15. 1. 2019

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

Režim Safe Harbour v rámci poskytování hostingových služeb

Internet jako systém navzájem propojených počítačových sítí poskytuje komukoliv připojení k internetové síti, prostřednictvím které je každému umožněn přístup k informacím, přenos dat a taktéž poskytování služeb nejrůznějších úložišť. S rozvojem internetu nabývá na rozměru i poskytování služeb, které hojně využívá každý z nás. S tímto rozmachem, jakož i neomezeným přístupem k nim, vyvstává celá řada otázek a problémů, zejména pokud jde o přenos, stahování a ukládání dat, s čímž souvisí i nárůst porušování práv třetích osob.

Mezi nejčastěji porušovanými právy patří práva týkající se duševního vlastnictví, zejména práv autorských a práva s nimi související, přesto se práva třetích osob mohou dostat do kolize s jinými garantovanými právy jako např. svobodou soukromí, ochranou osobních údajů, svobodou informací a podnikání; přesto však platí legální licence, že každý občan může činit vše, co není zákonem zakázáno[1], a současně soukromoprávní zásada, že lidé mají jednat poctivě a v dobré víře.[2]

Nezbytnost právní úpravy odpovědnosti v rámci poskytování globálního média došlo k přijetí Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (dále jen ,,Směrnice“). Přijetím směrnice byla provedena transpozice do zákona č. 480/2004 Sb., o některých službách informačních společnosti a o změně některých zákonů, ve znění pozdějších předpisů (dále jen ,,ZSIS“), který upravuje mj. práva a povinnosti poskytovatelů služeb informační služby známé též jako Internet Service Providers (dále jen ,,ISP“).

Podle § 2 písm. a) ZSIS je za službu považována jakákoliv služba, která je poskytována elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat, podle písm. d) cit. ustanovení se poskytovatelem služby rozumí každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti a podle písm. e) se uživatelem rozumí každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupnění.

Hostingové služby spočívají v poskytování platformy pro vkládání informací/obsahu na cloudové úložiště, různá diskusní fóra, osobní blogy nebo například sociální sítě, přičemž tyto služby se mohou lišit podle toho, zda podporují pouze některý formát obsahu, jako je tomu např. u YouTube, který umožňuje pouze nahrávání obrazově-zvukových záznamů, nebo zda podporují pouze obrazové záznamy, jako je tomu u sociální sítě Instagram atp.

Vyloučení odpovědnosti ISP dle článku 14 Směrnice

Podle článku 14 Směrnice odpovědnost poskytovatele je vyloučena, pokud (i) poskytovatel nebyl účinně seznámen s protiprávní činností nebo informací a ani s ohledem na nárok na náhradu škody si není vědom skutečností nebo okolností, z nichž by byla zjevná protiprávní činnost nebo informace,

nebo (ii) jakmile se poskytovatel o protiprávní činnosti nebo informaci dozvěděl, jednal s cílem je odstranit nebo znemožnit k nim přístup.

Naproti tomu ustanovení § 5 ZSIS nešťastně stanoví, že poskytovatel hostingových služeb odpovídá za obsah informací uložených, (i) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele je protiprávní, nebo (ii) 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 (tzv. mechanismus notice and take down).

Z výše uvedeného vyplývá, že legislativní znění ustanovení § 5 ZSIS neodpovídá smyslu a záměru článku 14 Směrnice. Zmiňovaného ustanovení § 5 ZSIS nevylučuje odpovědnost IPS, ale naopak ji zakládá, kdy ke vzniku odpovědnosti poskytovatele služby se nevyžaduje subjektivní vědomí, ale již pouhá možnost nabytí vědomosti o protiprávnosti obsahu uložených informací, což z pohledu pasivního, resp. neutrálního, poskytovatele je nepřiměřeně tvrdé. S ohledem na tento věcný nesoulad mezi oběma předpisy, musí být ZSIS vykládán eurokonformním výkladem, tj. že dané ustanovení § 5 odpovědnost poskytovatele vylučuje, nikoliv zakládá. Pro zvláštní režim vyloučení odpovědnosti se ustálil termín Safe Harbour (*bezpečný přístav*). Jsou-li dodržena pravidla bezpečného přístavu, nevzniká odpovědnost poskytovateli informačních služeb za obsah či jednání uživatele, avšak dozvěděl-li se poskytovatel služby o protiprávní povaze obsahu služby a neučinil neprodleně náležité kroky, ať již znepřístupněním či smazáním obsahu, pak poskytovatel služeb ztrácí tento režim a stává se právně odpovědným za obsah nahraný uživatelem. Elementární myšlenkou tohoto režimu je zachování pasivní role poskytovatele služby do uživatelského obsahu. Na režim Safe Harbour navazuje ustanovení § 6 ZSIS, podle něhož poskytovatelé nejsou povinni dohlížet na obsah jimi přenášených nebo ukládaných informací, nebo aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace. S touto otázkou souvisí i problematika filtrování informací, kdy se v takovém případě může IPS dostat do konfliktu se základními právy a svobodami. K uvedenému se vyjádřil i SDEU, kdy došel k závěru, že je v rozporu s právem EU uložení povinnosti ISP spočívající ve filtrování informací ukládaných na jeho server uživateli, kdy by taková obecná povinnost dohledu ukládala povinnost aktivního dohledu na takřka veškerými údaji všech uživatelů jeho služeb za účelem předcházení jakémukoliv budoucímu porušování práv duševního vlastnictví a vedl by k závažnému zásahu do svobody podnikání poskytovatele hostingových služeb, kdy by se účinky takového příkazu nedotkly pouze IPS, ale mohlo by též dojít k porušení základních práv uživatelů služeb v podobě porušení práva na ochranu osobních údajů atp.[3]

