ODPOVĚDNOST POSKYTOVATELŮ HOSTINGOVÝCH SLUŽEB SE ZŘETELEM K POVAZE A DRUHU PŘENÁŠENÉHO OBSAHU

Ján Matejka* – Alžběta Krausová**

Abstrakt: *V současnosti probíhající proces globalizace je úzce propojen mimo jiné s rozvojem služeb informační společnosti, které představují jeden z významně se rozvíjejících ekonomických sektorů a hodnot v tržím prostředí. K rozvoji jednotlivých ekonomických sektorů totiž výraznou měrou přispívá i jasná a srozumitelná právní regulace, která zajišťuje předvídatelnost a jistotu v právních vztazích. Oblast služeb informační společnosti je regulována jak na evropské, tak i na národní úrovni, což nezřídka vede k tomu, že zásadní právní instituty jsou vykládány účelově a nezřídka i chybně, což v kontextu globálního prostředí služeb internetu bohužel mnohdy nevede ani k zahájení soudního řízení (a tedy ve své výsledné podobě ani k hledání argumentů), a to nejenom z důvodů jeho zdlouhavosti, ale především celkové absence právní jistoty a nepřehlednosti celého portfolia této ochrany. Cílem tohoto článku je tak provést podrobnou interpretaci těch ustanovení zákona o některých službách informační společnosti upravujících tzv. globálně poskytované služby, tj. zejména služby ukládání obsahu informací poskytovaných uživatelem (hosting). Při interpretaci příslušných ustanovení bude brán zřetel zejména na teritoriální, věcnou i osobní působnost příslušných národních právních předpisů, včetně evropských směrnic a relevantní judikatury, jakož i na některé publikované názory a stanoviska ústředních správních orgánů. Zároveň bude brán zvláštní zřetel na problematiku zpracovávání a uchovávání osobních údajů poskytovateli hostingu a vztah mezi zákonem o některých službách informační společnosti a ochranou osobních údajů.*

Klíčová slova: *právní odpovědnost, konstruktivní vědomost, skutečná vědomost, obecný zákaz monitoringu, vztah speciality, subsidiarity a generality, poskytovatel hostingu, GDPR, ochrana osobních údajů, biometrické údaje*

ÚVOD

V právní vědě existuje jen velmi málo tradičních právních institutů či vztahů, jejichž zkoumání lze obětovat doslova celý vědecký život. Takovým institutem je bezesporu právní odpovědnost, která tak mimo jiné představuje rovněž jeden z nejstarších právních institutů vůbec. Pokud se pokusíme stručně analyzovat vývoj odpovědnostněprávních vztahů, nepochybně dospějeme k závěru, že v historii existoval mnohdy velmi protikladný vývoj názorů na postavení a odpovědnost člověka ve společnosti, stejně tak jako na vztah jeho svobody a jeho povinností. Tyto, mnohdy spíše filosofické než právní, spory pak nejenom, že v mnoha ohledech trvají dodnes, ale především z hlediska kvalitativního nabývají na významu. Stejně tak, jak dochází k vývoji těchto názorů, utváří se i samotná právní úprava, která navíc ještě musí účinně reagovat na nové výzvy netriviálních vztahů práva a nových technologií, zejména pak internetu.

O odpovědnostních vztazích kolem nových informačních technologií toho bylo napsáno relativně mnoho.[1] Řada klíčových otázek však zůstává stále neřešena, případně se

* JUDr. Ján Matejka, Ph.D., Ústav státu a práva AV ČR, v. v. i. E-mail: matejka@ilaw.cas.cz.

** Mgr. Alžběta Krausová, LL.M., Ústav státu a práva AV ČR, v. v. i. E-mail: krausova@ilaw.cas.cz. Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-26910S s názvem *Biometrické údaje a jejich zvláštní právní ochrana (Biometric Data and Their Specific Legal Protection)*.

[1] Viz např. POLČÁK, R. *Internet a proměny práva.* Praha: Auditorium, 2012, případně POLČÁK, R. – ČERMÁK, J. –

jejich řešení nachází stále ve fázi jejich identifikace, případně optimalizace adekvátního regulačního nástroje odpovídajícího zjištěným empirickým, systémovým, kontextovým a hodnotovým argumentům odůvodňujícím jeho potřebnost jako svého druhu důsledku jejich vzájemnému poměřování. Hledání takových řešení je v lepším případě na dobré cestě, v horším pak v nedohlednu, k čemuž často přispívá i nepochopení podstaty samotných technologií a souvisejících služeb ze strany jejich regulátorů, kteří nezřídka přicházejí se zavádějícími výklady či postupy. Právní praxe tak mnohdy používá nedokonalé normativní či interpretační konstrukce, v důsledku čehož platí více než jinde, že mezi realitou, tedy tím, co je v prostředí těchto služeb skutečně realizováno, a normativitou, tedy tím, co má být (lhostejno, zda z vůle regulátora či jiné), není shoda. Realita služeb informační společnosti a jeho normativní regulace jsou tak nezřídka vnímány jako dvě relativně samostatné kategorie. Jednou z takových diskutovaných otázek ohledně služeb informační společnosti je problematika právní odpovědnosti v souvislosti s poskytováním prostoru na internetu (odpovědnosti za hostingové služby[2]), kde tato teze platí více než kde jinde. Smyslem tohoto článku je tak nastínit možné způsoby řešení, návrhy *de lege ferenda* a upozornit na některá sporná výkladová stanoviska regulátora v této oblasti, jakož i vyjasnit některá interpretačně nejednoznačná či aplikačně sporná místa stávající právní úpravy.

1. NORMATIVNÍ REGULACE, JEJÍ KONCEPCE A VÝCHODISKA

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů (dále jen „ZSIS“) je zákon, který do českého práva implementuje ustanovení několika evropských směrnic. Jedná se zejména o Směrnici o soukromí a elektronických komunikacích[3] a o Směrnici o elektronickém obchodu.[4] Tento zákon tedy musí být interpretován jak v souladu s těmito směrnicemi,[5] tak i v souladu s ústavními zákony. Obsahově kolidující či navazující právní předpisy stejné právní síly, jako je ZSIS, včetně např. občanského zákoníku[6] nebo trestního zákoníku,[7] je tak nutno v případě souběhu

LOEBL, Z. – GŘIVNA, T. – MATEJKA, J. – PETR, M. *Cyber Law in the Czech Republic*. 2. vydání. Alpen aan den Rijn: Kluwer Law International, 2012.

2 V tomto směru jde tedy zejména o následující: poskytovatel volného prostoru (tzv. *hosting provider*) umožňuje třetím osobám – poskytovateli obsahu (tzv. *content provider*) umístit na svém serveru webové stránky, případně jiná data.

3 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

4 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 (směrnice o elektronickém obchodu).

5 Povinnost eurokonformního výkladu je blíže specifikována např. v rozsudku Soudního dvora EU ze dne 4. července 2006 ve věci C-212/04 v řízení *Konstantinos Adeneler a další proti Ellinikos Organismos Galaktos (ELOG)*. V čl. 108–111 Soudní dvůr uvádí povinnost vnitrostátních soudů přihlížet při výkladu práva k obsahu směrnice a při současném respektování obecných právních zásad (zejména zásady právní jistoty a zásady zákazu zpětné účinnosti) a zákazu výkladu vnitrostátního práva *contra legem* použít takové výkladové metody, aby zajistily plnou účinnost a soulad s cílem dotčené směrnice. Takový výklad tedy může být učiněn i *contra verba legis*.

6 Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

7 Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

regulace nebo aplikačního sporu o to, která z norem se má na konkrétní případ použít, interpretovat za použití tzv. kolizních pravidel.[8]

ZSIS se v § 3–6 věnuje odpovědnosti poskytovatelů zprostředkovatelských služeb v rámci informační společnosti. Tyto zprostředkovatelské služby dělí do tří kategorií podle jejich typu a stanoví pro ně odlišná pravidla. Jedná se o služby spočívající v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací (§ 3), dále o služby spočívající v přenosu informací poskytnutých uživatelem, kdy zároveň dochází k automatickému dočasnému ukládání informací (§ 4), a nakonec o služby spočívající v ukládání informací poskytnutých uživatelem, tj. o hostingové služby (§ 5). Právě toto poslední zmíněné ustanovení bude předmětem jak systémové, tak i obsahové právní analýzy. Text ustanovení zní v platném znění následovně:[9]

„§ 5
Odpovědnost poskytovatele služby za ukládání obsahu informací poskytovaných uživatelem

(1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen
   a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
   b) 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.

(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.“

V české odborné literatuře se nezřídka vyskytují spory o postavení a významu § 5 ZSIS ve vztahu k obecnému institutu odpovědnosti zakotvenému v různých právních předpisech stejné právní síly. Prvním sporem je otázka, zda § 5 ZSIS zakládá speciální typ odpovědnosti, nebo je naopak nástrojem k vyloučení odpovědnosti, která by poskytovateli služby ukládání obsahu informací poskytovaných uživatelem mohla vzniknout podle jiných předpisů. Důvodem vzniku tohoto sporu je patrně ne příliš zdařilý překlad směrnice o elektronickém obchodu[10] a text důvodové zprávy k ZSIS nesoucí se v podobném duchu,[11] které mohou při povrchní interpretaci naznačovat založení speciální odpovědnosti. Toto pochybení v interpretaci se promítlo i v jediném dostupném českém

[8] Kolizní pravidla se aplikují v následujícím pořadí: 1. *lex superior derogat lex inferiori* (přednost pravidla s vyšší právní silou), 2. *lex specialis derogat lex generali* (přednost zvláštní právní úpravy před obecnou právní úpravou), 3. *lex posterior derogat lex priori* (přednost později účinného právního předpisu před předpisem s dřívější účinností). K tomu více viz např. KNAPP, V. *Teorie práva*. Praha: C. H. Beck, 1995, s. 156–157.

