



Trestněprávní postih kyberkriminality

odpovědnost za cizí obsah

Primární a odvozená odpovědnost

- Primární – každý (v zásadě) nese odpovědnost za protiprávní obsah, který umístil na Internet
- Odvozená odpovědnost – odpovědnost za cizí obsah:
 - ISP
 - Uživatelé „podporovatelé“
 - Uživatelé - konzumenti

Role zprostředkovatelů - ISP

- Připojit se k Internetu lze jen prostřednictvím subjektů, které přístup na Internet umožňují; při umístění obsahu na Internet využívají uživatelé často služeb jiných osob, které takový prostor nabízejí
- **realizované aktivity** probíhají prakticky bez výjimky **zprostředkovaně**
- zprostředkovatelů je poměrně zásadní, neboť v jejich vůli (faktické moci) je to, zda uživatele připojí, odpojí, jeho příspěvek v diskusi smažou, soubory odstraní apod. - **„definiční autority“**
- „poskytovatelé služeb informační společnosti“ (z.č. 480/2004 Sb.), „service provider“ (Směrnice 2000/31/ES)
- **Information (popř. Internet) Service Provider“ (zkr.„ISP“)**

Směrnice o elektronickém obchodu

- Důvod regulace:
 - Objektivní odpovědnost ISP (PO a podnikající FO za přestupky; civilní delikty); v některých případech i subjektivní odpovědnost za nevědomou nedbalost (FO za přestupky, FO i PO za některé TČ)
 - neudržitelnost konstrukce, že by ISP v každém případě odpovídal za uživatelův obsah
 - Kontrolovat kvanta dat uživatelů
 - Omezovat svobodu projevu (nikoliv veřejnou mocí, ale třetím subjektem)
 - Odvrácená strana: úplné vyloučení odpovědnosti
 - nebylo dostatečné pro ochranu zájmů jednotlivce i společnosti
 - nelze vždy jednoduše zjistit identitu uživatele
 - subjekty, jejichž práva jsou obsahem zasažena nebo ohrožena mají reálně možnosti bránit se požadavkem na zdržení se dalšího šíření obsahu a na jeho odstranění vůči ISP
 - Spravedlivé (?): limitované vyloučení odpovědnost ISP podle druhu poskytované služby

Koncepce: Safe harbour

- pokud ISP dodrží definované podmínky, zůstává vyloučen z odpovědnostních vztahů
- Pokud ISP podmínky poruší a „vyplují“ z bezpečného přístavu, mohou být odpovědni
 - „mohou“
 - „Vyplutí z bezpečného přístavu“ samo o sobě odpovědnost nezakládá, ta je založena až v návaznosti na podmínky odpovědnosti stanovené jinými právními předpisy.
- Pod režim bezpečných přístavů nespadají aktivní služby, při kterých je zřejmé, že ISP obsah informací kontroluje

Koncepce: Safe harbour

- **Aktivní vs. pasivní služba**
- pro vyloučení odpovědnosti za obsah nesmí poskytovatel hrát aktivní roli takové povahy, že by bylo možné konstatovat, že uložená data zná či kontroluje
- C-324/09: optimalizaci prezentace nabídek k prodeji online nebo propagaci těchto nabídek
- C-236/08 až C-238/08: optimalizace pro vyhledávače naplňuje definiční znaky služby informační společnosti a podstatná pro určení odpovědnosti poskytovatele služby je analýza role, kterou poskytovatel systému placené optimalizace pro vyhledávače hraje při vypracování obchodního sdělení připojeného k reklamnímu odkazu nebo při stanovení či výběru klíčových slov.

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

- se vztahuje na **poskytovatele služeb informační společnosti** = každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti.
- **Službou informační společnosti** se rozumí jakákoliv služba
 - a) poskytovaná elektronickými prostředky;
 - b) na individuální žádost uživatele podanou elektronickými prostředky;
 - c) zpravidla za úplatu.

