmluvy nestanoví, že zařízení je určeno nebo přizpůsobeno primárně pro účely spáchání uvedených trestných činů; vyžaduje, aby zařízení bylo vytvořeno nebo přizpůsobeno k neoprávněnému přístupu.

Trestné činy související s dětskou pornografií

- Objektivní stránka spočívá v:
- výrobě dětské pornografie pro účely distribuce prostřednictvím počítačového systému;
- její nabízení nebo zpřístupňování, *distribuci* nebo *přenášení* prostřednictvím počítačového systému;
- její obstarávání prostřednictvím počítačového systému pro sebe nebo pro jinou osobu; (možnost výhrady)
- její držbě v počítačovém systému nebo na médiu pro ukládání počítačových dat (možnost výhrady).
  - *zpřístupnění* = též „*hyperlinks*“;
  - obsah pojmu pornografický materiál je ponechán na vnitrostátní úpravě;
  - *dítětem* se rozumí dítě mladší 18ti let;
  - pojem „*dětská pornografie*“ zahrnuje pornografické materiály, které vizuálně zobrazují … b) osobu, jež vyhlíží jako dítě, provádějící viditelný sexuální akt; c) realistické zobrazení dítěte provádějícího viditelný sexuální akt; (možnost výhrady)
  - **dodatečnou kvalifikační okolností** může být snížení věkové hranice dítěte až na 16 let.

Dětská pornografie a český TZ

- Novelizace (zákon č. 271/2007 Sb., účinný od 1.12.2007) změnila § 205 TZ, změna názvu „Ohrožování mravnosti“, nyní „Šíření pornografie“, ale též jeho znaků. Zavedení nových trestných činů.
- V § 205a je kriminalizováno přechovávání dětské pornografie a v § 205b zneužití dítěte k výrobě pornografie.
- § 205 odst. 2 písm. a) TZ: Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.
- § 205a TZ: Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě.
- Oproti původnímu poslaneckému návrhu není kriminalizováno šíření pornografického díla, které zobrazuje osobu, jež se jeví být dítětem.
- V případě ratifikace Úmluvy bude nezbytné v tomto směru vznést výhradu (viz shora).
- Při přípravě novely bylo využito **Návrhu trestního zákoníku**, proto současná právní úprava se v zásadě shoduje s návrhem.

Závazky procesněprávního charakteru

- nové způsoby zneužívání kybernetického prostoru - vytvoření nových, popř. úpravu stávajících (tradičních) procesních institutů, které umožní odhalit pachatele a zajistit důkazy, jež mohou vést k jeho usvědčení;
- diskuse, zda by neměla být uložena poskytovatelům služeb povinnost po určitou dobu shromažďovat a uchovávat data;
- **data provozní**, **data obsahová** a **data o odběratelích**
- následující **procesní opatření**:
  - bezodkladné uchování uložených počítačových dat (čl. 16),
  - bezodkladné uchování a částečné poskytnutí (zpřístupnění) provozních dat (čl. 17),
  - příkaz k vydání (čl. 18),
  - prohlídka a zajištění uložených počítačových dat (čl. 19),
  - shromažďování provozních dat v reálném čase (čl. 20),
  - zachycení dat o obsahu (čl. 21).

Závazky procesněprávního charakteru

- **procesní opatření významně zasahují do práva a svobod osob** (zásada subsidiarity a přiměřenosti).
- opatření je možné použít vždy jen **v konkrétním trestním řízení**. Nelze proto např. nařídit „odposlech“ obsahových dat bez souvislosti s konkrétním trestním řízením.
- stanovení některých opatření, např. příkazu k vydání podle čl. 18, může mít i **význam pro třetí strany** (např. správce dat);
- Trestní řád nemá ustanovení týkající se specificky počítačových dat. Využívají se proto stávající instituty trestního řádu jako např. povinnost k vydání věci (§ 78), odnětí věci (§ 79), zadržení, otevření a sledování zásilky (§ 86 – 87c), odposlech a záznam telekomunikačního provozu (§ 88, 88a), které však s ohledem na specifika počítačových dat nejsou vždy vyhovující.

Závazky v oblasti mez. spolupráce

- **doplňkově ke stávajícím nástrojům**;
- **ČR**, resp. ČSFR podepsala a ratifikovala obě hlavní Úmluvy týkající se právní pomoci ve věcech trestních i dodatkový protokol k druhé z nich;
- **v otázkách neupravených** mezinárodními úmluvami se postupuje **subsidiárně podle ustanovení trestního řádu** (§ 375 – 460y). Není-li právní styk mezi Českou republikou a jiným státem upraven mezinárodní smlouvou, orgány činné v trestním řízení vyhoví žádosti cizího státu jen, **je-li zajištěna vzájemnost**, tj. poskytne-li dožadující stát záruku, že v budoucnu vyhoví obdobné žádosti orgánu České republiky.
- **obsahové vymezení spolupráce -** Úmluva upravuje
  - obecné principy týkající se mezinárodní spolupráce (čl. 23) a vzájemné pomoci (čl. 25, 26),
  - obecné principy týkající se vydávání osob (čl. 24),
  - postupy týkající se žádostí o vzájemnou pomoc v případě neexistence aplikovatelných mezinárodních smluv (čl. 27, 28),
  - konkrétní ustanovení (čl. 29 – 35) včetně sítě 24/7 (čl. 35).

Závěrem

- současná právní úprava není souladná se závazky, zejména pokud jde o vyžadovaná procesní opatření.
- před ratifikací Úmluvy bude tedy třeba novelizovat příslušné zákony.
- bylo by jistě ke škodě, kdyby se Česká republika v důsledku nedostatečné legislativy stala překážkou v boji s kybernetickou kriminalitou na mezinárodní úrovni.

Děkuji za pozornost