[9] Zákonné ustanovení je uvedeno v platném znění ke dni 8. 6. 2017.

[10] Viz POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 149: *„Český právotvůrce však poněkud neobratně přeložil směrnici tak, že z výsledné dikce zákona není úplně jednoznačné, že smyslem zákona je ve skutečnosti omezit odpovědnost ISP. Jednoduché čtení předpisu totiž může na první pohled vyvolat dojem, že zákon tuto odpovědnost naopak zakládá.“*

[11] Viz Důvodová zpráva k zákonu č. 480/2004 Sb., o některých službách informační povinnosti, kde se v odůvodnění k § 5 a 6 uvádí: *„stává se odpovědným za obsah uložených informací“*.

judikátu zabývajícím se aplikací § 5 ZSIS, v němž Vrchní soud v Praze rozhodl,[12] že *„je dána odpovědnost žalovaného podle § 5 odst. 1 písm. b) zákona“*. Uvedený výklad, spočívající v názoru, že § 5 ZSIS zakládá speciální typ odpovědnosti, je však nepřípustný. Odporuje totiž samotnému smyslu směrnice o elektronickém obchodu, jejímž účelem je při splnění určitých podmínek vyloučit odpovědnost vznikající podle vnitrostátních právních předpisů.[13] Ustanovení § 5 ZSIS je tedy nutno primárně interpretovat tak, že jde o nástroj k vyloučení odpovědnosti, která by jinak mohla vzniknout podle obecných předpisů.[14] Tento názor vyjadřuje rovněž odborná literatura.[15] Vyloučení odpovědnosti je v tomto smyslu nazýváno „bezpečným přístavem“ (*safe harbor*). Po dobu „kotvení v tomto přístavu“, tj. za splnění podmínek pro vyloučení odpovědnosti, tak nelze na příslušného poskytovatele hostingových služeb uplatnit normy zakládající odpovědnost. Teprve po „vyplutí z tohoto bezpečného přístavu“, tj. v situaci, kdy poskytovatel přestane splňovat podmínky vyloučení odpovědnosti zakotvené v § 5 ZSIS, lze zkoumat, zda byly naplněny znaky vnitrostátní právní úpravy týkající se některého typu odpovědnosti.[16] Pro úplnost je třeba dodat, že v momentě, kdy poskytovatel přestane naplňovat podmínky bezpečného přístavu definované v § 5 ZSIS, nestává se automaticky odpovědným za obsah informací uložených u něj uživatelem. Jenom na základě toho, že obecně přestává být vyloučena odpovědnost, nelze bez dalšího stanovit, který typ odpovědnosti by měl vzniknout. To lze posoudit jen s ohledem na individuální okolnosti případu. Bez individuálního posouzení případu navíc nelze konstruovat odpovědnost, která by jinak například kvůli absenci protiprávnosti nevznikla.

Druhým sporem, který lze identifikovat v literatuře, je vztah mezi ZSIS a základním kodexem soukromého práva, občanským zákoníkem. V článku z roku 2015 byl vyjádřen názor,[17] že ZSIS nevylučuje povinnost prevence dle § 2900 a násl. občanského zákoníku

---

[12] Viz Rozsudek Vrchního soudu 3 Cmo 197/2010 – 82 ze dne 2. 3. 2011, s. 9.

[13] Viz 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 (směrnice o elektronickém obchodu), čl. 14 odst. 1, který stanoví: *„n e b y l poskytovatel služby o d p o v ě d n ý za informace ukládané na žádost příjemce“*, dále recitál 45 (*„omezení odpovědnosti zprostředkujících poskytovatelů služeb“*) a recitál 46 (*„Aby mohl poskytovatel služby informační společnosti spočívající v ukládání informací využívat omezení odpovědnosti, musí…“*), nebo Rozsudek Soudního dvora EU ze dne 23. března 2010 ve spojených věcech C-236/08 až C-238/08 v řízeních *Google France SARL a Google Inc. proti Louis Vuitton Malletier SA (C-236/08), Google France SARL proti Viaticum SA a Luteciel SARL (C-237/08)* a *Google France SARL proti Centre national de recherche en relations humaines (CNRRH) SARL a další (C-238/08)*, bod 109 *(„Omezení odpovědnosti uvedené v čl. 14 odst. 1 směrnice 2000/31“)*.

[14] Např. by mohlo jít o účastenství na trestném činu podle trestního zákoníku.

[15] Viz např. POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012 nebo HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 93: *„Inštitút vylúčenia zodpovednosti ale nemá zakladať zodpovednosť. Jeho cieľom je iba určiť celoplošne moment dokedy zodpovednosť za škodu a iné majetkové nároky nevznikne, resp. ju nemožno uplatniť. Ak sa inštitút vylúčenia zodpovednosti neaplikuje, znamená to len, že sa zodpovednosť poskytovateľa má posúdiť na základe princípov, ktoré sme uviedli vyššie (podľa vnútroštátneho práva).“* Viz také MAISNER, M. *Zákon o některých službách informační společnosti. Komentář*. Praha: C. H. Beck, 2016, s. 62: *„Logika zákonného řešení spočívá ve vytvoření zákonné výjimky z jinak stanovených pravidel odpovědnosti, která by mohla na straně ISP v souvislosti s provozem předmětné služby vzniknout.“*

[16] Buď jde o soukromoprávní odpovědnost, správněprávní odpovědnost nebo trestněprávní odpovědnost.

[17] Viz TELEC, I. Zakázané těžení a nebezpečná situace na elektronických úložištích dat. In: *Bulletin advokacie* [online]. 6. 3. 2015 [cit. 2016-04-07]. Dostupné z: <http://www.bulletin-advokacie.cz/zakazane-tezeni-a-nebezpecna-situace-na-elektronickych-ulozistich-dat>.

ani nároky z bezdůvodného obohacení podle § 2991 a násl. občanského zákoníku. Argumentuje přitom odkazem na čl. 14 odst. 3 směrnice o elektronickém obchodu, z nějž by podle něj měla vyplývat možnost členského státu aplikovat obecné vnitrostátní předpisy. Čl. 14 odst. 3 směrnice však zní následovně:

> *„Tímto článkem není dotčena možnost soudního nebo správního orgánu požadovat od poskytovatele služby v souladu s právním řádem členských států, aby ukončil protiprávní jednání nebo mu předešel, ani možnost členských států zavést postupy, které umožní odstranění nebo znemožní přístup k informaci.“*

Zmíněné ustanovení se tedy netýká možnosti aplikovat souběžně s vyloučením odpovědnosti poskytovatele za ukládání obsahu poskytnutého uživatelem jiná ustanovení, která tuto odpovědnost zakládají, a dát jim přednost. Směrnice pouze ponechává prostor pro oprávněný zásah v konkrétním případě, kdy takovýto zásah bude odůvodněný a kdy tento zásah nařídí soud nebo dotčený správní orgán v souladu s vnitrostátním právem.[18] Předmětný názor, respektive výklad, který dále mimo jiné dovozuje obecnou prevenční povinnost poskytovatelů hostingu, by tak znamenal nenaplnění účelu evropské směrnice a významné (úplné) popření smyslu § 5 a 6 ZSIS. Pro tyto a jiné nedostatky byl uvedený názor kritizován.[19]

Vztah ZSIS musí být ve smyslu svých speciálních pravidel i věcné působnosti ve vztahu k občanskému zákoníku, trestnímu zákoníku a dalším relevantním zákonům chápán jako zvláštní právní úprava, protože se vztahuje jen na omezené množství právních vztahů vznikajících pouze v určité oblasti. Podle pravidla *lex specialis derogat lex generalis* je nutné § 5 a 6 ZSIS uplatnit přednostně před obecnými zákonnými pravidly. V obdobném duchu se vyjadřuje i odborná literatura.[20] Vyjasnění výše uvedených sporných otázek za pomocí těchto ustálených interpretačních postupů tak leží především v důkladné analýze povahy a definiční podstaty těchto poskytovatelů, jakož i konkrétních podmínek vyloučení odpovědnosti ve světle jejich (preventivní) odpovědnosti a v mnoha ohledech kontravalentního vztahu speciality a subsidiarity souvisejících právních předpisů.

2. PROBLÉM DEFINICE POSKYTOVATELE HOSTINGOVÉ SLUŽBY

Definice poskytovatele služeb informační společnosti a samotné služby informační společnosti, kterých užívá § 5 ZSIS ve vztahu k informacím poskytovaným uživatelem jsou uvedeny přímo v ZSIS, a to konkrétně v ustanovení § 2 písm. d) ZSIS, podle kterého:

> *„poskytovatelem služby [je] každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti“*.