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

- **Tři typy subjektů:**

- **poskytovatelé připojení** (tzv. **mere conduit** neboli **prostý přenos**, či **access provider** - § 3 ZoNSIS, čl. 12 Směrnice), tedy poskytovatel služby, jež spočívá **v přenosu informací** poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo **ve zprostředkování přístupu** k sítím elektronických komunikací za účelem přenosu informací;
- **poskytovatelé služeb spočívajících v automatickém meziukládání informací** poskytnutých uživatelem (tzv. **caching** - § 4 ZoNSIS, čl. 13 Směrnice);
- **poskytovatelé služeb spočívající v ukládání (shromáždování) informací** poskytnutých uživatelem (tzv. **hosting** nebo **storage** - § 5 ZoNSIS, čl. 14 Směrnice).

Access provider

- Nejnižší míra odpovědnosti
- Ten může být odpovědný jen pokud
 - přenos sám iniciuje,
 - zvolí uživatele přenášené informace, nebo
 - zvolí nebo změní obsah přenášené informace.

Poskytovatel cachingu

- vyšší míra odpovědnosti
- může odpovídat za obsah informací, jestliže:
 - změní obsah informace,
 - nevyhoví podmínkám přístupu k informaci,
 - nedodrží pravidla o aktualizaci informace, která jsou obecně uznávána a používána v příslušném odvětví,
 - překročí povolené používání technologie obecně uznávané a používané v příslušném odvětví s cílem získat údaje o užívání informace, nebo
 - ihned nepřijme opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení či znemožnění přístupu k této informaci.

Host provider

- může být odpovědný za obsah uložených informací, jestliže
 - mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní,
 - se dozvěděl prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací, nebo
 - vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

Povinnost dohlížet na obsah

- Ani jeden z uvedených subjektů nemá **povinnost dohlížet na obsah jimi přenášených nebo ukládaných informací**, či aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace (§ 6).
- **Zákaz obecného dohledu však není podle judikatury SD EU překážkou tzv. speciálního (zvláštního) dohledu.** Česká úprava v § 6 jde patrně mimo rámec čl. 15 Směrnice, když nerozlišuje mezi dohledem obecným i zvláštním. C-484/14

Trestněprávní specifika

- Vyloučení odpovědnosti se tak týká i odpovědnosti trestní, a to bez ohledu na to, zdali jde o obecnou nebo zvláštní povinnost konat.
- Např. Access provider tak nemůže být při dodržení pravidel pro bezpečný přístav trestný ani za neoznámení či nepřekažení trestného činu. (což by patrně byl, kdyby nebylo této speciální právní úpravy)
- Pokud však ISP překročí pravidla pro zachování bezpečného přístavu, nemůže se dovolávat vyloučené odpovědnosti.
- musí být naplněny všechny znaky trestného činu včetně požadované formy zavinění.

Trestněprávní specifika

- Nulíček, M. **Nová evropská legislativa a její dopady na práva a povinnosti ISP.** *Právní rozhledy 9/2017, s. 317:* „I přes případnou ztrátu bezpečného přístavu nelze dovozovat trestní odpovědnost za spáchání trestného činu, neboť ISP nenaplňuje podmínky vzniku trestní odpovědnosti, a to i s ohledem na absenci úmyslu.“
- NESOUHLASÍM!

Trestněprávní specifika

- **subjekt (pachatel):** z hlediska právní formy často bude ISP právnickou osobou: zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob... (§§ 6, 7, 8);
- **jednání**, může mít činnost ISP podobu **konání**.
- méně častou bude situace, kdy je ISP sám pachatelem, např. pro to, že protiprávní obsah sám vytvořil.
- Častěji půjde o případy, kdy ISP sám protiprávní obsah nevytvořil, ale postupoval aktivně tak, že se podílel na jeho šíření, např. sám inicioval přenos (porušení pravidel vyloučené odpovědnosti u acces providera) nebo změnil obsah informace (porušení pravidel vyloučené odpovědnosti u cachingu) nebo vykonával rozhodující vliv na činnosti uživatele (porušení pravidel vyloučené odpovědnosti u host providera).