Co lze spravedlivě požadovat od ISP?

V rámci připojení k internetu dochází k přenosu objemných dat, přičemž k takovému přenosu se děje bezmála každou sekundu. Představme si situaci v podobě často používaného kanálu YouTube od společnosti Google, Inc., v jehož rámci uživatelé během jedné minuty nahrají do této služby bezmála 400 hodin obsahu, což není nikterak málo. S rostoucím popularitou YouTube vznikl i fenomén tzv. youtuberů, influencerů, kteří kolem sebe budují jistou komunitu fanoušků, právě jejich činnost spočívá v nahrávání nejrůznějších služeb na tento kanál. Je-li během jedné minuty nahráno 400 hodin obsahu, pak jedna minuta provozu této služby přináší 24 000 minut obsahu, který by museli příslušní zaměstnanci zkontrolovat.[4] Je naprosto nepředstavitelné a reálně i nemožné průběžně sledovat a kontrolovat obsah přenášených informací, proto na základě Směrnice byly členské státy povinny zajistit a přijmout opatření, na základě kterých by byla, za splnění určitých pravidel, vyloučena odpovědnost poskytovatelů za uložený obsah jeho uživateli, neboť tento obsah je nahráván a dále využíván třetími osobami, tj. uživateli služby, kteří jsou seznalý s obsahem, a tudíž by měli za něj nést i odpovědnost.

V rámci volného pohybu zboží a služeb by vyloučení režimu Safe Harbour vedlo k omezení volné soutěže a tím tedy k narušení vnitřního trhu EU, a jako takové by vedlo k rapidnímu navýšení nákladů na zajištění dohledu nad obsahem nahrávaných souborů, což je jednak nereálné, neproveditelné a velmi tvrdé pro poskytovatele, s čímž souvisí další problém, a to garance základních práv a svobod např. ochrany osobních údajů, svobody podnikání a potažmo i cenzura sdělovaných informací, kdy by uvedeným postupem nebyla zajištěna spravedlivá rovnováha mezi právem duševního vlastnictví na straně jedné a svobodou podnikání, právem na informace atd., na straně druhé, proto se na poskytovatele vztahuje vznik odpovědnosti pouze v případě nabytí vědomosti o protiprávnosti informací uložených uživatelem a neučinění nezbytných kroků k odstranění závadného obsahu nebo jeho znepřístupnění. Poskytovatel může nabýt takové vědomosti na základě podnětu, stížnosti nebo za jiných okolností. K uvedenému lze zmínit rozsudek Městského soudu v Praze, v němž byl řešen případ týkající se diskusního příspěvku vloženého na server iDNES.cz třetí osobou, kdy v diskuzi k článku žalobce neodstranil, resp. neznepřístupnil, obsah ukládaných informací v příspěvku uživatele s přezdívkou ,,Albert 52“, na jehož základě bylo možné zjistit informace o matce poškozené umožňující zjištění totožnosti její dcery a o tom, že její dcera byla znásilněna, a to ve spojení s předmětným článkem obsahujícím další podrobnosti trestního řízení. Společnost MAFRA, a. s. jakožto žalobce, se hájil tím, že jako IPS nemá povinnost dohlížet na obsah informací, neboť žalobce nebyl osobou, která by sporný příspěvek na server vložila, pouze založil diskuzi, v níž bylo umožněno zveřejňování názorů jednotlivými uživateli, a proto nemůže být odpovědný za správní delikt dle § 45a odst. 1 a 3 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, přičemž Policie České republiky požádala poskytovatele (MAFRA, a. s.) o sdělení IP adresy vkladatele příspěvku s odůvodněním, že je v dané věci prováděno šetření dle trestního řádu, kdy i po téměř jednom roce byl předmětný příspěvek uživatele ,,Albert 52“ veřejnosti přístupný. K odstranění závadného příspěvku společností MAFRA, a. s. došlo až v době, kdy proti ní bylo zahájeno správní řízení pro porušení zákazu zveřejňování osobních údajů umožňující zjištění totožnosti nezletilé poškozené v trestním řízení. Městský soud v Praze dospěl k závěru, že dozvěděl-li se žalobce na základě žádosti a několika urgencích od policejních složek o tom, že v souvislosti s předmětným příspěvkem je prováděno šetření pro podezření ze spáchání trestného činu, tak se žalobce měl blíže zabývat obsahem předmětného příspěvku a nenechat ho bez povšimnutí, a to více jak jedenáct měsíců. Kdyby se býval žalobce blíže zabýval obsahem předmětného příspěvku, zjistil by, že příspěvek skutečně obsahuje závadné informace, a proto soud konstatoval, že žalobce začal odpovídat za protiprávní obsah příspěvku jeho uživatele od okamžiku zaslané žádosti policie žalobci, a na základě uvedeného soud shledal spáchání správního deliktu žalobcem.[5]