---

[18] Viz např. HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 95.

[19] Viz MAISNER, M. Snaha o zakázané těžení ze zdánlivé absence výslovné legislativní úpravy a nebezpečná situace pro poskytovatele služeb informační společnosti. In: *Bulletin advokacie* [online]. 24. 9. 2015 [cit. 2016-04-07]. Dostupné z: <http://www.bulletin-advokacie.cz/snaha-o-zakazane-tezeni-ze-zdanlive-absence-vyslovne-legislativni-upravy>.

[20] Viz HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 95: *„Vylúčenie zodpovednosti podľa článkov 12 až 14 SEO, § 6 ZEO a § 3 až 5 ZSIS sa dotýka všetkých typov zodpovednosti, t. j. civilnoprávnej, administratívnoprávnej ako aj trestnoprávnej.“* Viz také JANSA, L. a kol. *Internetové právo*. Brno: Computer Press, 2016, s. 158, případně MATEJKA, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013.

Definici služby informační společnosti pak poskytuje § 2 písm. a) ZSIS:

> *„službou informační společnosti [je] jakákoliv služba poskytovaná 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“*.

Uvedená definice služby informační společnosti musí být interpretována ve světle práva EU, zejména s ohledem na čl. 2 písm. a) směrnice o elektronickém obchodu,[21] který pro úplnou definici odkazuje na čl. 1 odst. 2 směrnice 98/34/ES[22] ve znění směrnice 98/48/ES.[23] Konsolidované znění směrnice 98/34/ES zahrnující i další její úpravy[24] pak službu informační společnosti definuje v čl. 1 odst. 1 písm. b) a zároveň v příloze I. uvádí příklady služeb, které dané definici neodpovídají. Ve zkratce uvádíme pouze hlavní definiční znaky služby informační společnosti. Jedná se o každou službu, která je poskytovaná *„zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.“*[25]

V definici dle ZSIS chybí znak „na dálku“, kterým se rozumí služba poskytovaná bez současné přítomnosti stran. Podle čl. 1 přílohy I směrnice 2015/1535 nejde o *„služby poskytované za současné přítomnosti poskytovatele a příjemce, a to i tehdy, použije-li se přitom elektronické zařízení“*. S ohledem na nutnost eurokonformního výkladu národního práva[26] je tedy tento požadavek nutno aplikovat i na českou právní úpravu, která ohledně požadavku „na dálku“ mlčí. Pokud by ZSIS nebyl interpretován ve světle směrnice 2015/1535, pak by např. vyloučení odpovědnosti dle § 5 odst. 1 ZSIS zahrnovalo i případy, kdy uživatel využije službu uložení určitého souboru na úložiště poskytovatele přímo v obchodních prostorách poskytovatele hostingové služby za přítomnosti zaměstnance poskytovatele, aniž by však tento zaměstnanec nabyl vědomost o protiprávnosti ukládaného souboru. To by však odporovalo samotnému smyslu § 5 ZSIS, jak bude ostatně podrobněji rozvedeno níže. Přestože je v literatuře vyloučení elektronických služeb využívaných při současné přítomnosti poskytovatele a uživatele kritizováno,[27] v určitých případech má své opodstatnění a je nutno jej akceptovat.

---

[21] 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 (směrnice o elektronickém obchodu).

[22] Směrnice Evropského Parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů.

[23] Směrnice Evropského parlamentu a Rady 98/48/ES ze dne 20. července 1998, kterou se mění směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů.

[24] Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (kodifikované znění).

[25] K výkladu těchto požadavků viz např. POLČÁK, R. *Internet a proměny práva*, s. 140–144.

[26] Požadavek eurokonformního výkladu národního práva se pojí s požadavkem dosažení účelu evropské směrnice v národním právu. Soudní dvůr EU dovodil tuto povinnost ve svém rozsudku ze dne 10. dubna 1984 ve věci C-14/83 v řízení *Von Colson a Kamann proti Land Nordrhein-Westfalen*. Blíže k eurokonformnímu výkladu viz např. MAISNER, M. Snaha o zakázané těžení ze zdánlivé absence výslovné legislativní úpravy a nebezpečná situace pro poskytovatele služeb informační společnosti. In: *Bulletin advokacie* [online]. 24. 9. 2015 [cit. 2016-04-07]. Dostupné z: <http://www.bulletin-advokacie.cz/snaha-o-zakazane-tezeni-ze-zdanlive-absence-vyslovne-legislativni-upravy>.

[27] Viz např. HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 99–100.

Definice poskytovatelů služeb informační společnosti podle § 5 ZSIS zužuje typ služby informační společnosti, kterou svým uživatelům nabízejí. Jedná se o službu spočívající *„v ukládání informací poskytnutých uživatelem"*. Odborná literatura nazývá tuto službu zkráceně termínem *„hosting"*. Hostingem se pak v tomto smyslu chápe široké množství služeb. Odborná literatura uvádí následující příklady, přičemž výčet není považován za vyčerpávající:[28]

> *„služby webhostingu, služby pro soukromé ukládání dat v cloudu (Google Drive, DropBox atp.), služby pro úschovu a předávání dat (Uschovna.cz), služby pro úschovu a veřejné sdílení dat, zpravidla spojené s vyhledáváním (Ulozto.cz, Megaupload), provoz platforem pro ukládání a zpřístupňování videa (YouTube), provoz platforem pro provoz blogů (bloguj.cz), provoz diskuzních serverů a diskuzních fór (mageo.cz, twitter), internetové tržiště a aukce (eBay, Aukro), sociální sítě (Facebook, Google +, LinkedIn), […] komentáře a diskuze pod články (ve vztahu k těmto komentářům a diskuzím), poskytování inzerce pomocí klíčového slova, která zadává uživatel služby (ve vztahu k těmto klíčovým slovům), např. Google AdWords, Sklik, uživatelské recenze výrobků či jiných produktů v e-shopech (ve vztahu k těmto recenzím) a řada dalších, provozovatelé webmailových služeb (ve vztahu k obsahu e-mailů uložených v rámci webmailového serveru)."*

Definice poskytovatelů hostingových služeb je následně zpřesněna ještě judikaturou Soudního dvora EU[29] odkazující na směrnici o elektronickém obchodu a zejména její recitál č. 42.[30] Odborná literatura tak v této souvislosti rozlišuje dva typy služeb – pasivní služby a aktivní služby.[31] Pasivní hostingové služby jsou ty služby, které splňují právě uvedenou podmínku z recitálu č. 42 směrnice o elektronickém obchodu (tj. čistě technická, automatická a pasivní podoba). Na tyto služby se vztahuje vyloučení odpovědnosti podle § 5 ZSIS. Aktivní služby, které jdou nad rámec pasivity, nepožívají ochrany dle § 5 ZSIS. Hranice mezi pasivními a aktivními hostingovými službami může být přitom velmi nezřetelná a měla by být posuzována individuálně. Kritériem pro určení toho, zda se v konkrétním případě tedy jedná o aktivní hosting, by měla být kladná odpověď na otázku, zda poskytovatel hostingové služby zná nebo kontroluje předmětné informace.[32]

Vyloučení odpovědnosti ve vztahu k aktivním službám bylo řešeno v případu *L'Oréal SA* (C-324/09).[33] Soud právě zde v bodě 123 stanovil, že pro zachování vyloučení odpovědnosti je nutné, aby poskytovatel *„nehrál aktivní roli takové povahy, že by bylo možné*

---

[28] Viz JANSA, L. a kol. *Internetové právo,* s. 163.

[29] Viz např. čl. 113 rozsudku Soudního dvora EU ze dne 12. července 2011 ve věci C-324/09 v řízení *L'Oréal SA a další proti eBay International AG a další* nebo čl. 113 a 119 rozsudku Soudního dvora EU ze dne 23. března 2010 ve spojených věcech C-236/08 až C-238/08 v řízeních *Google France SARL a Google Inc. proti Louis Vuitton Malletier SA (C-236/08), Google France SARL proti Viaticum SA a Luteciel SARL (C-237/08)* a *Google France SARL proti Centre national de recherche en relations humaines (CNRRH) SARL a další (C-238/08).*

[30] Podle tohoto recitálu musí mít činnost poskytovatele hostingových služeb *„čistě technickou, automatickou a pasivní podobu, což znamená, že poskytovatel služeb informační společnosti nezná ani nekontroluje přenášené či ukládané informace."*

[31] Viz HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva,* s. 51.

[32] Viz MAISNER, M. Pasivní vs. Aktivní hosting: hranice režimu Safe Harbour. *Bulletin advokacie.* 2017, č. 1–2, s. 40 an.

[33] Rozsudek Soudního dvora EU ze dne 12. července 2011 ve věci C-324/09 v řízení *L'Oréal SA a další proti eBay International AG a další.*

konstatovat, že uložená data zná nebo kontroluje. Uvedený provozovatel hraje takovou roli v případě, že poskytuje pomoc, která spočívá zejména v optimalizaci prezentace dotčených nabídek k prodeji nebo jejich propagaci."V tomto směru je nutno poznamenat, že na optimalizaci prezentace nelze nahlížet paušálně, ale je třeba rozlišovat automatizovanou optimalizaci, při níž nedojde ke kontrole nebo nabytí znalosti o obsahu prezentace, a jinou optimalizaci.[34]

Mohlo by se zdát, že tímto přístupem zákonodárce podporuje pasivní přístup poskytovatelů k informacím, které ukládají, protože jejich odpovědnost vylučuje pouze v případech jejich neaktivity. Na druhou stranu je třeba si uvědomit, že původním účelem této právní úpravy je chránit poskytovatele, kteří zachovávají vůči obsahu neutralitu. Jak uvádí i důvodová zpráva k ZSIS, *„není rozumné požadovat od poskytovatelů, aby při vysokém počtu uživatelů a vysokém objemu uložených dat zjišťovali a posuzovali legálnost či nelegálnost veškerého obsahu uložených informací"*.[35] Na druhou stranu ale nelze vylučovat jejich odpovědnost v případech, kdy se neutrálně nechovají. V takovém případě by totiž právo umožnilo, aby o nelegálnosti obsahu poskytovatel věděl a nebyl postižitelný za jeho tolerování.

3. PŘEDPOKLADY VYLOUČENÍ ODPOVĚDNOSTI POSKYTOVATELE

Obecně lze identifikovat tři podmínky, při jejichž splnění není poskytovatel odpovědný. Konkrétně jde o:

a) podmínku absence pověření nebo kontroly (neexistence vlivu),
b) podmínku absence vědomosti,
c) podmínku pasivity a neutrality poskytovatele.[36]

Podmínky absence vědomosti a absence kontroly jsou detailně analyzovány v následujících kapitolách. Podmínka pasivity a neutrality poskytovatele se prolíná oběma níže analyzovanými podmínkami. Pro splnění této podmínky *„poskytovatel nesmí hrát aktivní roli takové povahy, že by bylo možné konstatovat, že uložená data zná či kontroluje"*,[37] to například na základě poskytování individuální pomoci uživateli. Za poskytování individuální pomoci však nelze považovat automatizované služby sloužící podpoře činností uživatelů včetně služeb, které fakticky zpracovávají uživateli nahraná data za podmínky, že jsou tyto služby obsahově indiferentní.[38]

3.1 Koncepce konstruktivní vědomosti

Konstruktivní vědomost je koncept definovaný jak směrnicí o elektronickém obchodu, tak i ZSIS. Jedná se o koncept paralelní ke skutečné vědomosti o protiprávní činnosti nabyté na základě konkrétního oznámení poskytovateli služby (viz níže). Absence kon-

[34] Příkladem takové optimalizace, při níž je zachován bezpečný přístav, je například služba kontroly pravopisu aj.
[35] Viz Důvodová zpráva k zákonu č. 480/2004 Sb., o některých službách informační povinnosti. Zvláštní část, odůvodnění k § 5 a 6.
[36] Viz HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 105–111, nebo JANSA, L. a kol., *Internetové právo*, s. 163–165.
[37] Viz MAISNER, M. *Zákon o některých službách informační společnosti. Komentář*, s. 77.
[38] Ibidem, s. 78–79.

struktivní vědomosti nezbytná pro vyloučení odpovědnosti poskytovatele je charakterizována směrnicí o elektronickém obchodu v čl. 14 odst. 1 písm. a) následovně:

> *„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."*

ZSIS stejnou podmínku ukládá v § 5 odst. 1 písm. a) následovně:

> *„Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní."*[39]

S ohledem na rozdílné znění obou dokumentů a s ohledem na obecné znění obou ustanovení se otevřel prostor pro různé druhy interpretací.

Nemalý zmatek, respektive silnou aplikační nejistotu do interpretace § 5 odst. 1 písm. a) ZSIS vneslo zejména výkladové stanovisko Ministerstva průmyslu a obchodu.[40] Toto výkladové stanovisko se zaměřuje na provozovatele datových úložišť a dovozuje, že jejich obchodní modely jsou primárně založeny na porušování autorských práv. Provozovatelé datových úložišť tedy nemohou využít vyloučení odpovědnosti podle § 5 odst. 1 písm. a) ZSIS, protože o protiprávnosti obsahu a činnosti uživatelů museli nutně vědět, jelikož ji sami podporují. Uvedené výkladové stanovisko trpí závažnými nedostatky – paušalizuje veškeré služby datových úložišť a dochází k závěrům, které nelze bez dalšího přijmout, je tedy nutno se vůči nim doktrinálně vymezit.

Hlavním zmíněným nedostatkem výkladového stanoviska je paušalizace služeb datových úložišť. Stanovisko popisuje obchodní model založený na atraktivnosti dostupných souborů, tudíž vysoké návštěvnosti a vyšších příjmech z umístěných reklam. Funkčnost modelu bez nelegálního obsahu považuje za krajně nepravděpodobnou. Přestože je všeobecně známo a uznáváno, že určitá míra nelegálního obsahu je v hostingových službách vždy přítomna, konstruuje toto stanovisko nejenom vědomost, ale i vůli provozovatelů datových úložišť napomáhat při porušování zákona. Nebere přitom v potaz následující základní faktory:

a) zákonné znění, které výslovně zmiňuje činnost jednoho uživatele, a nikoli *uživatelů*, a nepřímo tak signalizuje, že pro ztrátu bezpečného přístavu musí jít o vědomost o konkrétním případě, a nikoliv o obecné povědomí;
b) zvážení další činnosti provozovatele, která spočívá v prevenci nahrávání nelegálního obsahu, zavádění filtrovacích systémů, blokování uživatelů, kteří se provinili v minulosti apod.;
c) popularitu obsahu vytvářeného samotnými uživateli,[41] který tito uživatelé z vlastní vůle sdílejí na internetu a nijak tím neporušují autorské právo.

---

[39] V české právní úpravě jde o podmínku nevědomé nedbalosti, přičemž většina států EU používá podmínku vědomé nedbalosti. Viz POLČÁK, R. *Internet a proměny práva*, s. 149.

[40] Výkladové stanovisko odboru poštovních služeb a služeb informační společnosti Ministerstva průmyslu a obchodu ze dne 12. září 2012 k problematice odpovědnosti poskytovatelů služeb informační společnosti, kteří pasivně hostí nebo „přenášejí" obsah, podle § 3 až 6 zákona č. 480/2004 Sb., o některých službách informační společnosti. In: *Ministerstvo průmyslu a obchodu* [online]. 12. 9. 2012 [cit. 2016-04-07]. Dostupné z: <http://download.mpo.cz/get/46881/52910/592313/priloha001.pdf>.

Paušalizaci zániku vyloučení odpovědnosti ve vztahu k obchodnímu modelu datového úložiště odmítl i německý soud v případu GEMA v. Rapidshare.[42] Soud zde judikoval, *„že samotný obchodní model nezakládá plnou odpovědnost za porušení autorských práv"*.[43] Odpovědnost provozovatele datového úložiště závisí na tom, *„jestli přijal rozumná opatření k zabránění zásahu do autorských práv v momentě, kdy se o něm prokazatelně dozvěděl"*.[44]

Stanovisko dochází k závěru, že *„je-li si poskytovatel služby informační povinnosti,*[45] *jež spočívá v ukládání informací poskytnutých uživateli, vědom, že výše jeho příjmů nebo výnosů přímo souvisí s mírou protiprávního obsahu ukládaných uživateli, nemůže se dovolávat toho, že neodpovídá za tento obsah podle § 5 zákona č. 480/2004 Sb."*[46] Jak už bylo zmíněno výše, v odůvodnění stanoviska se však bohužel tato vědomost rovnou předpokládá, a to s ohledem na další předpoklad, podle nějž vyšší míra nelegálního obsahu na datovém úložišti znamená automaticky vyšší příjmy provozovatele datového úložiště,[47] a to bez ohledu na to, zda provozovatel účtuje vyšší sazby za stahování nelegálního obsahu nebo ne.[48] V této souvislosti je ale nutno se ptát, zda vůbec existuje nějaké datové úložiště, v němž výše příjmů nezávisí na povaze ukládaných informací. Pokud totiž žádné datové úložiště není imunní vůči fluktuaci příjmů v závislosti na povaze ukládaných informací, pak se podle tohoto výkladového stanoviska nemůže dovolávat vyloučení

---

41 Podle odborné literatury je množství tzv. *„user-generated content (UGC)"*, respektive *„user-created content (UCC)"* mnohem vyšší v porovnání s autorskými díly profesionálních subjektů: *„IMDb, největší online databáze filmů, obsahuje 963.309 filmů a televizních epizod vyprodukovaných od roku 1888 až do současnosti. Naproti tomu je na YouTube denně nahráno 65.000 nových příspěvků – což znamená, že YouTube trvá jen patnáct dní k tomu vyprodukovat stejný počet videí jako je v IMDb."* Viz CHA, M. – KWAK, H. – RODRIGUEZ, P. a kol. I tube, you tube, everybody tubes: analyzing the world's largest user generated content video system. *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. 2007 [cit. 2016-04-07]. Dostupné z: <http://koasas.kaist.ac.kr/bitstream/10203/24804/1/mia_imc07_sumitted.pdf>.

42 Rozsudek Bundesgerichtshof ze dne 15. srpna 2013 č. j. I ZR 80/12 ve věci *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA) proti File-Hosting-Dienst www.rapidshare.com. Bundesgerichtshof in Namen des Volkes Urteil I ZR 80/12*. In: *Der Bundesgerichtshof* [online]. 15. 8. 2013 [cit. 2017-06-08]. Dostupné z: <http://juris.bundesgerichtshof.de/cgi–bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=5a5ed98dc0acd1d48cce75505ff02b66&nr=65241&pos=15&anz=20>.

43 Viz HARAŠTA, J. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem. *Právní rozhledy*. 2014, č. 17, s. 590 an.

44 Ibidem.

45 Zde je v originále stanoviska pravděpodobně překlep. Mělo by jít o službu informační společnosti, nikoliv o službu informační povinnosti.

46 Viz Výkladové stanovisko odboru poštovních služeb a služeb informační společnosti Ministerstva průmyslu a obchodu ze dne 12. září 2012 k problematice odpovědnosti poskytovatelů služeb informační společnosti, kteří pasivně hostí nebo „přenášejí" obsah, podle § 3 až 6 zákona č. 480/2004 Sb., o některých službách informační společnosti. In: *Ministerstvo průmyslu a obchodu* [online]. 12. 9. 2012 [cit. 2016-04-07]. Dostupné z: <http://download.mpo.cz/get/46881/52910/592313/priloha001.pdf>, s. 1.

47 Ibidem. Viz odůvodnění samotného stanoviska na s. 3–4: *„Přestože nelze vyloučit, že tento obchodní model by byl funkční i při neexistenci nelegálního obsahu na datovém úložišti, jeví se tato možnost v současných podmínkách jako krajně nepravděpodobná. Lze se totiž zcela logicky domnívat, že pokud by někdo byl vlastníkem tak atraktivního obsahu, pro který jsou uživatelé ochotni si zaplatit vyšší rychlost stahování, tak tento obsah neumístí zadarmo bez dalšího na určité datové úložiště a nezajistí tím příjem pro jinou osobu – provozovatele tohoto datového úložiště. Je více než pravděpodobné, že držitel práv k atraktivnímu obsahu by postupoval tak, aby měl příjem sám, nikoliv provozovatel datového úložiště."*

48 Pokud by provozovatel účtoval za stahování nelegálního obsahu vyšší sazby než za obsah neporušující právo, pak by bylo možné odkázat se dle okolností případu na vědomost provozovatele datového úložiště dle § 5 odst. 1 nebo § 5 odst. 2 ZSIS.

odpovědnosti žádný poskytovatel služeb hostingu. V případě, že by se mu totiž zvedly příjmy, pak by vždy musel předpokládat, že se tak děje jedině v souvislosti se zvýšením míry nelegálního obsahu na jím poskytovaném hostingovém prostoru a automaticky by přestal mít možnost využít výjimky z odpovědnosti dle § 5 ZSIS. Taková interpretace by ovšem popírala smysl a účel přijetí ZSIS. Právní názor tohoto výkladového stanoviska, včetně jeho argumentace, tak nelze přijmout a je nutno jej odmítnout.[49]

Po odmítnutí výkladového stanoviska Ministerstva průmyslu a obchodu zůstává otázkou, jak interpretovat situaci, kdy poskytovatel nabude konstruktivní vědomost dle § 5 odst. 1 písm. a) a ztratí titul pro vyloučení odpovědnosti.

Z normativní konstrukce zákona (§ 5 a násl.) a směrnice o elektronickém obchodu lze dovodit, že konstruktivní vědomost se musí týkat konkrétního jednání nebo konkrétní informace. Nelze tedy mluvit o obecném povědomí. Poskytovatel může tuto vědomost nabýt, zejména pokud provede přezkum z vlastního podnětu a odhalí tak protiprávní situaci nebo činnost.[50] V případě, že jsou poskytovateli protiprávní činnost nebo obsah oznámeny, avšak toto oznámení se ukáže jako nedostatečné, měl by na daný případ poskytovatel reagovat ve smyslu své obecné fiduciární odpovědnosti, respektive péče řádného hospodáře, včetně např. přiléhavého odkazu na principy loajality, potřebné znalosti a pečlivost ve smyslu ustanovení § 159 odst. 1 občanského zákoníku apod. Odborná literatura uvádí, že *„opomenutie tohoto šetrenia by mohlo viesť k založeniu konštruktívnej vedomosti“*.[51] Zároveň literatura zmiňuje nutnost vyhnout se úmyslné slepotě (*willful blindness*), *„t. j. situácii, kedy pred porušovaním práv na svojej službe vedome zatvára oči“*.[52]

Doktrína *„willful blindness“* má svůj původ v angloamerickém právu, avšak lze se jí inspirovat i v českém právu. Podle této doktríny je úmyslnou slepotou případ, kdy si je osoba vědoma vysoké pravděpodobnosti faktu, jež je předmětem sporu, a vědomě se vyhýbá potvrzení této skutečnosti.[53] Tuto doktrínu však omezuje zákaz požadovat po poskytovateli hostingu, aby aktivně monitoroval své uživatele.[54] V oblasti poskytování hostingu se tedy doktrína *„willful blindness“* aplikuje zejména v prevenční rovině ve vztahu k opakovanému porušování autorských práv stejnými osobami. V tomto případě je podle judikatury k udržení bezpečného přístavu a vyloučení odpovědnosti nutné, aby poskytovatel služby učinil vše, co od něj lze rozumně žádat, aby předešel použití své služby osobami, které opakovaně porušují autorské právo.[55] Konkrétní příklady takových opatření však uvedeny nejsou. Doporučit lze například namátkové kontroly uživatelů, u nichž byla v minulosti zjištěna protiprávní aktivita, avšak absenci provádění těchto

[49] V podobném duchu se vyjadřuje i odborná literatura. Viz např. HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 111.

[50] Viz bod 122 Rozsudku Soudního dvora EU ze dne 12. července 2011 ve věci C-324/09 v řízení *L'Oréal SA a další proti eBay International AG a další*.

[51] Viz HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 108.

[52] Ibidem.

[53] Viz rozsudek *Viacom International, Inc. v. YouTube, Inc.* 676 F.3d 19. In: *Berkman Klein Center for Internet and Society at Harvard University* [online]. 5. 4. 2012 [cit. 2017-01-11]. Dostupné z: <https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf>.

[54] Ibidem.

[55] Rozsudek *In re Aimster Copyright Litigation*, 334 F.3d 643. In: *Digital Law Online* [online]. 30. 6. 2003 [cit. 2017-01-11]. Dostupné z: <http://digital-law-online.info/cases/67pq2d1233.htm>.

kontrol nelze považovat za *„willful blindness“*. Za *„willful blindness“* lze ale považovat situaci, kdy poskytovatel učí uživatele, jak šifrovat protizákonné šíření právem chráněných děl, protože takto si poskytovatel sám znemožní předcházet porušování autorských práv.[56] Na závěr doplňujeme, že odborná zahraniční literatura nepohlíží na *„willful blindness“* jako na samostatný důvod, při němž automaticky dochází k zániku vyloučení odpovědnosti. Jde však o významný indikátor, který může být u soudu použit jako prostředek k určení záměru poskytovatele hostingových služeb.[57]

3.2 Skutečná vědomost

V ustanovení § 5 odst. 1 písm. b) ZSIS je zakotvena definice tzv. skutečné vědomosti a podmínky pro vyloučení odpovědnosti ve chvíli, kdy se poskytovatel prokazatelně dozví o porušování práva učiněném prostřednictvím jeho služby.

Klíčová je zde interpretace termínu *„protiprávní povaha obsahu informace nebo jednání“* a informace o této protiprávnosti. K povaze oznámení se rozsáhle vyjadřuje odborná literatura,[58] která klade důraz na obsah oznámení poskytovateli. Ten totiž nemůže považovat každé oznámení za důvodné. Reagovat by měl vždy na oznámení, které je určité, váže se ke konkrétnímu případu a dokládá protiprávnost uložené informace. Oznámení, které nestanoví, v čem je určitá informace protiprávní, není dostatečně určité.

Pro vyloučení odpovědnosti musí v tomto ohledu poskytovatel neprodleně konat, aby se udržel v bezpečném přístavu. Neprodlenost je v tomto smyslu relativní, protože se opět odvíjí od konkrétního případu a posouzení, jak často poskytovatel sám kontroluje automatický běh služby. Dále je rozumné zahrnout do kritéria neprodlenosti i lhůtu, během níž poskytovatel služby kontaktoval třetí stranu, jež sporovaný obsah poskytla, aby se k protiprávnosti sama vyjádřila. Měla by tak však učinit ve lhůtě pevně stanovené poskytovatelem služby, aby ten pak mohl dle svého dalšího uvážení jednat.

3.3 Kontrola nad uživatelem

Se skutečnou vědomostí dle § 5 odst. 1 písm. b) ZSIS úzce souvisí koncept kontroly nad uživatelem, který je definován v § 5 odst. 2 ZSIS. Podle tohoto ustanovení odpovídá poskytovatel služby *„vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele“*. Termín rozhodující vliv je přitom klíčový, protože jeho výklad má dopad na určení momentu, v němž přestává být poskytovatel vyňat z omezení odpovědnosti. Charakteristickým znakem rozhodujícího vlivu je podle literatury *„faktické aktivní ovlivnění“* individuální povahy.[59] Za rozhodující vliv na uživatele tak nemůže být považováno například silně motivační schéma pro využívání služby a poskytování obsahu prostřednictvím této služby. Rozhodujícím vlivem se

[56] Ibidem.

[57] Viz např. SIRICHIT, M. Catching the Conscience: An Analysis of the Knowledge Theory under 512 (C)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags. *Albany Law Journal of Science & Technology*. 2013. Vol. 23, Issue 1, s. 85–190. Viz s. 108.

[58] Viz např. POLČÁK, R. Odpovědnost poskytovatelů služeb informační společnosti. *Právní rozhledy*. 2009, č. 23, s. 837 an., nebo HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 115 an.

[59] Viz MAISNER, M. *Zákon o některých službách informační společnosti. Komentář*, s. 94.

naopak rozumí konání uživatele na pokyn poskytovatele, a to ať v rámci pracovněprávního nebo jiného vztahu včetně situací, kdy právní titul absentuje a uživatel je poskytovatelem určitým způsobem nucen k určitému chování (např. vyhrožováním).[60]

4. OBECNÉ DŮVODY VYLOUČENÍ (PREVENTIVNÍHO) DOHLEDU

ZSIS v § 6 výslovně stanoví, že poskytovatelé služeb dle § 5 ZSIS nejsou povinni dohlížet na obsah jimi přenášených nebo ukládaných informací, ani aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace. Implementuje tím čl. 15 směrnice o elektronickém obchodu, který se nazývá „Neexistence obecné povinnosti dohledu". Recitál 47 směrnice zároveň stanoví, že *„zákaz ukládat poskytovatelům služeb povinnost dohledu uložený členským státům platí pouze pro povinnosti obecné povahy. Zákaz se netýká povinnosti dohledu ve zvláštních případech, a zejména nebrání rozhodnutím vnitrostátních orgánů přijímaným v souladu s vnitrostátními předpisy."*

Obecnou povinnost dohledu vylučuje i evropská judikatura. Podle ní *„opatření vyžadovaná ze strany dotčeného poskytovatele on-line služby nemohou spočívat v aktivním dohledu nad všemi údaji každého z jeho zákazníků za účelem předcházení jakémukoliv dalšímu porušování práv duševního vlastnictví prostřednictvím internetových stránek tohoto poskytovatele. Kromě toho taková povinnost obecného dohledu by byla neslučitelná s článkem 3 směrnice 2004/48, který stanoví, že opatření uvedená v této směrnici musí být nestranná a přiměřená a nesmí být nadměrně nákladná."*[61]

Judikatura se vyjadřuje i k charakteristikám filtrovacího systému, který by představoval zakázané uložení povinnosti obecného dohledu. Po poskytovatelích tedy nelze požadovat, aby zavedli systém filtrování *„všech elektronických sdělení přenášených prostřednictvím jeho služeb, zejména s využitím programů ‚peer-to-peer'; použitelný vůči všem jeho zákazníkům bez rozdílu; preventivně; výlučně na jeho náklady, a bez časového omezení, způsobilý identifikovat pohyb elektronických souborů obsahujících hudební, kinematografické nebo audiovizuální dílo, k němuž navrhovatel údajně vlastní práva duševního vlastnictví, v síti tohoto ISP za účelem zablokování přenosu souborů, jejichž výměna porušuje autorská práva"*.[62] Podle stejného rozhodnutí je protiprávní požadovat po poskytovateli zavést systém filtrování, který *„obnáší sledování veškerých elektronických sdělení přenášených v síti dotyčného ISP […] přičemž toto sledování je navíc časově neomezené, vztahuje se na veškeré budoucí porušování práv a předpokládá povinnost chránit nejen existující díla, ale i díla budoucí, která v okamžiku zavedení uvedeného systému ještě nebyla vytvořena."*[63]

---

[60] Ibidem. Komentář se zde detailně věnuje i negativnímu vymezení kontroly uživatele poskytovatelem. Na jednání uživatele tak nelze nahlížet jako na jednání na základě pověření v těchto případech: *„poskytovatel poskytuje pouze zprostředkovatelské služby; poskytovatel nejedná prostřednictvím uživatelského účtu (fingované jednání uživatele); poskytovatel nejedná prostřednictvím svého spolupracovníka či spřízněné osoby; a poskytovatel nevykonává formu dohledu či nedisponuje vlivem nad jednáním třetí osoby v oblasti občanského, korporátního a pracovního práva."*

[61] Viz Rozsudek Soudního dvora EU ze dne 12. července 2011 ve věci C-324/09 v řízení *L'Oréal SA a další proti eBay International AG a další*, bod 139.

[62] Viz Rozsudek Soudního dvora EU ze dne 24. listopadu 2011 ve věci C-70/10 v řízení *Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, bod 29.

[63] Ibidem, bod 47.

Přítomnosti určité míry porušování práv třetích osob ve službě se všeobecně předpokládá. Jenom na základě takovéhoto povědomí nelze po poskytovateli požadovat, aby proaktivně monitoroval nebo prohledával obsah ve své službě. Na druhou stranu odborná literatura rozlišuje mezi mladou a zavedenou službou poskytování hostingu.[64] S ohledem na požadavek přístupu k problematice porušování autorských práv s řádnou péčí hospodářského subjektu je poskytovatel povinen učit se z toho, jak přibývají případná porušení autorských práv. Na základě identifikovaných jednotlivých porušení práva by tedy měl poskytovatel pro zvýšení své vlastní právní ochrany zavádět určitá preventivní opatření, zejména pak v rovině sekundární a terciární prevence, tak, aby pomohl předcházet dalšímu porušování práv. Zároveň se však na stejném místě uvádí, *„že niektoré služby by ani ex post nemali niesť žiadnu alebo len veľmi obmedzenú povinnosť zabezpečiť službu"*.[65]

Jak již bylo uvedeno výše, k obecnému zákazu dohledu se vyjádřil i Soudní dvůr EU. V případu *SABAM proti Netlog NV* Soudní dvůr vyjádřil rovněž názor, že by obecná povinnost dohledu představovaná v tomto případě systémem filtrování implikovala nutnost aplikovat právo na ochranu osobních údajů, protože systém filtrování *„by totiž obnášel na jedné straně identifikaci, systematický rozbor a zpracování informací vztahujících se k profilům vytvořeným na sociální síti uživateli této sítě"*.[66] Odpovědnost poskytovatelů hostingových služeb tedy není viditelně omezena pouze na oblasti definované v ZSIS, ale je třeba ji zasadit do širšího kontextu dalších právních pravidel.

5. PREVENČNÍ POVINNOST A KONTRAVALENTNÍ VZTAH SPECIALITY A SUBSIDIARITY (PŘÍKLAD E-SOUKROMÍ *LARGO SENSU*)

Při aplikaci odpovědnostních vztahů dle ZSIS je nutno řešit i související vztahy speciality (generality) a subsidiarity. Zatímco ZSIS tak představuje z pohledu poskytovatelů *lex specialis* (ve vztahu k zákonům definujícím jiné druhy odpovědností), řada dalších předpisů pak představuje *lex generalis*, typicky *jde o* oblast vztahu k ochraně práv duševního vlastnictví (viz výše), ochrany soukromí, případně anonymity či identifikace jednotlivce v rámci nových technologií používaných v elektronických sítích a službách).

Typický příkladem těchto nezřídka opomíjených vztahů je aplikačně problematická oblast ochrany osobních údajů. Směrnice o *e-Privacy* č. 2002/58/EC[67] (dále jen „směrnice *e-Privacy*") tak např. upravuje některá pravidla v oblasti zpracování osobních údajů v elektronických komunikacích, s dosahem do služeb informační společnosti, zejména povinnost hlášení narušení bezpečnosti osobních údajů při zajišťování sítí a poskytování služeb elektronických komunikací a pravidla pro rozesílání obchodních sdělení.

Tato problematika pojmově širšího e-soukromí byla běžně posuzována optikou tradiční (občanskoprávní) ochrany osobnosti, minimálně však byla v aplikační praxi nahlížena

64 Viz HUSOVEC, M. *Zodpovednosť na internete podľa českého a slovenského práva*, s. 84–85.
65 Ibidem, s. 91.
66 Viz Rozsudek Soudního dvora EU ze dne 16. února 2012 ve věci C-360/10 v řízení *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) proti Netlog NV*, body 24, 48 a citace z bodu 49.
67 Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

skrze pravidla pro zpracování osobních údajů. Ke srozumitelnosti nepřispěla ani relativně samostatná právní úprava nakládání s informacemi typu *„cookies"*. Ke zpraktičtění ochrany osobních údajů v prostředí internetu bohužel nepomohlo ani zjednodušení definice zásadního a poměrně složitého institutu ochrany osobních údajů, souhlasu se zpracováním osobních údajů, v prostředí internetu fakticky ztotožněného s kliknutím prováděným na stránce zobrazené ve webovém prohlížeči.

Bez zásadního povšimnutí širší odborné veřejnosti po dlouhou dobu zůstávala nezávazná stanoviska bruselské expertní skupiny WP29[68] týkající se celé řady otázek spojovaných s internetem, např. posouzení povahy provozních údajů, odpovědnosti poskytovatelů služeb internetových vyhledávačů, *cookies* (s výhradou vůči přísné evropské úpravě co se týče tzv. *first-party-analytic cookies*), zpracování údajů při online reklamě, anonymizačních či pseudonymizačních technik v prostředí internetu. Situace se zásadně změnila až v několika posledních letech, když tato stanoviska začala být zohledňována některými nejvyššími soudy a především Soudním dvorem EU, při rozhodování o otázkách přeshraničního zpracování osobních údajů v globálních podmínkách, nadnárodními společnostmi a při vymezení jejich povinností vůči občanům členských států EU.

Významným předpisem, jehož přijetím zdaleka neskončila diskuse k výše uvedeným otázkám, je především obecné nařízení o zpracování osobních údajů č. 2016/679,[69] které bylo přijato v květnu 2016 a bude účinné od května 2018 (dále jen „GDPR"). Z obsahu povinností vyplývajících z tohoto nařízení je patrné, že současná judikatura výrazně ovlivní i výklad jeho ustanovení, a to včetně např. debaty o povaze IP adres před Soudním dvorem EU apod. Uvedené je způsobilé změnit rovněž současný přístup Komise EU k právě probíhající revizi směrnice o *e-Privacy*. Samostatnou pozornost si tak zaslouží samostatně životaschopná a silně projudikovaná otázka odpovědnosti za vlastní i cizí obsah na internetu a jeho vztah k odpovědnosti za zpracování osobních údajů.

5.1 Odpovědnost za zpracování osobních údajů v případech regulovaných ZSIS

ZSIS lze ve vztahu k obecné úpravě (zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, dále jen „ZOÚ") považovat za zvláštní zákon (*lex specialis*), který se na zpracování informací, včetně osobních údajů, při poskytování služeb informační společnosti uplatní přednostně, tj. např. v rámci svých speciálních pravidel tam, kde zvláštní právní předpis (ZOÚ) věc sám neupravuje. Nejedná se pouze o otázky zveřejnění nepravdivých či dehonestujících osobních údajů v prostředí internetu, jak je obvykle uvažováno. Stejně silně může do soukromí člověka (dotčené osoby) na internetu, a to – až paradoxně – i větším časovým odstupem, zasáhnout dostupnost údajů neúplných či zastaralých (v této rovině jasně uvažoval SDEU v případu *Google proti Mario Costeja Gonzáles*,[70] když rozhodoval o právu být zapomenut).

---

[68] Pracovní skupina na ochranu osobních údajů zřízená podle článku 29 směrnice 95/46/ES, angl. *Article 29 Data Protection Working Party*.

[69] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), angl. *General Data Protection Regulation*.

[70] Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014 ve věci C-131/12, v řízení *Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*.

Z pohledu ZOÚ je poskytovatel služeb informační společnosti správcem osobních údajů, který stanoví účel a prostředky zpracování údajů. V interakci s jinými poskytovateli v rámci dodávek služeb však nelze vyloučit, že současně bude i zpracovatelem údajů pro jiné správce (pro související, z pohledu práva však samostatné účely zpracování údajů). Zákonné principy ochrany osobních údajů předpokládají dokonalou (plnou) kontrolu správce nad zpracováním (a to i v případě řetězení nasmlouvaných zpracovatelů), s nímž spojují objektivní odpovědnost správce za výsledek konání. Tato konstrukce se v prostředí internetu ukazuje jako silně zjednodušená, neboť nelze po správcích řady internetových služeb spravedlivě požadovat, aby kontrolovali či usměrňovali způsoby, jak jejich klienti, uživatelé služeb, zacházejí s informacemi, zejména pokud tyto údaje sami uživatelé zveřejňují a jinak šíří. ZSIS proto přisvědčuje tradičnímu pojetí odpovědnosti za zpracování osobních údajů pouze v případech, kdy správce – poskytovatel služeb přenosy a ukládání údajů sám iniciuje, aktivně ovlivňuje, mění atp. (§ 3 a § 4 ZOÚ).

V řadě životních situací, kdy jsou údaje poskytovány (ukládány) uživateli služeb, je však odpovědnost poskytovatelů služeb za zpracovávané osobní údaje výrazně snížena. Podle § 5 odst. 1 písm. b) ZSIS poskytovatel odpovídá pouze tehdy, pokud se prokazatelně dozvěděl 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. Poskytovatelé služeb přitom nejsou povinni dohlížet na obsah jimi přenášených nebo ukládaných informací a aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.

V takových případech musí dotčená osoba coby osoba namítající protiprávnost určitých uložených informací, svých osobních údajů, být schopna, kromě prokázání svojí totožnosti i faktu, že konkrétní použité (zveřejněné) údaje se jí týkají, dále zejména doložit, že ke zpracování jejích údajů není dán řádný právní titul. Absencí právního titulu rozumíme nejen, že ke zveřejnění či jinému zpracování neposkytla dotčená osoba souhlas, ale také že není dán ani jiný zákonný důvod pro zpracování osobních údajů uvedený v § 5 odst. 2 písm. a) až g) ZOÚ (plnění smlouvy či právní povinnosti, existence jiného sporu s dotčenou osobou, ochrana jiných práv, oprávněné zveřejnění údajů atd.).

Dotčená osoba se může s konkrétním podezřením obrátit na poskytovatele služeb nejdříve formou žádosti o informaci podle § 12 nebo o vysvětlení podle § 21 odst. 1 ZOÚ. V jistých případech totiž teprve až po obdržení dodatečných informací týkajících se zpracování údajů bude schopna doložit své tvrzení, že některá ze zveřejněných informací je zveřejněna protiprávně.

Pokud se poskytovatel služby dozví o zřejmě protiprávní povaze některé z uložených informací, je povinen tuto situaci řešit a to neprodleně. Musí učinit příslušné kroky k odstranění nebo k znepřístupnění závadných informací. Z § 5 odst. 2 písm. e) ZOÚ však vyplývá pro poskytovatele možnost nelikvidovat a uchovat ty předmětné osobní údaje, které mohou být využitelné pro ochranu jeho práv a právem chráněných zájmů (typicky navazující řízení o náhradu škody, trestní řízení). Poskytovatel je však v takovém případě povinen zajistit, aby údaje nebyly přístupné dalším osobám.

Jestliže poskytovatel služeb ani po věrohodném, respektive doloženém sdělení, že konkrétní zveřejnění určitých údajů je protiprávní, tyto neodstraní ani neznepřístupní, může se poškozená osoba odstranění protiprávního stavu domáhat podnětem Úřadu

pro ochranu osobních údajů, který na základě jejího podnětu může s daným provozovatelem zahájit řízení, kontrolní nebo správní, pro podezření z porušení povinností při zpracování osobních údajů.

V návaznosti na zjištění získaná v rámci úředního, kontrolního či správního, může být pak povinnost konat poskytovateli úředně nařízena, a to uložením nápravy, např. příkazem osobní údaje znepřístupnit, blokovat či zlikvidovat. Pokud bude zjištěno porušení zákona, může Úřad pro ochranu osobních údajů současně vést správní řízení pro podezření ze spáchání přestupku nebo jiného správního deliktu za porušení povinností při zpracování osobních údajů (především se ZOÚ).

Typickým odpovědným subjektem v případech poskytování služeb v prostředí internetu jsou podle ZOÚ ve spojení se ZSIS především poskytovatelé služeb. Nelze však vyloučit, v případě zahraničních poskytovatelů služeb, ani odpovědnost jiných tuzemských subjektů, na něž také dopadá působnost ZOÚ a dozorová kompetence Úřadu pro ochranu osobních údajů, např. poskytovatele webhostingových služeb. V určitých případech je představitelné zastavení dané aplikace jako celku či přístupu k ní, tedy nikoliv pouze odstranění protiprávně uložených údajů (pokud k nim poskytovatel hostingu nemá přístup).

5.2 Role a odpovědnost podle GDPR

GDPR převzalo na základě svého čl. 29 základní vymezení rolí subjektů odpovědných za zpracování osobních údajů, správce a zpracovatele, s tím, že ke zpracování jinými osobami jednajícími z pověření správce nebo zpracovatele a majícími přístup k osobním údajům je třeba pokynu správce (nestanoví-li povinnost zpracovávat přímo zákon). GDPR tak na několika místech na rozdíl od stávající směrnice zdůrazňuje úlohu správce, a to zejména vymezením vůči pouhému zpracovateli, kdy zpracovatel nesmí zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. Avšak zpracovatel porušující pravidla dle GDPR tím, že určil účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce (viz čl. 28). A pokud GDPR umožňuje správci nebo zpracovateli jmenovat své zástupce, nevylučuje právní kroky, které by mohly být zahájeny proti správci nebo zpracovateli samotnému.

Novinkou GDPR je možnost stanovení společných správců, pokud to účely a prostředky zpracování vyžadují. Společní správci musí mezi sebou transparentním ujednáním vymezit své podíly na odpovědnosti za plnění povinností podle čl. 26 GDPR.

Ačkoliv nové technologie byly jedním ze zásadních důvodů pro přijetí GDPR (viz recitál č. 6), respektuje text nařízení tezi technologické neutrality. Při výkladu pravidel pro zpracování dat v prostředí internetu je nutno vedle povinností správců a zpracovatelů, formulovaných pro všechny sektory zpracování údajů, přihlédnout k povinnostem odvozeným z modernizovaných, respektive prohloubených práv dotčených osob (subjektů údajů), typických pro online prostředí, jako jsou např. právo být zapomenut a právo na omezení zpracování a přenositelnost údajů.

Základní povinností správce osobních údajů je zavést vhodná technická a organizační opatření, a to s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob. Tato

opatření musí být nastavena a podle potřeby revidována a aktualizována s přihlédnutím k řadě aspektů (včetně stavu techniky a rizikům pro práva osob, jež sebou zpracování nese), s důrazem na nutnost pseudonymizace a minimalizace údajů a tvorby záruk k ochraně dotčených osob (čl. 24 a 25 GDPR).

Například na neexistenci obecné povinnosti dohledu zmíněnou v kapitole 4 je tedy nutno pohlížet i z hlediska speciálních ustanovení GDPR týkajících se profilování dospělých fyzických osob a dětí, které zasluhují dle GDPR zvláštní ochranu. Systémy filtrování nebo případně jiná preventivní opatření, která budou využívat automatizovaných postupů analýzy informací vztahujících se k fyzické osobě za účelem hodnocení nebo předvídání jejího chování, a následně budou tyto informace používat pro rozhodování o umožnění či neumožnění vykonávání určitých aktivit uživatelem, totiž podléhají ještě přísnějšímu režimu, kdy jsou správci stanoveny specifické povinnosti. S ohledem na úpravu GDPR tedy nelze po poskytovateli hostingu spravedlivě požadovat zavádění jakýchkoli preventivních opatření souvisejících se zpracováváním osobních údajů. Za určitých okolností se totiž poskytovatel hostingového obsahu může dostat do situace, kdy by mohl začít v rámci profilování zpracovávat i kategorie osobních údajů, jejichž zpracování je z principu zakázáno. Jedná se o zpracovávání údajů o znacích chování fyzické osoby, které umožňuje jedinečnou identifikaci této osoby, tj. o biometrický údaj. Přestože jsou totiž biometrické údaje chápány primárně jako údaje o měřitelných fyzických nebo fyziologických znacích osoby, začíná se v souvislosti s neustálým rozvíjením monitorovacích technik hovořit o behaviorální biometrice a biometrických údajích tzv. druhé generace. Tyto biometrické údaje nevypovídají o tom, co člověk je, ale zaměřují se na procesy spojené s jeho fungováním, tedy jaký člověk je v průběhu času. V případě možnosti analýzy dostatečného množství dat lze za určitých podmínek nahlížet na profil chování fyzické osoby jako na biometrický údaj umožňující jedinečnou identifikaci této osoby. Zpracování této zvláštní kategorie osobních údajů ale podléhá dle čl. 9 GDPR mnohem striktnějšímu režimu. S dodržením zákonnosti zpracování by tak zpravidla vyvstaly nepřekonatelné problémy.

ZÁVĚR

Interpretačně netriviální místa právní úpravy v praxi nezřídka mohou vést regulátora k vydání sporných aplikačních postupů a interpretačních stanovisek, kterým by bylo možno předejít, pokud by byl důsledně uplatňován princip speciality a generality. Uvedené bylo možné demonstrovat na příkladu tzv. globálně poskytovaných služeb, tj. konkrétně služeb ukládání obsahu informací poskytovaných uživatelem (hosting) s ohledem na kritéria povahy a druhu přenášeného obsahu, a to zejména pak pokud jde o předměty duševního vlastnictví (typicky autorská díla), ochranu osobních údajů (včetně údajů biometrických) aj. V tomto ohledu tak bylo nutno především odmítnout interpretaci obsaženou ve výkladovém stanovisku Ministerstva průmyslu a obchodu, docházející k závěru, že v případech, kdy si je poskytovatel služby spočívající v ukládání informací poskytnutých uživateli vědom, že výše jeho příjmů nebo výnosů přímo souvisí s mírou protiprávního obsahu ukládaných uživateli, nemůže se dovolávat toho, že neodpovídá za tento obsah podle zákona. Tento závěr trpěl z pohledu logické interpretace podstatným nedostatkem spočívajících v tom, že v nesprávném předpokladu, respektive tvrzení,

že vyšší míra nelegálního obsahu na datovém úložišti znamená vyšší příjmy provozovatele datového úložiště, a to bez ohledu na to, zda provozovatel účtuje vyšší sazby za stahování nelegálního obsahu, či nikoliv. Takovýto argument vede nutně k úvaze, zda vůbec existuje nějaké datové úložiště (např. *cloud*), v němž výše příjmů nezávisí na povaze ukládaných informací. Pokud totiž žádné datové úložiště není imunní vůči fluktuaci příjmů v závislosti na povaze ukládaných informací, pak se podle tohoto výkladového stanoviska nemůže dovolávat vyloučení odpovědnosti žádný poskytovatel služeb hostingu. Taková interpretace by ovšem popírala hlavní smysl i účel přijetí předmětné regulace. Z těchto důvodu tak bylo nutno závěry tohoto výkladového stanoviska, včetně jeho dílčích závěrů a argumentace, bez dalšího odmítnout. S výše uvedeným výkladovým vodítkem souvisí i koncept kontroly nad uživatelem (§ 5 odst. 2 ZSIS), podle kterého odpovídá poskytovatel služby vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele. Takovým charakteristickým znakem rozhodujícího vlivu pak musí nutně být především faktické aktivní ovlivnění individuální povahy, nikoliv pouze určité motivační schéma pro využívání služby a poskytování obsahu prostřednictvím této služby. Za rozhodující vliv tak nutno považovat především takové konání uživatele na pokyn poskytovatele, a to ať v rámci pracovněprávního nebo jiného vztahu včetně situací, které absentuje jak právní titul, tak je i současně poskytovatelem určitým způsobem nucen k určitému chování (např. vyhrožováním apod.).

V tomto kontextu tak nutno rovněž nahlížet i na samotný obecný zákaz dohledu nad obsahem dat ukládaných uživatelem, který nutno ve shodě se shora uvedenou judikaturou Soudního dvora EU interpretovat tak, že obecná povinnost dohledu (systému filtrování) neobsahuje postup dle zákonných principů ochrany osobních údajů, který by tak implikoval složitý mechanizmus identifikace, systematického rozboru, filtrace a zpracování informací vztahujících se k vytvářeným profilům (např. na sociálních sítích apod.). Uvedené však nesmí směřovat k závěru, že neexistence obecné povinnosti dohledu (viz kapitola 4 tohoto článku) vylučuje tyto poskytovatele z režimu jiných speciálních ustanovení GDPR týkajících se profilování dospělých fyzických osob a dětí, které zasluhují dle GDPR zvláštní ochranu. Systémy filtrování nebo případně jiná preventivní opatření, která budou využívat automatizovaných postupů analýzy informací vztahujících se k fyzické osobě za účelem hodnocení nebo předvídání jejího chování a následně budou tyto informace používat pro rozhodování o umožnění či neumožnění vykonávání určitých aktivit uživatelem, totiž podléhají ještě přísnějšímu prevenčnímu režimu, kdy jsou správci osobních údajů stanoveny specifické povinnosti. S ohledem na úpravu GDPR však nelze po poskytovateli hostingu spravedlivě požadovat zavádění preventivních opatření souvisejících se zpracováváním osobních údajů. Za určitých okolností se totiž poskytovatel hostingového obsahu může dostat do situace, kdy by mohl začít v rámci profilování zpracovávat i kategorie osobních údajů, jejichž zpracování je z principu zakázáno (typicky údaje o znacích chování fyzické osoby, které umožňuje jedinečnou identifikaci této osoby, tj. např. o biometrické údaje, případně behaviorální údaje tzv. druhé generace). Zpracování těchto kategorií osobních údajů tak podléhá dle čl. 9 GDPR mnohem striktnějšímu preventivnímu režimu než tomu vyplývajícímu z ZSIS.

Analysis of the Liability of Hosting Service Providers with Regard to the Nature and Type of Transferred Content

Ján Matejka – Alžběta Krausová

Abstract: *The currently ongoing process of globalization is closely intertwined, inter alia, with the development of information society services. These services represent one of significantly emerging economic sectors on the market. Development of individual economic sectors is, however, dependent also on clear and comprehensible legislation which ensures predictability and certainty in legal relationships. Information society services are regulated both at the European and national level which often leads to the situation when fundamental legal institutes are interpreted purposefully and repeatedly also erroneously. In the context of the global nature of Internet services, this, unfortunately, does not result in commencing judicial proceedings (therefore, also in not searching for legal arguments) not only because of the lengthiness of such proceedings but also because of the overall absence of legal certainty as well as a lack of clarity of the whole portfolio of this protection. Therefore, the aim of this article is to interpret in detail the provisions of the Act on certain information society services that regulate the so called globally provided services, namely services providing hosting to users' contents. The interpretation of the relevant provisions will take into account the territorial, material and personal scope of the relevant national legislation, European directives and relevant case law, as well as some published opinions and statements of central administrative authorities. At the same time, special consideration will be given to the issue of processing and retention of personal data by a hosting service provider and to the relationship between the Act on certain information society services and the right to the protection of personal data.*

Key words: *liability, constructive knowledge, actual knowledge, no-monitoring obligation, relationship of specialty, subsidiarity and generality, hosting provider, GDPR, personal data protection, biometric data*