Trestněprávní specifika

- Jelikož zákon v některých případech ukládá ISP povinnost konat (týká se jen cachingu a host providera), pak může z jednání ISP spočívat i v **opomenutí** povinnosti konat ve smyslu § 112 TZ.
- § 112: Jednáním se rozumí i opomenutí takového konání, k němuž byl pachatel povinen podle jiného právního předpisu, úředního rozhodnutí nebo smlouvy, v důsledku dobrovolného převzetí povinnosti konat nebo vyplývala-li taková jeho zvláštní povinnost z jeho předchozího ohrožujícího jednání anebo k němuž byl z jiného důvodu podle okolností a svých poměrů povinen.
- Poskytovatele cachingu: povinnost ihned přijmout opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní. Host provider: povinnost neprodleně učinit veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
- Jestliže některý z těchto subjektů **opomene konat, odpovídá za následek způsobený tímto opomenutím v závislosti na svém zavinění.**

Notice and take down

- dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
- Dozvědět se od koho a jak? Ústně, písemně, anonymně - dostatečně určitá informaci, aby protiprávní obsah bylo možné identifikovat (neurčitost by vyžadovala zapovězený obecný dohled)
- Protiprávní povaha? (jak ji posoudit?) – znalost trestních norem = ignorantia iuris nocet; znalost skutkových okolností závisí na vědomí ISP:
 - výrok uživatele v diskusním fóru může být sám o sobě dostatečně způsobilý, aby umožňoval ISP jej kvalifikovat jako protiprávní,
 - Jindy k takovému závěru bude potřebovat informací více, např. u trestného činu pomluvy podle § 184 TZ nemusí nutně ISP vědět, že sdělená informace je nepravdivá.

Příklad

- Uživatel umístí na webový server soubor obsahující dětskou pornografii (§ 192 odst. 3 – výroba a jiné nakládání s dětskou pornografií). Jiný uživatel upozorní host providera na tento soubor. Host provider je schopen bez obtíží seznat, že se skutečně o dětskou pornografii jedná, zůstane však nečinný, aniž by mu v odstranění souboru bránila jakákoliv překážka technického charakteru. Jelikož host provider se prokazatelně dozvěděl o protiprávní povaze ukládaných informací, měl povinnost konat, tedy odstranit soubor s dětskou pornografií. Pokud tak neučinil, lze jeho opomenutí považovat za jednání, konkrétně, že činí veřejně přístupným počítačové (resp. filmové či elektronické) pornografické dílo. Tohoto jednání se host provider dopustil přes to, že se o souboru s dětskou pornografií dozvěděl a aniž by mu v tom bránili jakékoliv okolnosti, svou povinnost nesplnil. Jednal tedy v úmyslu toto dětské pornografické dílo (nadále) činit veřejně přístupným.

Odpovědnost za cizí obsah podporovatelem

- otázka tzv. odkazů (**hyperlink**) z vlastních interaktivních webových stránkách na webové stránky jiného s protiprávním obsahem
- Obdobně případ „laikování“.
- řešení toho problému je třeba hledat v obecných normách. Pečlivě je třeba zkoumat zavinění. **Je-li úmyslem pachatele tímto způsobem podporovat nebo šířit obsah závadných stránek**, přichází do úvahy jak některá z forem součinnosti, tak odpovědnost za pachatelství trestného činu. O pachatelství půjde tam, kde znaky skutkové podstaty trestného činu jsou formulovány tak, že zahrnují podporu nebo šíření takového obsahu (např. § 191, 192, 270, 305, 356, 403 až 405 TZ), či kořistění z trestného činu jiné osoby (např. § 189 odst. 1 al. 2 TZ).

Odpovědnost za cizí obsah konzumentem

- V případech, kdy trestní zákoník sankcionuje přístup k obsahu nebo jeho přechovávání, byť pro vlastní potřebu (obdobně jako u drog)
- § 191 odst. (1): Kdo **přechovává** fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.
- § 191 odst. (2) Stejně bude potrestán ten, kdo prostřednictvím informační nebo komunikační technologie **získá přístup k dětské pornografii**.



Děkuji za pozornost

 grivna@prf.cuni.cz