Aktivní versus pasivní poskytování hostingových služeb

Pasivním poskytovatelem hostingových služeb je ten, kdo poskytuje službu na základě pasivních technických prostředků, čímž nedochází z jeho strany k přímým a manuálním zásahům vůči obsahu, přičemž existence automatizovaných funkcí služeb například pomocí filtrování obsahu nebo vyhledávání v rámci služeb nezakládá aktivitu poskytovatele ve smyslu ustanovení § 5 ZSIS. Pro poskytovatele internetových služeb je proto zásadní udržet své služby v pasivním režimu, čímž tak nebude naplněna podmínka pro založení odpovědnosti za zpracování obsahu. Za předpokladu, že poskytovatel vystupuje natolik aktivně v rámci poskytování hostingových služeb, dochází ke ztrátě bezpečného přístavu. Rozlišení mezi aktivním a pasivním přístupem poskytovatele hostingových služeb je dost problematické a obtížné, přičemž je nezbytné tento přístup poskytovatele hodnotit vždy ve vztahu ke konkrétnímu obsahu. Soudní dvůr Evropské unie (dále jen ,,SDEU“) se ve svém rozsudku C-324/09 ze dne 12. 7. 2011 ve věci L´Oréal SA a další vs. eBay International AG zabýval otázkou pasivity v rámci poskytování hostingových služeb, v němž uvedl následující. Pro vyloučení odpovědnosti za obsah nesmí poskytovatel hrát aktivní roli takové povahy, že by bylo možné konstatovat, že uložená data zná nebo kontroluje. Za aktivní přístup nelze přesto považovat jakýkoliv zásah ze strany poskytovatele, kam například spadá řazení souborů podle velikosti nebo druhu

souboru. V rámci automatizovaného řazení přenášených informací nedochází k možnosti seznámení se s obsahem přenášených dat. Podstatou pro rozlišení, zda se jedná o aktivní nebo pasivní přístup je, že poskytované služby mohou fungovat bez aktivního zásahu, tj. bez manuálního zásahu, ze strany poskytovatele; z uvedeného tedy vyplývá, že se nejedná o formu aktivního přístupu poskytovatele služeb, pokuď obsah (soubory) jsou upravovány, resp. zpracovány, formou automatizovaného nástroje.

Závěr

Ze závěru SDEU vyplývá, že IPS pro udržení režimu bezpečného přístavu ve vztahu ke konkrétnímu obsahu nesmí hrát aktivní roli takové povahy, z něhož by bylo možné dojít k závěru, že uložený obsah informací zná či jej kontroluje, přičemž právě otázka aktivity ISP bude v konkrétním případě hrát důležitou roli, na základě které se bude individuálně posuzovat ten který případ, neboť pasivní, resp. neutrální, role poskytovatele je předpokladem pro uplatnění režimu Safe Harbour. Lze tedy uzavřít, že IPS není povinen daný obsah jakkoliv sledovat a kontrolovat, neboť takovým jednáním může dojít k zásahu do základních práv a svobod jak uživatele informační společnosti, tak třetí osoby, proto zastává-li ISP pasivní a neutrální roli v rámci poskytování služeb, pak nenese právní odpovědnost za případná porušení práv třetích osob ze strany uživatelů za předpokladu, že se nedozví o protiprávnosti obsahu ukládaných informací a neučiní za tímto účelem vhodná opatření.

Mgr. Anna Dufková,
asistentka Městského soudu v Praze

---

[1] čl. 2 odst. 4 ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů, a čl. 4 odst. 1 ústavního zákona č. 2/1993 Sb., Listina základních práv a svobod
[2] § 6 odst. 1 a § 7 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[3] rozsudek SDEU C-360/10 ve věci SABAM proti Netlog NV
[4] MAISNER, Martin. Filtrování ze strany ISP ve světle aktualit evropského práva [Systém ASPI]. Wolters Kluwer. ASPI ID LIT232467CZ. Dostupné v systému ASPI
[5] rozsudek Městského soudu v Praze ze dne 19. 8. 2015, č.j. 11 A 114/2013-39

Další články:

- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR
- DEAL MONITOR
- DEAL MONITOR

- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie