Je svoboda šířit a přijímat informace ve virtuálním prostředí svobodou virtuální?

Kristina Rademacherová*

Is the Freedom to Share and Receive Information in a Virtual Environment a Virtual Freedom?

Summary: *With the emergence of information and communication technology, the freedom of expression including the freedom to receive and impart information has undergone significant changes. Even though the democratization processes of online information publication seemingly evoke an unlimited possibility to spread and accept almost anything in a virtual environment, the freedom to receive and impart information in cyberspace is not a process without obstacles. Certain principles and legal rules may be deducted from the decision-making practice of the European Court of Human Rights and the Court of Justice of the European Union, as well as from the recommendations of certain international organizations. The freedom to receive and impart information in cyberspace may be seen not only as a basic human right, but also from the point of view of the EU prohibition of any free market restrictions based on any form of discrimination.*

Key words: *dissemination of information, virtual environment, cyberspace, Internet, freedom of expression*

Schopnost získat, uschovat a využít informace je pro člověka zásadní. Bez informací lze těžko dospět k moudrému úsudku, učinit rozumnou volbu. Sdílení informací je klíčové pro globalizované finanční trhy, národní i mezinárodní bezpečnost, pro oblast vzdělávání, zdravotnictví či sociálních služeb. Lidské společenství bychom mohli označit za informační od samého počátku,[1] neboť informace byly odjakživa důležitým faktorem při spravování věcí soukromých i veřejných.[2] Přístup k informacím ovšem doznal podstatných změn. Zatímco všemocný stát absolutistického typu nesdílel se svými občany informace o vládnutí, ve státě, jehož vláda je omezena a založena na důvěře občanů, informační embargo neobstojí.[3] Lidské společenství si uvědomuje význam informací a ke zvýšení míry své informovanosti stále více využívá moderních informačních a komunikačních technologií, což vede k tomu, že jsme denně konfrontováni s nepřeberným množstvím informací a informačních systémů. Předpokladem ideální informační společnosti,[4] v níž probíhá ničím neomezená tvorba, zpracování a distribuce informací, je právě svoboda projevu a svoboda šířit a přijímat informace pomocí informačních a komunikačních technologií.

Hodnotovým základem informační společnosti jsou svoboda a solidarita. Solidarita se ve virtuálním prostředí projevuje přirozenou tendencí člověka ke vzájemné informační výměně.[5] Právo šířit a přijímat informace ve virtuálním prostředí[6] předpokládá ničím neomezenou možnost informace vytvořit a rozšiřovat (aktivní přístup uživatele), ale také možnost informace nalézt a získat k nim

* Autorka působí jako externí doktorandka na katedře správního práva a správní vědy PF UK. Článek byl zpracován s podporou finančních prostředků Univerzity Karlovy, SVV č. 260 359, na rok 2017. E-mail: kristina.rademacherova@gmail.com.

1 Podle Polčáka lze každou společnost považovat za informační, neboť informace jsou tím, co zajišťuje lidskému společenství přežití a rozvoj. Právě využívání informačních a komunikačních technologií je však tím, co ze společnosti činí informační společnost. Polčák, R. *Internet a proměny práva.* Praha 2012, str. 275.

2 Birkinshaw, P. *Freedom of information: the law, the practice, and the ideal.* 4. vyd. Cambridge 2010, str. 8–9.

3 Tamtéž, str. 18–23.

4 K dokonalé či ideální informační společnosti podrobněji Polčák, R., c. d., str. 275–280.

5 Typickým projevem je např. rozšířené sdílení dat. Podrobněji Polčák, R., c. d., str. 284–287.

6 Pojmy virtuální prostředí a kybernetické prostředí, resp. kyberprostor, jsou v textu užita jako synonyma. Kyberprostor zahrnuje Internet, tj. celosvětovou počítačovou komunikační síť, i veškerá globální média, komunikační kanály a systémy vzájemně propojených počítačových zařízení, tj. internetové sítě. „Internet" ve smyslu celosvětové informační a komunikační sítě píšeme s velkým počátečním písmenem, zatímco „internet" označuje jakoukoliv propojenou počítačovou síť. Smejkal, V. *Kybernetická kriminalita.* Plzeň 2015, str. 52.

přístup umožňující jejich využití (pasivní přístup). Co se týče svobody projevu ve virtuálním prostředí, může se na první pohled zdát, že se dotýká pouze aktivního projevu uživatele veřejné části virtuálního prostředí.[7] Podle Ústavního soudu je projevem sdělení informace nebo vyjádření názoru slovem, písmem, obrazem či jiným způsobem, který zahrnuje i expresivní projevy.[8] Svoboda projevu je však ve virtuálním prostředí úzce spjata s informační svobodou (svobodou šířit a přijímat informace) v tom smyslu, že jednak může být svobodný projev podmíněn právě informační svobodou (stát, který cenzuruje informace ve veřejném prostoru, tak činí většinou s cílem ovlivnit svobodu projevu svých občanů[9]), dále pak může být výkon práva šířit informace (typicky v případě sdílení online obsahu v podobě odkazů) rovněž projevem svobody projevu, neboť ve virtuálním prostředí stačí k vyjádření vlastního názoru i jednoduché kliknutí myší.[10] Vzájemně podmíněný vztah si uvědomují i státy s totalitním režimem omezujícím svobodu projevu, které svým občanům odmítají poskytovat neomezený přístup k Internetu.[11] Vztah svobody projevu a práva šířit a přijímat informace je ve virtuálním prostředí podmíněn významněji než v prostředí offline.[12]

Před rozvojem informačních a komunikačních technologií bylo veřejné šíření informací vázáno na interakci s tradičními médii, která veřejnosti zprostředkovávala informace, jež uznala za vhodné. Tradiční média ovlivňovala sdílený obsah i jeho auditorium.[13] Zatímco tradiční média dovedl stát kontrolovat a omezit poměrně snadno, při kontrole obsahu virtuálního prostředí je dosažení stejných výsledků problémem.

Svobodu projevu a právo na informace zaručuje čl. 17 odst. 1 Listiny základních práv a svobod[14] (dále též „Listina"), která jimi chápe právo vyjadřovat názory i svobodu vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na státní hranice.[15] Charakter svobody projevu, tzv. *status negativus*, ji řadí do sféry osobní autonomie jedince, do níž stát nesmí zasahovat.[16] Svoboda projevu má jak aspekt pozitivní, neboť její nositel ji *může* využít, tak aspekt negativní, tedy nikoho nelze k projevu v jakékoli formě nutit.[17] Článek 10 Evropské úmluvy o ochraně základních lidských práv a svobod (dále též „Úmluva") hovoří o právu na svobodu projevu zahrnující svobodu zastávat názory i svobodu přijímat a rozšiřovat informace nebo myšlenky bez zásahu státních orgánů a bez ohledu na státní hranice. Bez rozlišení, zda hovoříme o právu, či svobodě, zůstává obsah stejný.

Smyslem svobody projevu je možnost poznání sebe samých a společnosti, v níž žijeme. Spolu se svobodou šířit a přijímat informace nám zajišťuje prostředek nápravy společnosti, nejsme-li s jejím stavem spokojeni.[18] Svoboda projevu a právo šířit a přijímat informace patří mezi základní náležitosti demokratické společnosti. Jak svoboda projevu, tak právo šířit a přijímat informace jsou ovšem omezeny lidskou důstojností. Lidská důstojnost je klíčovým prvkem řady základních lidských práv, především práva na soukromý život a informační sebeurčení, zaručených čl. 10 Listiny. Na lidskou důstojnost přitom nelze nahlížet jen jako na subjektivní kategorii, ale měla by být objektivní nezcizitelnou hodnotou, způsobilou vytyčit svobodě šířit a přijímat informa-

7 Typickým příkladem jsou internetová diskusní fóra, blogy či sociální sítě, kde lze snadno a relativně účinně projevit vlastní názor a které často nabývají kritického, až nenávistného charakteru. K rozboru svobody projevu na Internetu a nenávistných projevů na internetových diskusních i sociálních sítích srov. např. Výborný, Š. *Nenávistný internet versus právo.* Praha 2013, str. 28 a násl.

8 Nález Ústavního soudu ČR ze dne 16. 6. 2015, sp. zn. I. ÚS 3018/14, bod 45. K rozlišení projevu srov. např. Bartoň, M. Rozlišení projevu od jiného jednání v kontextu dogmatiky svobody projevu. *Právní rozhledy*, 2014, roč. 22, č. 9, str. 317–325.

9 V tomto ohledu vyvolává protichůdné názory snaha některých státníků regulovat falešné zprávy na Internetu, odůvodněná ochranou občanů před manipulací ohrožující průběh voleb, bezpečnost státu, politickou stabilitu atd. Např. Rerich, J. Svět se snaží bránit nepravdivým informacím na internetu. In: *Český rozhlas plus* [online]. Dostupné na <http://www.rozhlas.cz/plus/svet/_zprava/svet-se-snazi-branit-nepravdivym-informacim-na-internetu--1680394>.

10 Srov. sdílení zpráv na sociálních sítích typu Facebook či Twitter nebo možnost ohodnotit příspěvek jednoduchou ikonou palce nahoru či dolů, vyjadřující souhlasný či nesouhlasný postoj. K dalekému využití uvedených funkcí sítí Facebook srov. Roosendaal, A. Facebook Tracks and Traces Everyone: Like This! Tilburg Law School Legal Studies Research Paper Series No. 03/2011. In: *SSRN* [online]. Dostupné na <https://ssrn.com/abstract=1717563> nebo <http://dx.doi.org/10.2139/ssrn.1717563>. Široké vnímání pojetí projevu vede i k opuštění pojmu svobody slova ve prospěch pojmu svobody projevu, který lépe vyjadřuje i neverbální projevy svobody. Srov. Bartoň, M. *Svoboda projevu a její meze v právu ČR.* Praha 2002, str. 18.

11 Vlivem arabského jara zablokovala Eritrea v roce 2011 své plány poskytnout občanům přístup k mobilnímu internetovému připojení, a Internet je tak dostupný pro méně než 1 % eritrejské populace. Severní Korea poskytuje přístup k Internetu jen vybraným jedincům a pouze vzdělávací instituce mají přístup k státem kontrolovanému intranetu. Eritrea a Severní Korea jsou dle studie zveřejněné roku 2015 Výborem pro obranu novinářů (CPJ) dvě nejvíce cenzurované země světa. Srov. CPJ. 10 Most Censored Countries. In: *Committee to Protect Journalists* [online]. Dostupné na <https://cpj.org/2015/04/10-most-censored-countries.php.

12 Pojem „offline" je v textu, při vědomí určitého zjednodušení, užit jako protiklad virtuálního prostředí.

13 Matejka, J. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha 2013, str. 187.

14 Usnesení předsednictva České národní rady č. 2 ze dne 28. prosince 1992, o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

15 Srov. čl. 17 odst. 2 Listiny.

16 Bartoň, M., *Svoboda*, str. 19.

17 Filip, J. *Vybrané kapitoly ke studiu ústavního práva*. Brno 2001, str. 129.

18 Podle Václava Bělohradského je vysoký počet lidí, kteří jsou ochotní omezit svobodu slova, jakmile jsou vyděšení pokřiveností společnosti, kterou svoboda slova odhalila, nebezpečný. Bělohradský, V. *Mezi světy a mezisvěty (filosofické dialogy)*. Praha 1997, str. 140.

ce ve virtuálním prostředí určité meze.

Omezení svobody projevu a práva šířit a přijímat informace z hlediska informačního sebeurčení závisí především na míře, v jaké se informační sebeurčení uplatní v určité sféře života. Ústavní soud rozlišuje sféru soukromou a sféru sociální. Zatímco v soukromé sféře, v níž jde o ochranu soukromí a práva na čest, platí naprosté informační sebeurčení (tj. je věcí každého, co a v jakém rozsahu bude sdílet jako veřejnou informaci), ve sféře sociální, tj. dle Ústavního soudu ve sféře společenské, občanské a profesionální, neplatí naprosté informační sebeurčení a za určitých podmínek do ní lze oprávněně vstoupit.[19]

Faktický výkon svobody projevu včetně svobody šířit a přijímat informace doznal s příchodem informačních a komunikačních technologií značných změn. Klíčovou roli hrál celosvětový systém veřejných propojených počítačových sítí – Internet –, jehož idea spočívá na principech informační svobody a solidarity, ale i informačního sebeurčení.[20] Internet plní podle Evropského soudu pro lidská práva zásadní roli v přijímání a výměně informací zejména tehdy, když jsou informace jinde obtížně dohledatelné.[21] Využití informačních sítí navíc umožňuje snadné vytváření a šíření nových informací. Podle Michala Bobka lze podstatu virtualizace šíření informací spatřit v demokratizaci jejich publikace, kterou umožnil Internet zejména díky snadné soukromé distribuci informací o fyzických a právnických osobách i orgánech veřejné moci.[22] Se vznikem kyberprostoru tak přišel svět, ve kterém může být každý vydavatelem.[23]

Ačkoli se informace v kyberprostoru šíří snadno, platí v něm obdobná omezení jako v prostředí mimo virtuální prostor. Text se věnuje nejen informační svobodě ve virtuálním prostředí, ale i možným překážkám výkonu práva šířit a přijímat informace ve virtuálním prostředí bez omezení ze strany orgánů veřejné moci a zabývá se doporučeními mezinárodních organizací i rozhodovací praxí Evropského soudu pro lidská práva a Soudního dvora Evropské unie. Dotýká se rovněž otázky vlivu státních hranic na svobodu šíření informací ve virtuálním prostředí.

Informace ve virtuálním prostředí vs. počítačová data

Virtuální či kybernetické prostředí je myšlený, uměle vytvořený prostor, ve kterém dochází ke komunikaci počítačových zařízení a k šíření informací nejrůznějšího druhu. Díky kybernetice, vědě zabývající se studiem chování složitých organizovaných systémů technických, biologických i sociálních,[24] začala být informace vnímána jako synonymum pro poznání vnější reality nejen lidmi, nýbrž i stroji.[25] V roce 1990 hovořil Barlow o kyberprostoru jako o aktuálním spojení mezi počítačem a telekomunikačními sítěmi.[26] Masové rozšíření Internetu na počátku 90. let předurčilo podobu rychle se utvářejícího trhu služeb.[27] Možnosti využití Internetu k osobním i komerčním aktivitám se staly katalyzátorem technologického a společenského vývoje lidstva s dopady v rámci světové globalizace.

Překotný vývoj informačních technologií za posledních téměř sto let někteří přirovnávají k „druhé průmyslové revoluci" v historii lidstva. Zatímco první průmyslová revoluce sňala z lidí břemeno fyzicky namáhavé a nepříjemné práce, tato přinesla možnosti zpracování velkého kvanta informací při fenomenální rychlosti.[28] Informační technologie, podobně jako parní stroje, umožnily nové využití energie. Stroje nyní představují počítačová zařízení a zpracovaná energie je promítána ve virtuálním prostředí.

Jakmile se připojení k Internetu stalo široce dostupné,[29] téměř každý získal možnost účastnit se rozsáhlé výměny informací ve virtuální realitě kyberprostoru, kde spolu

19 Podrobněji nález Ústavního soudu ČR ze dne 15. 5. 2012, sp. zn. II. ÚS 171/12, bod 19. Ke kolizi ochrany soukromí, informačního sebeurčení v profesní sféře a práva veřejnosti na informace významné pro posouzení nezávislosti soudce srov. nález Ústavního soudu ČR ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05, bod 34 a násl.

20 Yar, M. *Cybercrime and society: crime and punishment in the information age.* 2. vyd. Thousand Oaks 2013, str. 7.

21 Rozsudek ESLP ze dne 1. 12. 2015, stížnost č. 48226/10 a 14027/11, bod 51.

22 Jako soukromé aktivity lze chápat soukromé internetové stránky, self-posting, blogy a sociální sítě. Blíže viz stanovisko generálního advokáta Michala Bobka ve věci C-194/16 *(Bolagsupplysningen OÜ Ingrid Ilsjan proti Svensk Handel AB)*, bod 67.

23 Lessig, L. *Code. Version 2.0.* New York 2006, str. 2.

24 Zrod kybernetiky je spjat s rokem 1948, ve kterém vydal Norbert Wiener ve Spojených státech amerických své dílo *Cybernetics, or Control and Communication in the Animal and Machine*, tedy Kybernetika čili řízení a komunikace u živočichů a ve stroji. Jde o vědu čerpající především z poznatků matematiky, biologie a neurofyziologie. Kybernetika také podnítila rozvoj informatiky. Viz Knapp, V. a kol. *Právo a informace.* Praha 1988, str. 14 a násl.

25 Smejkal, V., c. d., str. 34.

26 Barlow, J. P. Crime and Puzzlement: in advance of the law on the electronic frontier. *Whole Earth Review*, 1990, str. 44–57.

27 Castells, M. *The internet galaxy: reflections on the internet, business, and society.* Oxford 2003.

28 Halton, J. The anatomy of computing. In: Forester, T. (ed.). *The Information technology revolution,* Cambridge, Mass., 1985.

29 V roce 2013 bylo k Internetu připojeno přes 2,7 bilionu obyvatel světa, tj. asi 40 % světové populace. Rozvojové země rychle dohánějí zbytek světa – počet jejich obyvatel připojených k Internetu se v letech 2009 až 2013 zvýšil o 27 %. Broadhurst, R. – Grabosky, P. – Alazab, M. – Bouhours, B. – Chon, S. – Da, Ch. Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. In: *SSRN* [online]. 2013, str. 2. Dostupné na <http://ssrn.com/abstract=2211842>.

komunikují počítačová zařízení díky přenosu dat. Počítačová data vždy nesou určitou informaci. V některých případech jí porozumí pouze stroj, v jiných jedině lidská mysl. Člověk vidí v textu především smysl plynoucí z jednotlivých slov, slovních spojení i specifik dané situace a prostředí. Systémy výpočetní techniky primárně identifikují formální vlastnosti textu. Mezi formálními a sémantickými vlastnostmi textu však existují složité vztahy. Počítač (stroj) je schopen porozumět textu především v rámci, který mu člověk předem určí.[30] U lidí je ovšem sémantické pochopení textu ryze individuální, utvářené světonázorem a životní zkušeností. Těžko si lze představit, že tuto část vnitřní psychiky bude někdy možné přenést na stroj. I u stroje však nalézáme obdobu životní zkušenosti. Stroj je schopen zlepšit svůj výkon skrze učení z operací prováděných v minulosti. V dnešní době jsou algoritmy založené na strojovém učení běžně využívány v komerční i nekomerční oblasti (internetové vyhledávače, fenomén big data,[31] rozpoznání biometrických údajů, detekce podvodných finančních operací),[32] strojové učení může hrát významnou roli na poli bezpečnosti při detekci potenciálně nebezpečného chování lidí i strojů. Ač může algoritmus při dobrém výkonu produkovat podobné výsledky, jaké by v obdobné situaci učinil člověk,[33] na poli sémantického porozumění textu existuje vzhledem k individualitě lidské mysli teoreticky nepřeberné množství výsledků. Skutečným přelomem ve výzkumu umělé inteligence bude objev počítače schopného učit se z komunikace s lidmi a přinášet zcela nové výstupy, nikoli kompiláty dříve zadaných parametrů.[34]

Bez ohledu na stoupající výskyt aktivit počítačových systémů zůstává Internet primárně prostorem lidské interakce.[35] Architektura propojené sítě mu zajistila vysokou odolnost vůči kontrole ze strany jednotlivce i státu.[36] Ačkoli se právo zabývá regulací informací již několik staletí,[37] o počítačová data se právní věda začala zajímat až v průběhu 20. století díky kybernetice a rozvoji informačních a komunikačních technologií.[38]

Již na sklonku 80. let 20. století spatřoval Cejpek v kybernetické komunikaci, nastupující po rukopisech a tisku, tj. řečové a dokumentové komunikaci, poslední fázi vývoje komunikace lidské společnosti.[39] V kybernetické fázi lidské komunikace se rapidně zvyšuje množství informací, k nimž má člověk přístup, což klade vysoké nároky na schopnost kritické analýzy při jejich využití nejen jednotlivci, ale i veřejnou mocí. Snahy předpovědět chování jednotlivce či skupiny obyvatel v různých oblastech života z dostupných informací zpracovaných počítačovou metodou mohou vést k zavádějícím výsledkům, jejichž správnost (zatím) neumíme ověřit. Problematické nejsou jen falešné zprávy nebo podvodné obchodní nabídky, ale i chybné závěry z pravdivých údajů v oblasti pojišťovnictví, zdravotnictví či bezpečnosti, které mohou mít negativní dopady na jednotlivce, skupiny obyvatel i stát.[40]

Není to pouze aktivita zákonodárce, co přímo i nepřímo mění podobu kybernetického prostředí a ovlivňuje v něm efektivitu právních norem. Podle Lessiga neřídí vztahy v kyberprostoru právní norma, nýbrž kód.[41] Značnou část řídicího kódu vytvářejí ti, kdo určují technický způsob zpracování dat, poskytovatelé služeb informační společnosti.[42] Podle Abelovského technologie ovlivňuje chování subjektů v kyberprostoru tím, že formuje nejen chápání příkazů a zákazů, ale i hodnotových otázek v právu.[43] Technologie může ovlivnit podobu právní regulace

30 Podrobněji Knapp, V. a kol., c. d., str. 47–48.
31 Pojem „big data" označuje databáze velkých objemů dat, ať již strukturovaných, či nikoli, které jsou personalizované, pseudonymizované či anonymizované. Blíže Kasl, F. Internet věcí a ochrana dat v evropském kontextu. *Revue pro právo a technologie* [online], 2016, č. 13, str. 116. Dostupné na <https://journals.muni.cz/revue/article/view/4946>.
32 Witten, I. H. – Frank, E. *Data mining: practical machine learning tools and techniques*. 2. vyd. Amsterodam 2005.
33 Surden, H. Machine Learning and Law. *Washington Law Review*, 2014, sv. 89, č. 1, str. 87 a násl. Dostupné též na <https://ssrn.com/abstract=2417415>.
34 Srov. např. rozhovor s Tomášem Mikolovem, výzkumníkem na poli umělé inteligence: Němečková, H. – Mareš, M. Nevěřící Tomáš. *Forbes Česko. Speciální edice*, 2018, str. 76–85.
35 Awan, I. – Blakemore, B. (eds.). *Policing cyber hate, cyber threats and cyber terrorism.* Farnham 2012, str. 5.
36 Na konci 60. let byla ve Spojených státech amerických pro účely vojenské komunikace vyvinuta síť ARPANET (Advanced Research Projects Agency Network), spojující pracoviště některých univerzit s vládními agenturami. Technologie této sítě umožnila rozdělit sdílenou informaci na jednotlivé pakety dat, které se nejrůznějšími cestami dostaly až k adresátovi. Právě variabilita možných cest zajistila síti vysokou odolnost. Yar, M., c. d., 2013, str. 7.
37 Srov. cenzuru, propagandu či ochranu duševního vlastnictví. Viz Polčák, R. Informace a data v právu. *Revue pro právo a technologie* [online], 2016, č. 13, str. 73. Dostupné na <https://journals.muni.cz/revue/article/view/4946>.
38 Knapp, V. a kol., c. d., str. 14 a násl.
39 V poslední fázi se zároveň všechna předchozí komunikační období kumulují. Podrobněji Knapp, V. a kol., c. d., str. 7–10.
40 Zajímavý je transparentní přístup k systému automatizované predikce lidského chování, o němž pojednává Tal Zarsky. Srov. Zarsky, T. Transparent Predictions. *University of Illinois Law Review*, 2013, sv. 2013, č. 4, str. 1503 a násl. Dostupné na <https://ssrn.com/abstract=2324240>.
41 Blíže Lessig, L., c. d.
42 Polčák, R. *Internet*, str. 107 a násl.
43 Abelovský, T. Počítač ako sudca. *Revue pro právo a technologie* [online], 2016, č. 14, str. 34. Dostupné na <https://journals.muni.cz/revue/article/view/6119>.

kyberprostoru i zpětně, reaguje-li právo na technologický vývoj novelizací norem. Jedním z největších problémů regulace transakcí ve virtuálním prostředí však bývá pozdní reakce legislativy na technologický pokrok.[44]

Šíření informací ve virtuálním prostředí a jeho překážky

Koncept prostředí neomezeného hranicemi států představuje pro právní vědu oříšek po několik desetiletí. Právní norma působí v kyberprostoru specificky a mnozí přirovnávají kyberprostor k minovému poli.[45] Počítačová zařízení, která se nacházejí po celém světě, umožňují interakci různých skupin osob, které díky technologii sítě vytvářejí nové informace a ovlivňují způsob jejich šíření. Aktéři virtuálního prostředí tak mohou být nejen příjemcem, nýbrž i zdrojem informace.[46]

Výkon práva šířit a přijímat informace ve virtuálním prostředí závisí na mnoha společenských faktorech, ať technických, právních, či psychologických, které se neustále vyvíjejí. Zásadní vliv na šíření a přijímání informací má architektura vzájemně propojených počítačových sítí[47] a chování poskytovatelů služeb informační společnosti,[48] vytvářející technické předpoklady šíření dat po síti. Podstatný dopad má i podoba mezinárodní a národní právní úpravy a rozhodovací praxe orgánů veřejné moci na konkrétním území, která se často liší. Například v Evropské unii je aplikace sekundárního práva členskými státy v oblasti online obchodování s digitálními službami značně různorodá.[49] Vedle technických a právních předpokladů nelze opomenout ani vliv schopností a znalostí uživatelů. Ti jsou nejen koncovými příjemci, ale čím dál častěji i autory nových informací a manažery informací již existujících.

Zmíněné faktory se vzájemně ovlivňují. Provázáním chování poskytovatelů služeb informační společnosti s chováním samotných uživatelů vznikají další možnosti filtrace informací ve virtuálním prostředí. Poskytovatelé internetového připojení, kteří jsou zprostředkovateli informací ve virtuálním prostředí, umožňují nastavit filtraci hledaného obsahu Internetu. Rodiče i pedagogové tak mohou zamezit dětem přístup k nevhodnému materiálu ve virtuálním prostřední.[50] Zatímco lze takové chování v mezích výkonu rodičovské odpovědnosti považovat za bezproblémové, blokace šíření informací ve virtuálním prostředí ze strany uživatele s administrátorskými právy, považuje-li určité informace za nevhodné či škodlivé (aniž by musely být protizákonné), již představuje pro svobodný přístup k informacím určité riziko, zejména pokud omezení práva na informace není přiměřené kolidujícímu zájmu, kterým může být ochrana mravnosti či veřejné morálky, a nemají-li ostatní uživatelé možnost domoci se objektivního posouzení blokace nebo se o blokaci vůbec dozvědět.

Šíření informací ve virtuálním prostředí mohou bránit obdobné překážky jako v offline světě. Schopnosti a vlastnosti příjemců informací bývají stejné. Jestliže jsou tak například informace šířeny jen v určitých jazykových verzích, aniž by automatizovaný překladač nabízel kvalitní a uživatelsky jednoduchou variantu srozumitelného získání informace z cizojazyčného textu, může být překážkou i jazyková bariéra uživatelů.[51] V souvislosti s vývojem automatizovaných překladů a širokou paletou jazyků, ve kterých jsou běžně informace zveřejňovány, lze však předpokládat pokles významu této překážky, neboť informace zveřejněné na Internetu budou kdekoli na světě nejen okamžitě dostupné, nýbrž i srozumitelné.[52]

Technologické překážky šíření informací ve virtuálním prostředí plynou z architektury daného virtuálního prostředí a z jednání poskytovatelů služeb informační společnosti. Nefunkční připojení k síti nebo blokace online služby jsou překážkou znemožňující v danou chvíli pro konkrétní počítačový

---

44 Van Cleynenbreughel, P. The European Commission's Geo-blocking Proposals and the Future of EU E-commerce Regulation. *Masaryk University Journal of Law and Technology*, 2017, č. 11, str. 56.

45 Polčák, R. – Škop, M. – Macek, J. *Normativní systémy v kyberprostoru: úvod do studia*. Brno 2005, str. 5.

46 Aktivní participace na sociálních sítích a různých komunikačních platformách na Internetu je přitom z psychologického hlediska pro uživatele virtuálního prostředí výhodná, neboť zlepšuje jeho sebehodnocení a pocit kontroly. Blíže Jeeyun, O. – Saraswathi, B. – Sundar, S. S. Clicking, Assessing, Immersing, and Sharing: An Empirical Model of User Engagement with Interactive Media. *Communication Research* [online], 2015. Dostupné na <https://doi.org/10.1177/0093650215600493>. Xu, Q. – Sundar, S. S. Interactivity and memory: Information processing of interactive versus non-interactive content. *Computers in Human Behavior* [online], 2016, sv. 63, str. 620–629. Dostupné na <www.sciencedirect.com/science/journal/07475632/63/supp/C>.

47 Blíže Smejkal, V., c. d., str. 45 a násl.

48 Polčák, R., *Informace*, str. 67–91.

49 Van Cleynenbreughel, P., c. d., str. 55–56.

50 Lessig, L. – Resnick, P. Zoning Speech on the Internet: A Legal and Technical Model. *Michigan Law Review*, 1999, str. 416 a násl. Dostupné na <https://cyber.harvard.edu/wg_home/uploads/200/1999-06.pdf>.

51 Obtížně se lze dostat např. k platné a účinné právní úpravě mnoha cizích států, a to nejen k samotnému překladu právního předpisu, nýbrž přímo i k národnímu automatizovanému systému, který umožňuje aktuálně platnou oficiální verzi vyhledat.

52 K poklesu významu neznalosti konkrétního jazyka zveřejněné informace viz stanovisko generálního advokáta Michala Bobka ve věci C-194/16 *(Bolagsupplysningen OÜ Ingrid Ilsjan proti Svensk Handel AB)*, bod 76.

systém jakýkoli přenos dat, tedy i informací. K blokaci připojení či online služby může dojít ve vztahu ke konkrétnímu uživateli i plošně vůči všem, kteří se připojí k síti skrze IP adresu charakterizovanou vztahem k určitému území.

Právní norma může znemožnit šíření informací ve virtuálním prostředí toliko nepřímo, neboť jejím cílem je dosáhnout požadovaného chování subjektů právních vztahů a bránit jejich nežádoucímu chování. Právo tak může vykonávat svůj vliv na šíření informací ve virtuálním prostoru pouze snahou působit na veškeré subjekty, které ovlivňují informační svobodu v kyberprostoru, a to buď hrozbou sankcí, či naopak poskytnutím určité výhody. Adresátem právních norem regulujících virtuální prostředí by měli být všichni aktéři virtuálního prostředí, tj. tvůrci architektury kyberprostoru, poskytovatelé služeb informační společnosti, jednotlivé státy mezinárodního společenství, i koncoví uživatelé.

Způsob, jakým právo přistupuje k regulaci informací ve virtuálním prostředí, ovlivňuje i právní kultura, tradiční hodnoty či náboženství dané země. Informace lze členit do mnoha různých kategorií a na příkladu regulace svobody projevu lze zřetelně poznat odlišnou právní praxi států. To, co je v jedné jurisdikci vnímáno jako součást svobodného projevu, se v jiné považuje za nedovolený projev porušující práva politických, náboženských a jiných skupin. Zatímco zveřejnění jedné informace bude na území Spojených států amerických chráněno prvním dodatkem k Ústavě, stejná informace bude v Německu považována za propagaci nacistické ideologie. Virtuální prostředí však vytváří jediný prostor bez státních hranic a postih osoby, která v něm zveřejní a dále šíří konkrétní informaci v rozporu s národním právním řádem, je obtížný.[53]

Podle Lessiga a Resnicka by právo mělo motivovat jednotlivé aktéry ve virtuálním prostředí, tj. odesílatele, příjemce i zprostředkovatele informací, k poskytnutí nezbytných údajů za účelem určení, zda bude výměna informací blokována, či nikoli. Dostatečnou motivací je obvykle vznik odpovědnosti aktéra za opomenutí blokovat informaci, jejíž šíření je protizákonné. Právo by mělo rovněž stanovit základní pravidlo pro hraniční případy, ve kterých nelze okamžitě určit, zda jde, či nejde o nezákonný obsah. Jelikož Lessig a Resnick rozdělují jednotlivé aktéry ve virtuálním prostředí na odesílatele, příjemce a zprostředkovatele, soustředí se i na vymahatelnost práva u těchto subjektů. Základní otázkou vymahatelnosti práva ve virtuálním prostředí přitom je, jak snadno lze dosáhnout cíle regulace právními prostředky. Zatímco příjemců informací je ve virtuálním prostředí mnohem více než odesílatelů, odesílatelé informací se často nacházejí mimo jurisdikci státu prosazujícího právní normu, a tudíž jsou jeho právními nástroji prakticky neregulovatelní. Jako mnohem snazší a levnější cesta se proto jeví regulovat příjemce informací, potažmo zprostředkovatele výměny, kteří jsou v dosahu jurisdikce daného státu.[54] I pro státy je obvykle nejsnazší podrobit právní regulaci zprostředkovatele informací, typicky poskytovatele internetového připojení. Ačkoli zprostředkovatelé vědí o charakteru informace a její potenciální protizákonnosti nejméně (na rozdíl od odesílatele a příjemce informace), jsou pro státní orgány nejsnáze dosažitelní: jejich počet je mnohem menší než počty příjemců a odesílatelů a s relativní stálostí sídlí na území jednoho státu.[55] Zprostředkovatelé výměny informací podléhají dozoru orgánů státní správy a poskytování služeb informační společnosti v souladu s právní úpravou státu sídla bývá v jejich zájmu.

Limity práva šířit a přijímat informace ve virtuálním prostředí vyplývající z mezinárodního a evropského práva

Právo svobodně šířit a přijímat informace je zásadní součástí široce pojatého práva na svobodu projevu. Podle Matejky představuje toto právo nástroj *sui generis* k hledání spravedlivé rovnováhy mezi svobodou jednotlivce a jeho povinnostmi, když se jako univerzální právní princip dostává do konfliktu s jinými hodnotami a chráněnými zájmy. Díky konfliktům plní právo na svobodu projevu svůj účel a smysl. Ve virtuálním prostředí dochází ke střetům chráněných zájmů stále častěji,[56] neboť toto prostředí usnadňuje komunikaci mezi nejrůznějšími osobami a násobí příležitosti ke konfliktům, které se běžně odehrávají offline. Ve virtuálním prostoru

53 Lessig, L. – Resnick, P., c. d., str. 395–396.
54 Tamtéž, str. 401–403.
55 Tamtéž, str. 413–415.
56 Matejka, J., c. d., str. 37–38.

neexistuje příliš velká vzdálenost dvou míst,[57] je možná interakce při neznalosti adresáta či příjemce a jiné kulturní či náboženské prostředí, nedostatek znalostí, prostředků i kuráže, které potenciálnímu konfliktu práv a svobod v offline světě brání, nehrají stejnou roli.[58] Počítat je nutné i se specifiky právních vztahů ve virtuálním prostředí, která se projevují v odlišném pojetí práv a svobod.[59]

Obecně lze základní lidská práva a svobody omezit buď zákonem, anebo *ad hoc* v důsledku jejich vzájemného střetu.[60] Které základní právo či svobodu bude nutno v konkrétním případě střetu upřednostnit, určují nezávislé soudní orgány. Při střetu základních práv stojících na stejné úrovni je „vždy věcí nezávislých soudů, aby s přihlédnutím k okolnostem každého jednotlivého případu pečlivě zvážily, zda jednomu právu nebyla nedůvodně dána přednost před právem druhým".[61] Ani svoboda projevu, ani právo přijímat a šířit informace nejsou neomezitelné. Listina i řada mezinárodněprávních dokumentů některá omezení předpokládají a stanoví pro ně podmínky. Právní vztahy ve virtuálním prostředí jsou také čím dál častěji předmětem rozhodovací činnosti nadnárodních soudních institucí a předmětem mezinárodních debat o budoucí podobě právní regulace. Z rozhodovací činnosti Evropského soudu pro lidská práva, Soudního dvora Evropské unie i Výboru Organizace spojených národů pro lidská práva[62] lze vyvodit řadu základních principů, pravidel i doporučení pro přípustné omezení práva svobodného šíření informací a přístupu k nim ve virtuálním prostředí.

Mezinárodní pakt o občanských a politických právech a závěry Výboru Organizace spojených národů (OSN) pro lidská práva

Článek 19 Mezinárodního paktu o občanských a politických právech[63] (dále též „Pakt") přiznává každému právo zastávat svůj názor bez překážky, jakož i právo na svobodu projevu, které zahrnuje svobodu vyhledávat, přijímat a rozšiřovat informace a myšlenky všeho druhu, bez ohledu na hranice, ať už ústně, písemně nebo tiskem, prostřednictvím umění, nebo jakýmikoli jinými prostředky podle vlastní volby. Článek 19 odst. 3 Paktu však zdůrazňuje aspekt zodpovědnosti a předpokládá nutná omezení, která mohou být ovšem jen taková, jaká stanoví zákon, přičemž musejí být nutná k respektování práv nebo pověsti jiných, ochraně národní bezpečnosti, veřejného pořádku, veřejného zdraví nebo morálky. Další omezení svobody projevu pak zakládá čl. 20 Paktu, který stanoví zákonný zákaz válečné propagandy, jakož i projevů národní, rasové a náboženské nenávisti představující podněcování k diskriminaci, nepřátelství nebo násilí. Na rozdíl od omezení svobody projevu dle čl. 19 odst. 3 Paktu, tj. z taxativních legitimních důvodů reagujících na konkrétní hrozbu chráněného zájmu, tedy *ex post*, dochází v případě ochrany míru a potlačování diskriminace či násilí k plošnému omezení svobody projevu *a priori*, již na základě zákona. Další možná omezení předpokládá čl. 4 Paktu, a to pro případy mimořádných, úředně vyhlášených situací, během nichž mohou smluvní státy z důvodu ohrožení života národa omezit svobodu projevu podle potřeb konkrétní situace. Výbor pro lidská práva dal ovšem najevo, že mimořádnost situace ohrožení národa bude vykládat velice restriktivně. Omezení svobody projevu tak podle něj přichází v úvahu pouze při výjimečném ohrožení života národa, kam by běžně neměly spadat živelné či průmyslové katastrofy. Omezení svobody projevu dále nesmí přesáhnout rozsah, který daná situace nutně vyžaduje, ani nesmí být diskriminační.[64]

Ochrana práv a pověsti jiných se vztahuje na individuálně určené osoby i na členy nejrůznějších komunit, a chrání tak členy společenství odlišující se od většiny okolního obyvatelstva svou vírou, etnicitou, sexuální orientací apod. Podle postoje Výboru pro

[57] Nenachází-li se počítač příliš daleko od dosahu připojení k wi-fi.

[58] Podrobnému rozboru vlastností virtuálního prostředí ve vztahu k proměně lidského jednání, zejména při páchání trestné činnosti, se věnují například Bert-Jaap Koops a David Wall. Srov. Koops, B.-J. The Internet and Its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011. *Transnational Criminology Manual* [online], 2010, č. 1. Dostupné na <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223>. Wall, D. *Cybercrime: the transformation of crime in the information age.* Cambridge 2007, str. 30–51.

[59] Patrně k nejvýraznějšímu posunu došlo v chápání práva na soukromí a pojmu soukromí vůbec. Již v roce 2001 prohlásil soudce Nejvyššího soudu Spojených států amerických Antonin Scalia, že tvrdit, že míra soukromí zůstala technickým pokrokem nedotčena, by bylo bláznovstvím. Viz *Kyllo proti Spojeným státům americkým*, 533 U.S. 27, 33-34.

[60] Holländer, P. *Základy všeobecné státovědy.* Praha 1995, str. 71.

[61] Nález Ústavního soudu ČR ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16. Svoboda projevu a právo na informace se jako základní politická práva často dostávají do konfliktu s právem na ochranu osobnosti a soukromého života.

[62] Výbor pro lidská práva (Human Rights Committee, HRC) je smluvní orgán Organizace spojených národů s mandátem posuzovat individuální stížnosti. Dalšími jsou Výbor pro odstranění rasové diskriminace, Výbor pro odstranění diskriminace žen a Výbor proti mučení.

[63] Mezinárodní pakt OSN o občanských a politických právech. Dostupné na <http://www.osn.cz/wp-content/uploads/2015/03/mezinar.pakt-obc.a.polit_.prava_.pdf>.

[64] Srov. čl. 4 Paktu. K podrobným podmínkám derogace práv srov. Výbor OSN pro lidská práva (HRC). *CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency.* 2001. Dostupné na <http://www.refworld.org/docid/453883fd1f.html>.

lidská práva musí jakékoliv omezení odpovídat striktním požadavkům nutnosti a proporcionality a musí sloužit k ochraně konkrétního legitimního cíle, pro který bylo přijato.[65] Jestliže se smluvní strany rozhodnou omezit svobodu projevu, musejí jasně a zřetelně určit konkrétní hrozbu a osvědčit i nutnost a proporcionalitu omezujícího opatření. Výbor pro lidská práva tak zdůraznil, že mezi omezením svobody projevu a existencí hrozby musí být dána jasná a přímá souvislost.[66] Přestože čl. 4 odst. 2 Paktu nezmiňuje svobodu projevu ve výčtu práv, od nichž se nelze odchýlit ani za mimořádných okolností ohrožení státu, Výbor pro lidská práva poukázal na to, že žádné ohrožení státu ve smyslu čl. 4 Paktu nemůže odůvodnit odchýlení se smluvního státu od zákazu válečné propagandy a podněcování k diskriminaci dle čl. 20 Paktu.[67]

Jakákoli omezení operací na webových stránkách, blogu či jiných informačních platformách na Internetu, včetně systémů zajišťujících internetovou komunikaci, musejí odpovídat požadavkům čl. 19 odst. 3 Paktu o omezení výkonu práva na svobodu projevu, uvedeným výše. Pod systémy zajišťující internetovou komunikaci spadají i webové prohlížeče, jako je Google Chrome, Mozilla Firefox či Internet Explorer, což jsou počítačové programy umožňující uživatelům prohlížet webové stránky podle zvolených kritérií. Řada prohlížečů však nezveřejňuje algoritmus, na jehož základě dochází k výběru výsledků vyhledávání, a kontrola legitimního zásahu do svobody vyhledávat, přijímat a rozšiřovat informace je tudíž obtížná.[68] Ve stanovisku k čl. 19 Paktu[69] poukázal Výbor pro lidská práva na skutečnost, že právo na svobodu projevu zahrnuje nejen komentování vlastních a veřejných záležitostí, umělecký či náboženský projev, ale například i politický diskurz, lobbing či komerční reklamu, a tedy se vztahuje na veškeré komunikační prostředky, včetně internetových komunikačních platforem. Smluvní strany Paktu by měly všemi dostupnými prostředky podporovat nezávislost nových médií šířených elektronickými prostředky a zaručit k nim volný přístup. V rámci publicistiky zdůraznil Výbor pro lidská práva roli nezávislých bloggerů a dalších osob, které šíří informace vlastními prostředky, ať již tiskem, či po Internetu. Jakýkoliv státní akreditační systém není proto slučitelný s podmínkami čl. 19 odst. 3 Paktu. Přistoupí-li smluvní stát k omezení informací dostupných online, mělo by se omezení týkat jen konkrétně zaměřeného, specifického obsahu, proti generickým zákazům a omezením online obsahu virtuálního prostředí se Výbor pro lidská práva výslovně staví. Praxi států aplikujících plošná omezení týkající se specifických webových stránek a informačních systémů považuje za odporující požadavkům pro omezení svobody projevu dle čl. 19 odst. 3 Paktu.[70]

Evropská úmluva o ochraně základních lidských práv a svobod a judikatura Evropského soudu pro lidská práva

Právo rozšiřovat a přijímat informace bez zásahu státních orgánů a bez ohledu na hranice zaručuje právo na svobodu projevu ve smyslu čl. 10 Úmluvy. V demokratickém právním státě musí mít omezení práva na svobodu projevu vždy zákonný základ. Šíření informace ve virtuálním prostředí může sice zamezit technologie (Lessigův kód), která je řídicím elementem virtuálního prostředí, ovšem pokud by k tomu došlo bez zákonného podkladu, jednalo by se o užití kódu v rozporu s požadavky Úmluvy pro zásah státu do práva na svobodu projevu. Kód nikdy nesmí nahradit zákonný podklad omezení práva na svobodu projevu.

Uplatnění základních lidských práv a svobod vyplývajících z Úmluvy v prostředí Internetu se věnují doporučení Výboru ministrů Rady Evropy. Jde o modelovou legislativu určenou smluvním státům, která působí svou přesvědčivostí především na politické úrovni. Výbor ministrů Rady Evropy vydal i doporučení vztahující se ke svobodnému přeshraničnímu přenosu informací na Internetu,[71] podle kterého mají smluvní státy Úmluvy

65 Výbor OSN pro lidská práva (HRC). *Communication No. 1022/2001, Velichkin v. Belarus*. Postoj přijatý dne 20. 10. 2005. Dostupné na <http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2F85%2FD%2F1022%2F2001&Lang=en>.

66 Výbor OSN pro lidská práva (HRC). *Communication No. 926/2000, Shin v. Republic of Korea*. Postoj přijatý dne 25. 4. 2000. Dostupné na <http://juris.ohchr.org/Search/Details/1107>.

67 Výbor OSN pro lidská práva (HRC). *CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency*. 2001, bod 13 písm. e). Dostupné na <http://www.refworld.org/docid/453883fd1f.html>.

68 K tomu srov. případ *KinderStart v. Google*, 2007. Rice, D. Google wins out in challenge to its website rating system. In: *International Law Office* [online]. 12. 10. 2016. Dostupné na <http://www.internationallawoffice.com/Newsletters/E-commerce/USA/Howard-Rice-Nemerovski-Canady-Falk-Rabkin/Google-Wins-Out-in-Challenge-to-its-Website-Rating-System>.

69 Výbor OSN pro lidská práva (HRC). *CCPR General Comment No. 34: Article 19: Freedoms of opinion and expression.* 2011, body 11 a 22. Dostupné na <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

70 Tamtéž, bod 43.

71 Doporučení CM/REC(2015)6 Výboru ministrů Rady Evropy ze dne 1. 4. 2015 ohledně svobodného přeshraničního přenosu informací na Internetu. Dostupné na <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20>.

garantovat každému, kdo se nachází v jejich jurisdikci,[72] právo na svobodu projevu na základě čl. 10 Úmluvy bez diskriminace vyplývající mimo jiné z příslušnosti jedince k určitému národu či národní menšině. Úmluva by měla ve virtuálním prostředí působit stejně jako mimo ně. Působnost čl. 10 Úmluvy se přitom vztahuje nejen na obsah, nýbrž i na způsob šíření informace ve virtuálním prostředí – tj. na přenos počítačových dat po síti.[73] Jakékoli omezení způsobů či metod, kterými jsou informace ve virtuálním prostředí šířeny, by nutně současně zasáhlo i právo informace svobodně přijímat a šířit. Státní politika i obchodní aktivity soukromých osob omezující poskytování online služeb nebo blokující šíření závadného obsahu v rámci jednoho státu mohou bránit volnému přenosu informací na Internetu, ať už náhodně, nebo cíleně. Takové jednání má nezřídka dopady i na území jiných států, což v krajním případě může představovat i zásah do jejich suverenity.[74] Státy však mohou omezit přenos informací v souladu s čl. 10 Úmluvy, pokud půjde o nutné omezení bez nepřiměřeného dopadu na přeshraniční přenos informací přes Internet. Doporučení Výboru ministrů Rady Evropy obsahuje i principy náležité péče *(due diligence)* pro praxi států omezující přenos informací přes Internet.[75]

Výbor ministrů Rady Evropy se zabýval rovněž filtrováním obsahu Internetu a možnými dopady filtrace na svobodu projevu.[76] Použití filtrů představuje vlastní regulaci informací přijímaných skrze virtuální prostředí ze strany uživatelů, kteří mohou v různém rozhraní blokovat obsah (informace), který uznají za nevhodný.[77] Ve vztahu k užití filtrů je stěžejním vědomí uživatelů o použití filtrace a o jejím rozsahu. Internetoví uživatelé by dle doporučení Výboru ministrů Rady Evropy měli mít i možnost zpochybnit blokaci či filtraci obsahu a žádat její objasnění a nápravu. Ve spolupráci se soukromým sektorem by státy měly zajistit i to, aby nesprávně blokovaný obsah byl v přiměřeném čase a bez zbytečných komplikací zpřístupněn.[78] Orgány veřejné moci by neměly filtrovat přenášené informace z jiných než taxativně vypočtených hledisek dle čl. 10 odst. 2 Úmluvy, v souladu s jejich výkladem Evropským soudem pro lidská práva. Konkrétní požadavky jsou určeny pro celostátní užití všeobecné blokace či filtračních mechanismů ze strany státu. K takovému opatření lze přistoupit pouze v případě specifického a jasně identifikovaného obsahu, a to poté, co kompetentní státní orgán rozhodl o protiprávnosti takového obsahu, jestliže je jeho rozhodnutí přezkoumatelné jiným nezávislým orgánem v řízení, které splňuje požadavky spravedlivého procesu ve smyslu čl. 6 Úmluvy. Státní orgán musí současně zaručit, že blokace či filtrační mechanismy budou použity v souladu s požadavky čl. 10 odst. 2 Úmluvy.[79]

Svobodný projev, včetně realizace práva přijímat a šířit informace ve virtuálním prostředí, fakticky umožňuje neomezené množství soukromých internetových platforem, v jejichž rámci působí i nezávislá média, organizace na ochranu lidských práv, političtí disidenti a jiní. Ti se ve virtuálním prostředí mohou stát i cílem kybernetických útoků.[80] Na riziko hrozící svobodě projevu i svobodě shromažďovací a sdružovací ve virtuálním prostředí ve vztahu k soukromému sektoru online služeb upozorňuje deklarace Výboru ministrů Rady Evropy ze dne 7. 12. 2011.[81]

I Evropský soud pro lidská práva (dále též „ESLP") již poukázal na skutečnost, že čím dál větší objem informací a služeb je dostupný

---

72 Termín „jurisdikce" je zde užit v užším slova smyslu, tzn. jako pravomoc státu uplatňovaná na určitém území za aplikace jeho norem místní působnosti. Srov. Táborová, A. Veřejnoprávní ochrana informační společnosti v místní působnost práva. *Revue pro právo a technologie*, 2010, č. 1, str. 33.

73 Srov. hosting, online službu spočívající v uložení a zprostředkování počítačových dat poskytovatelem služby bez jejich znalosti.

74 Srov. body 1 až 4 doporučení CM/REC(2015)6 Výboru ministrů Rady Evropy ze dne 1. 4. 2015 ohledně svobodného přeshraničního přenosu informací na Internetu. Dostupné na <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f20>.

75 Srov. pravidla 1.2 a 2 tamtéž.

76 Doporučení CM/REC(2008)6 Výboru ministrů Rady Evropy ze dne 26. 3. 2008 ohledně opatření na podporu dodržování svobody projevu a informací ve vztahu k internetovým filtrům. Dostupné na <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4>.

77 Filtry jsou efektivním a rozšířeným nástrojem především na poli rodičovské ochrany dětí před nevhodným obsahem na Internetu, ale i ve vztahu k blokaci nevyžádané reklamy a zpráv.

78 Srov. bod I doporučení CM/REC(2008)6.

79 Srov. bod III tamtéž; shodně též 3. princip v deklaraci Výboru ministrů Rady Evropy ohledně svobody komunikace na Internetu ze dne 28. 5. 2003. K použití filtrace a uplatnění zásady nediskriminace ve vztahu k sociálním platformám srov. doporučení CM/REC(2012)4 Výboru ministrů Rady Evropy ze dne 4. 4. 2012 ohledně ochrany lidských práv ve vztahu ke službám sociálních sítí. Dostupné na <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b>.

80 Nejčastěji jde o útok typu DDOS (z anglického termínu „distributed-denial-of-service attack"), tedy o řízený útok velkého množství počítačových zařízení na konkrétní místo v síti za pomoci obrovského množství požadavků k přístupu v jeden okamžik. Důsledkem DDOS útoku dochází k přetížení a k zablokování webové stránky či serveru a oprávněným uživatelům internetové služby (serveru) je přístup k ní znemožněn.

81 Deklarace Výboru ministrů Rady Evropy ze dne 7. 12. 2011 o ochraně svobody projevu a svobody shromažďovací a sdružovací ve vztahu k soukromě provozovaným internetovým platformám a poskytovatelům online služeb. Dostupné z <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb844>.

pouze skrze Internet.[82] Informace přístupné skrze Internet, který plní klíčovou úlohu v realizaci práva na informace, proto spadají pod ochranu čl. 10 Úmluvy.[83] Internet hraje v každodenním životě obyvatel mnoha zemí zásadní roli. Čím dál tím více států i mezinárodních institucí vnímá přístup k Internetu jako základní právo, neboť Internet fakticky umožňuje výkon mnoha základních lidských práv a svobod, které Úmluva garantuje.[84] Právo přijímat informace dokonce vykládá ESLP v tom smyslu, že je v zásadě zakázáno státním orgánům, aby zamezily přístup k informaci, kterou jiní zveřejnili právě za účelem jejího šíření.[85] Tento požadavek má pro virtuální prostředí zásadní význam, nutně však musí jít ruku v ruce i s jasným vymezením odpovědnostních vztahů v případě porušení práv a oprávněných zájmů jiných osob. Orgány veřejné moci musejí mít současně dostatečné prostředky k tomu, aby mohly dalšímu šíření informace zamezit, dostane-li se do konfliktu s veřejným zájmem. Obdobným způsobem by měla být ve virtuálním prostředí poskytována ochrana i oprávněným zájmům soukromým.

Podle dosavadní judikatury se ESLP nebrání myšlence činit zprostředkovatele informací ve virtuálním prostředí odpovědnými za zákonnost šířených informací na webových platformách, jde-li o zprostředkovatele zpravodajství (provozovatele zpravodajských portálů), zejména tehdy, profitují-li z množství komentářů uživatelů a z návštěvnosti webu.[86] Internet však na druhou stranu poskytuje nové možnosti pro fungování demokracie tím, že přispívá k výměně názorů mezi občany. Dalo by se říci, že klíčovou složku demokracie v prostředí Internetu tvoří zejména komentáře,[87] které jsou esencí svobody projevu ve virtuálním prostředí. Ty z projevů ve virtuálním prostředí, které nejsou slučitelné se zásadami, z nichž Úmluva vychází, však s ohledem na zákaz zneužití práva podle čl. 17 Úmluvy nemohou požívat ochrany dle čl. 10 Úmluvy. ESLP jasně stanovil, že za takové projevy považuje bez dalšího popírání holokaustu, ospravedlňování pronacistické politiky či ztotožňování všech muslimů s původci závažných teroristických činů.[88]

V případě omezení práva na informace ze strany státních orgánů, kdy dochází ke snaze zamezit šíření informace ve virtuálním prostředí, musejí státy zvážit, zda je určitá „virtuální blokace" informace přiměřená a ospravedlnitelná. Zásah státu by měl být menší tam, kde blokace přístupu k webové stránce znemožní zúčastnit se debaty o veřejném zájmu.[89] V tomto ohledu však nelze směšovat blokaci webových stránek, které porušují autorská práva, tj. blokaci v ryze obchodním zájmu, s blokací webových stránek usilující o zamezení šíření politicky nežádoucího obsahu. ESLP se jasně vyjádřil, že využívá-li osoba aktivně určitou webovou platformu k šíření a studiu informací, dochází plošnou blokací takové platformy státem k zásahu do veřejného subjektivního práva osoby, práva na svobodu projevu ve smyslu čl. 10 Úmluvy.[90] Webovou stránku YouTube označil ESLP za unikátní a zásadní nástroj umožňující přijímat a sdílet myšlenky a názory ostatních bez ohledu na to, co publikují tradiční média ve státě. Pokud dojde na základě administrativního rozhodnutí k plošnému zamezení přístupu k takové platformě, jakou je web YouTube, lze považovat všechny její aktivní uživatele za osoby, jejichž práva přiznaná Úmluvou a protokoly k ní byla porušena ve smyslu čl. 34 Úmluvy.[91]

V případě kolize svobody projevu dle čl. 10 Úmluvy s jiným soukromým zájmem, například s právem na ochranu soukromí a rodinného života dle čl. 8 Úmluvy, zdůraznil ESLP potřebu vyvažování: zásah do soukromého života musí nabýt takové intenzity, aby omezení svobody projevu odůvodnil i v prostředí Internetu. Přitom se zdá, že přítomnost hanlivých komentářů v internetových diskusích hodnotí ESLP jako čím dál běžnější jev, a zásah do soukromého života v prostředí internetové diskuse nemusí vždy dosáhnout oné potřebné míry intenzity.[92]

82 Rozsudek ESLP ze dne 16. 1. 2016, *Kalda v. Estonia*, č. 17429/10, bod 52.
83 Rozsudek ESLP ze dne 10. 3. 2009, *Times Newspapers Ltd v. United Kingdom*, č. 3002/03 a č. 23676/03, bod 27.
84 Rozsudek ESLP ze dne 17. 1. 2017, *Jankovskis v. Lithuania*, č. 21575/08, bod 62.
85 Rozsudek ESLP ze dne 16. 1. 2016, *Kalda v. Estonia*, č. 17429/10, body 41 a 42.
86 Rozsudek ESLP ze dne 16. 6. 2015, *Delfi AS v. Estonia*, č. 64569/09.
87 Odlišné stanovisko soudců Sajó a Tsotsoria z rozsudku ESLP ze dne 16. 6. 2015, *Delfi AS v. Estonia*, č. 64569/09.
88 Rozhodnutí ESLP ze dne 20. 2. 2007, *Pavel Ivanov v. Russia*, č. 35222/04.
89 Rozsudek ESLP ze dne 10. 1. 2013, *Ashby Donald and Others v. France*, č. 36769/08.
90 Rozsudek ESLP ze dne 1. 3. 2016, *Cengíz and others v. Turkey*, č. 48226/10 a č. 14027/11, body 50 a 54. Rozsudek ESLP ze dne 18. 12. 2012, *Ahmet Yildirim v. Turkey*, č. 3111/10, bod 51.
91 Rozsudek ESLP ze dne 1. 3. 2016, *Cengíz and others v. Turkey*, č. 48226/10 a č. 14027/11, body 52 až 53.
92 Usnesení ESLP ze dne 7. 2. 2017, *Pihl v. Sweden*, č. 74742/16. Rozsudek ESLP ze dne 16. 6. 2015, *Delfi AS v. Estonia*, č. 64569/09. V případě stále se objevujících hanlivých komentářů však lze využít další ze zaručených práv v prostředí Internetu, a sice právo „být zapomenut" tak, jak jej shledal Soudní dvůr Evropské unie v rozsudku ze dne 13. května 2014, *Google Spain a Google*, C-131/12.

Zaručuje Úmluva v rámci práva na přístup k informacím každému i právo na přístup k Internetu?[93] Měl by mít každý právo ke „vstupu" do virtuálního prostředí, které je stále zásadnější pro vznik, šíření a přijímání nejrůznějších informací? V případu *Jankovskis*[94] se ESLP zabýval vyvažováním práva na přístup k Internetu vůči bezpečnostnímu riziku, které vyplývalo pro stát z poskytnutí neomezeného přístupu k počítačové síti osobám ve výkonu trestu odnětí svobody. V projednávaném případu se stěžovatel, který vykonával trest odnětí svobody v litevském vězení, domáhal přístupu na Internet, aby získal informaci, jež byla zveřejněna pouze na webových stránkách litevského ministerstva školství. Jednalo se přitom o veřejně dostupnou informaci, navíc šířenou orgánem státní moci. Přestože ESLP zdůraznil, že Internet plní důležitou roli při zpřístupňování informací široké veřejnosti, uvedl, že není možné vykládat čl. 10 Úmluvy ve smyslu povinnosti státu garantovat vězňům přístup na Internet. Ve vztahu k vězeňské populaci existují určitá omezení právě v jejím přístupu k Internetu. Jestliže však národní právní řád garantuje všem bez rozdílu přístup k určitému typu informací,[95] pak odmítnutí zpřístupnění takové informace skutečně znamená porušení práva přijímat informace podle čl. 10 Úmluvy. Podle ESLP měl orgán veřejné moci zvažovat, zda nelze bezpečnostní riziko v daném případě překonat, například omezeným přístupem vězňů k Internetu.[96] Z citovaného rozhodnutí tedy lze dovodit, že ESLP nepovažuje právo na přístup k Internetu za právo zaručené všem osobám bez rozdílu. Stěžejním zůstává pro ESLP konkrétní charakter informace, kterou osoba požaduje. Jestliže konkrétní informace garantuje (vnitrostátní) právní řád a tyto informace jsou dostupné veřejnosti pouze skrze Internet, pak by měl stát zaručit i přístup k Internetu, alespoň v rozsahu umožňujícím seznámit se s danými informacemi. S digitalizací veřejné správy však lze očekávat odklon od hlediska charakteru informace a příklon k požadavku všeobecného přístupu k Internetu pro každého.

Judikatura Soudního dvora Evropské unie

V Evropské unii (dále též „EU") lze na problematiku svobodného šíření informací prostřednictvím Internetu nahlížet z hlediska principu volného pohybu služeb. Článek 56 Smlouvy o fungování EU (dále též „SFEU") zakazuje omezit volný pohyb služeb uvnitř EU pro státní příslušníky členských států usazené v jiném členském státě, než se nachází příjemce služeb. Dle čl. 2 směrnice 2000/31/ES o elektronickém obchodu nemohou členské státy z důvodů spadajících do koordinované oblasti omezovat volný pohyb služeb informační společnosti z jiného členského státu. Za omezení svobody poskytování služeb v jiných členských státech je nutné považovat všechna opatření, která jeho výkon zakazují, brání mu nebo jej činí méně atraktivním.[97] Z judikatury Soudního dvora EU (dále též „SDEU") vyplývá, že zakazuje-li právní úprava členského státu EU poskytovatelům usazeným v jiných členských státech nabízet prostřednictvím Internetu na jeho území služby, jde o omezení volného pohybu služeb v podobě, v jaké jej zaručuje čl. 56 SFEU,[98] neboť v takovém případě dochází k omezení svobody rezidentů z dotčeného členského státu využívat prostřednictvím Internetu služeb nabízených v jiných členských státech.[99]

Podle čl. 52 a čl. 62 SFEU lze volný pohyb služeb v EU omezit, je-li to nutné z hlediska veřejného pořádku, veřejné bezpečnosti nebo ochrany zdraví. Z judikatury SDEU vyplývají konkrétní výjimky z principu volného pohybu služeb ve virtuálním prostředí. Musí jít o naléhavé důvody plynoucí z veřejného zájmu, jako jsou např. ochrana spotřebitelů, předcházení podvodům či podněcování k nadměrným výdajům za hru. Ani v těchto případech však nesmějí členské státy přistoupit k diskriminačním opatřením na základě státní příslušnosti.[100] Blokace přenosu online služeb provozovaných z jiného členského státu by neměla být v rozporu s čl. 56 SFEU, může-li je z důvodu ochrany veřejného zájmu nabízet v daném státě jediný poskytovatel,

93 Mezi prvními státy, které uznaly samostatné právo na přístup k Internetu v rámci širšího pojetí základních lidských práv, bylo Finsko, následované Estonskem. I francouzský Ústavní tribunál ve svém rozhodnutí zrušil právní úpravu, na jejímž základě bylo možné uživatele odpojit na omezenou dobu od Internetu z důvodu porušení autorských práv, s poukazem na to, že právo na přístup k Internetu je již třeba považovat za nezcizitelné občanské právo. Viz Kokeš, M. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In: Šimíček, V. (ed.). *Právo na soukromí*, Brno 2011, str. 128.

94 Rozsudek ESLP ze dne 17. 1. 2017, *Jankovskis v. Lithuania*, č. 21575/08.

95 V projednávaném případě zaručoval litevský právní řád všem občanům přístup k informacím o možnostech dalšího vzdělávání.

96 Rozsudek ESLP ze dne 17. 1. 2017, *Jankovskis v. Lithuania*, č. 21575/08, body 54 až 62.

97 Rozsudky SDEU ze dne 20. 2. 2001, *Analir a další*, C-205/99, bod 21, ze dne 15. 1. 2002, *Komise v. Itálie*, C-439/99, bod 22, ze dne 8. 9. 2009, *Liga Portuguesa de Futebol Profissional a Baw International*, C-42/07, bod 51.

98 Rozsudky SDEU ze dne 6. 11. 2003, *Gambelli a další*, C-243/01, bod 54, ze dne 8. 9. 2009, *Liga Portuguesa de Futebol Profissional a Baw International*, C-42/07, bod 52.

99 Rozsudek SDEU ze dne 8. září 2009, *Liga Portuguesa de Futebol Profissional a Baw International*, C-42/07, bod 53.

100 Stanovisko generálního advokáta SDEU Macieje Szpunara ve věci C-49/16, bod 39.

který podléhá přísné státní kontrole.[101] Blokaci internetových stránek poskytovatelů nelegálních online služeb na základě rozhodnutí správního orgánu neshledal protiústavní ani český Ústavní soud.[102] Existence povolovacího řízení před národním správním orgánem, na jehož základě mohou být v členském státě poskytovány online služby, zakládá přípustné omezení volného pohybu služeb (bez ohledu na vydání či nevydání správního povolení), jestliže k němu dochází na základě legitimního důvodu. Orgány veřejné moci, které povolují poskytování internetových služeb (typicky v koncesním řízení), musejí vést řízení transparentním způsobem, dodržovat zásady rovného zacházení a především zásadu zákazu diskriminace na základě státní příslušnosti.[103] Pokud by národní právní úprava stanovila pro poskytovatele internetových služeb usazených na území jiných členských států nepřímo diskriminační podmínky, jde o porušení čl. 56 SFEU.

Z judikatury SDEU plynou pro virtuální prostředí i jasná omezení šíření informací porušujících práva duševního vlastnictví. SDEU jednoznačně určil, že provozovatelé online tržišť se musejí jako zprostředkovatelé online služeb podrobit soudnímu zákazu vydanému za účelem zabránění dalšímu porušování práv duševního vlastnictví.[104] V návaznosti na správní či soudní rozhodnutí o ochraně před dalším porušováním autorských práv se lze domáhat zamezení zprostředkování škodlivých informací i u poskytovatelů připojení k Internetu, kteří mají na starosti pouhý přenos informace.[105] Soudní zákaz dalšího porušování autorských práv lze vydat vůči všem zprostředkovatelům, jejichž služby jsou využívány k porušování autorských práv,[106] ať už jde o internetovou platformu typu The Pirate Bay, umožňující uživatelům sdílet autorská díla bez souhlasu autorů, nebo obecně o poskytovatele internetového připojení, kteří mají na starosti pouhý přenos bez znalosti obsahu přenášených informací.[107] Podle SDEU lze vydat plošný soudní příkaz k blokaci platforem zaměřených na sdílení informací porušujících autorská práva. Obdobné závěry lze učinit i ve vztahu k ochraně osobnosti, tedy k požadavku odstranění hanlivých informací z virtuálního prostředí.[108]

Všeobecná blokace šíření škodlivých informací na Internetu na základě soudního příkazu vydaného v jediném členském státě v EU zatím neexistuje. Zajímavé závěry lze proto očekávat od vyjádření se k předběžné otázce, zda je provozovatel internetového vyhledávače v rámci vyhovění žádosti směřující k odstranění odkazu povinen odkaz odstranit na všech doménových jménech svého vyhledávače tak, aby se neobjevoval bez ohledu na místo, ze kterého je na Internetu vyhledáván (tedy i vůči IP adrese mimo jurisdikci daného státu).[109]

K rozvoji informační společnosti se snaží přispět i směrnice o opakovaném využití informací veřejného sektoru[110] (dále též „směrnice PSI"), tj. informací vytvořených orgány veřejné moci na státní, regionální i místní úrovni.[111] Vychází z premisy, podle níž informace z veřejného sektoru, ať už právní, dopravní, meteorologické, finanční, či hospodářské, nemusejí sloužit jen ke kontrole činnosti orgánů veřejné správy, nýbrž jsou zajímavým obchodním artiklem.[112] Především z komerčního úhlu pohledu nahlíží na sdílení informací veřejné správy a soukromého sektoru také směrnice PSI, která zavazuje členské státy, aby umožnily opakované použití údajů orgánů veřejné správy pro komerční i nekomerční využití, ledaže by byl přístup k nim omezen nebo vyloučen vnitrostátním právním řádem

101 Stanovisko generálního advokáta SDEU Macieje Szpunara ve věci C-49/16, bod 32; usnesení SDEU C-166/17.
102 V daném případě šlo o provozování online hazardních her. Nález Ústavního soudu ČR ze dne 14. 2. 2017, Pl. ÚS 28/16.
103 Stanovisko generálního advokáta SDEU Macieje Szpunara ve věci C-49/16, zejm. bod 50. Skutkový stav spočíval v tom, že obchodní společnost nabízela skrze Internet v Maďarsku hazardní hry bez povolení od tamějších správních orgánů, ač byla držitelkou povolení k poskytování těchto služeb v jiných členských státech. Na základě správních rozhodnutí maďarských orgánů byl přístup na stránky společnosti v Maďarsku blokován.
104 Z rozsudku SDEU ze dne 12. 7. 2011, *L'Oréal*, C-324/09, vyplývá, že čl. 11 směrnice 2004/48/ES o dodržování práv duševního vlastnictví se vztahuje i na virtuální prostředí.
105 Rozsudek SDEU ze dne 15. 9. 2016, *Mc Fadden*, C-484/14.
106 Čl. 11 směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví. Dostupné na <http://eur-lex.europa.eu/homepage.html>.
107 Rozsudek SDEU ze dne 14. 6. 2017, C-610/15. Pod pojem „sdělování autorského díla veřejnosti" ve smyslu směrnice 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti totiž spadá i zpřístupnění a správa platformy pro sdílení na Internetu. Zpřístupněním hypertextových odkazů na chráněná díla skrze Internet jakožto zpřístupněním autorského díla veřejnosti se zabýval i rozsudek SDEU ze dne 8. 9. 2016, C-160/15.
108 Stanovisko generálního advokáta SDEU Michala Bobka ve věci C-194/16 *Bolagsupplysningen OÜ Ingrid Ilsjan v. Svensk Handel AB*, v níž se stěžovatelka sídlící v Estonsku domáhala odstranění hanlivých informací z webových stránek švédského svazu obchodu.
109 Žádost o rozhodnutí o předběžné otázce podaná Conseil d'État (Francie) dne 21. 8. 2017 ve věci C-507/17 *Google Inc. v. Commission nationale de l'informatique et des libertés*.
110 Směrnice Evropského parlamentu a Rady 2013/37/EU ze dne 26. 6. 2013, kterou se mění směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru.
111 Oproti původní směrnici z roku 2003 došlo zejména k rozšíření věcné působnosti směrnice PSI, k úpravě zásady zpoplatnění opakovaného použití údajů a k zavedení práva na jejich opakované použití.
112 V tomto ohledu je diskutabilní vhodnost zahrnutí úpravy do zákona č. 106/1999 Sb. Podrobněji Polčák, R. Informace veřejného sektoru a jejich další komerční využití. In: *Veřejná správa* [online], 2008, č. 7. Dostupné na <http://www.mvcr.cz/clanek/informace-verejneho-sektoru-a-jejich-dalsi-komercni-vyuziti.aspx>.

či výjimkami dle směrnice. Směrnice PSI tak zakládá veřejné subjektivní právo na příjem informací ze strany orgánů veřejné moci. Informace by měl orgán veřejné moci, pokud je to možné a vhodné, poskytovat v otevřeném a strojově čitelném formátu spolu s metadaty tak, aby byly snadno zpracovatelné počítačovým programem.[113] Právo na příjem informací ve virtuálním prostředí je však i zde limitováno projevy informačního sebeurčení dotčených osob či veřejným zájmem na ochraně bezpečnosti státu. Sdílení informací veřejným sektorem je omezeno ochranou osobních údajů, ochranou soukromí a ochranou osobnosti, ochranou obchodního tajemství, ale také ochranou utajovaných informací.[114] Ačkoli rozsah informací, k nimž členské státy poskytnou neomezený přístup, jakož i rozhodnutí, zda povolí jejich opakované použití, zůstává na členských státech, s ohledem na novelizaci původní směrnice z roku 2003 lze očekávat postupné rozšiřování minimálního rozsahu sdílených informací.[115]

Geo-blocking[116] jako technická překážka šíření informací ve virtuálním prostředí EU?

Z ustálené judikatury SDEU vyplývá, že jakékoli omezení online obchodu mezi členskými státy, není-li objektivně zdůvodněno obecným zájmem dle čl. 36 SFEU nebo kategorickými požadavky, je omezením volného pohybu zboží v rozporu s čl. 34 SFEU.[117] Bránit volnému pohybu informací po síti nemusejí jen státy, ale i poskytovatelé služeb informační společnosti, kteří využitím technických metod brání přenosu počítačových dat do jiných členských států a blokují přístup k webové stránce internetovým uživatelům z území jiného státu. Tato praxe brání vzniku jednotného trhu online služeb v rámci EU.[118]

Geo-blocking nebo též zeměpisné blokování označuje opatření poskytovatelů služeb informační společnosti spočívající v blokaci přístupu k webovým stránkám a jinému online rozhraní a přesměrování potenciálních zákazníků z jedné země na jinou verzi webového obsahu, který byl pro jejich zemi určen.[119] V určitých případech znemožňuje všem osobám vystupujícím v síti pod IP adresou daného státu získat přístup k informacím, které se ve virtuálním prostředí jinak vyskytují. K blokaci na Internetu může přitom docházet i v jiném než ryze obchodním zájmu.[120]

Odstranění zeměpisného blokování by mělo vést k pozitivním dopadům na spotřebitele i podnikatele ve všech členských státech EU; zvláště pozitivní dopady se předpokládají u menších členských států. Zatímco spotřebitelé by měli těžit z nižších cen a bohatší nabídky zboží, podnikatelé z nových obchodních příležitostí.[121] Jiný pohled na zeměpisnou blokaci nabízí Mazziotti, podle kterého není důvodu kvůli přetrvávající praxi zeměpisného blokování v EU panikařit. Podle Mazziottiho přinášejí technické překážky sdílení – zejména pro právo duševního vlastnictví (především pro filmový průmysl) – řadu pozitiv a umožňují přizpůsobit se požadavkům různého kulturního i jazykového prostředí v rámci EU. Místo odstranění zeměpisné blokace proto navrhuje zpřesnit licenční podmínky v jednotlivých zemích.[122]

K zamezení zeměpisnému blokování při obchodování s online službami (v rámci tzv. digitálního trhu služeb) přijala EU dne 14. června 2017 nařízení o přeshraniční přenositelnosti online služeb poskytujících obsah v rámci vnitřního trhu[123] (dále jen „nařízení o přenosu online služeb"), které stanoví poskytovatelům placených online služeb povinnost umožnit zákazníkům z území jiného členského státu online přístup k totožnému

113 Srov. čl. 5 odst. 1 ve spojení s výkladovým ustanovením čl. 2 směrnice PSI.
114 Srov. § 7, § 8a a § 9 zákona č. 106/1999 Sb.
115 V tomto směru bude zajímavé sledovat rozhodnutí SDEU ve věci předběžné otázky položené Vrchním soudem Slovinské republiky ze dne 25. 4. 2017, sp. zn. C-215/17.
116 V českém jazyce označováno také doslovně jako „zeměpisné blokování". Viz Strategie pro jednotný digitální trh EU. In: *Evropská rada a Rada EU* [online] Dostupné na <http://www.consilium.europa.eu/cs/policies/digital-single-market/>.
117 Rozsudek SDEU ze dne 2. 12. 2010, *Ker-Optika*, C-108/09, body 56 až 57.
118 Strategie pro jednotný digitální trh EU. In: *Evropská rada a Rada EU* [online] Dostupné na <http://www.consilium.europa.eu/cs/policies/digital-single-market/>.
119 Komise EU. *Geo-blocking practices in e-commerce: Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition. Brussels: SWD(2016) 70 final.* Dostupné na <http://ec.europa.eu/competition/antitrust/ecommerce_swd_en.pdf>.
120 Příkladem je vládní cenzura virtuálního obsahu zobrazovaného uživatelům nacházejícím se v Čínské lidové republice. Srov. Young, X. Deconstructing the Great Firewall of China. In: *ThousandEyes Blog* [online]. Dostupné na <https://blog.thousandeyes.com/deconstructing-great-firewall-china/>; Bradsher, K. China Blocks WhatsApp, Broadening Online Censorship. In: *The New York Times* [online]. Dostupné na <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html>.
121 Duch-Brown, N. – Martens, B. The Economic Impact of Removing Geo-blocking Restrictions in the EU Digital Single Market. Digital Economy Working Paper 2016/02. In: *SSRN* [online]. Brusel 2016. Dostupné na <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2783647>.
122 Mazziotti, G. Is geo-blocking a real cause for concern in Europe? European University Institute Working Paper LAW 2015/43. In: *Cadmus* [online]. Dostupné na <http://cadmus.eui.eu/handle/1814/38084>.
123 Nařízení Evropského parlamentu a Rady (EU) 2017/1128 ze dne 14. června 2017 o přeshraniční přenositelnosti online služeb poskytujících obsah v rámci vnitřního trhu. Dostupné na <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1516567525397&uri=CELEX:32017R1128>.

obsahu, k jakému mají přístup zákazníci na území domovského státu. Nařízení o přenosu online služeb se vztahuje zejména na poskytovatele placených audiovizuálních, hudebních a herních služeb.[124] Online obsah, který si uživatel nepředplatil, tudíž přenositelný být nemusí.

Ačkoli má poskytovatel služby podle čl. 3 odst. 1 nařízení o přenosu online služeb povinnost zajistit platícím zákazníkům dočasně pobývajícím na území jiného členského státu přístup k totožnému obsahu online služby, tj. zajistit možnost využít online služby stejným způsobem jako v členském státě jejich bydliště, tento požadavek totožnosti se výslovně nevztahuje na kvalitu online služby.[125] Kvalita online služeb poskytovaných spotřebitelům pobývajícím v jiném než domovském státě tím pádem může být natolik odrazující, že spotřebitelé nebudou po dobu pobytu v jiném státě online službu využívat. Poskytovatel služby v takovém případě sice vyhoví požadavkům nařízení, avšak bezproblémový přístup z jiných členských států k online službě bude umožněn pouze formálně. Poskytovatel online služby za úplatu má také povinnost při uzavření smlouvy ověřit místo pobytu zákazníka. Ověření nemusí proběhnout jen díky kontrole IP adresy, ale i netechnickými způsoby.[126] V případě bezplatného poskytování online služeb budou poskytovatelé zpravidla ověřovat stát bydliště zákazníka, přičemž se mohou rozhodnout, že zákazníkům dočasně pobývajícím v jiném členském státě umožní přístup k online službě jen při ověření členského státu bydliště.[127]

V souladu s politikou jednotného digitálního trhu navrhla Komise EU dále přijmout nařízení, které má odstranit neoprávněné zeměpisné blokování a jinou diskriminaci na vnitřním trhu nepřímo vyplývající ze státní příslušnosti, místa bydliště nebo usazení zákazníků.[128] Diskriminační kritéria mohou být aplikována například na základě informací o fyzickém místě zákazníka, jako je IP adresa, z níž uživatel přistupuje k online rozhraní,[129] či adresa zadaná pro dodání zboží, volba jazyka nebo stát vydání platebního prostředku.[130] Toto nařízení[131] (dále též „nařízení o zeměpisném blokování") přijaly Evropský parlament a Rada[132] dne 28. 2. 2018 a účinné bude od 3. 12. 2018.

Nařízení o zeměpisném blokování má umožnit řádné fungování vnitřního trhu a přispět ke vzniku jednotného digitálního trhu, z jeho působnosti je však vyloučena široká škála služeb běžně poskytovaných především online. Podle čl. 1 odst. 3 se úprava nařízení o zeměpisném blokování nevztahuje mimo jiné na audiovizuální služby, včetně kinematografických služeb, a na rozhlasové vysílání[133] a dále se podle čl. 1 odst. 5 úprava nedotkne pravidel již uplatňovaných v oblasti autorského práva; tudíž není pochyb, že audiovizuální služby, které poskytují přístup k dílům chráněným autorskými právy (zejména územními licencemi), budou z působnosti nařízení o zeměpisném blokování vyňaty. Nicméně audiovizuální služby jsou v dnešní době uživatelům v EU poskytovány v čím dále tím větší míře pouze online. V praxi to znamená, že blokaci online audiovizuálních služeb umožňujících přístup k dílům chráněným autorskými právy (typicky se bude jednat o poslech hudby či sledování filmů a seriálů), kterou poskytovatelé služeb provádějí z důvodu státní příslušnosti uživatelů, nebude nařízení o zeměpisném blokování nijak bránit.

Podmínky zákazu zeměpisné blokace však nejsou natolik striktní, jak se na první pohled může zdát. Článek 3 odst. 1 nařízení o zeměpisném blokování zakazuje obchodníkům, aby technickými nebo jinými prostředky blokovali nebo omezovali přístup zákazníka k online rozhraní obchodníka z důvodů souvisejících s jeho státní příslušností, místem bydliště nebo místem usazení, přičemž stejné podmínky by měly platit i pro mobilní aplikace.[134] Podle čl. 3 odst. 2 nařízení

[124] Čl. 4 nařízení o přenosu online služeb.
[125] Srov. čl. 3 odst. 3 nařízení o přenosu online služeb.
[126] Zajímavou možností je v tomto ohledu ověření zápisu zákazníka v místním voličském seznamu. Srov. čl. 5 odst. 1 nařízení o přenosu online služeb.
[127] Srov. čl. 6 odst. 1 a čl. 9 nařízení o přenosu online služeb.
[128] Zákazníkem se dle čl. 2 odst. 13 nařízení o zeměpisném blokování rozumí „spotřebitel, který je státním příslušníkem některého členského státu nebo má místo bydliště v některém členském státě, nebo podnik, který má místo usazení v některém členském státě, a získá službu či nakoupí zboží nebo usiluje o získání služby či koupi zboží v Unii, a to pouze za účelem jejich konečného užití".
[129] Online rozhraním je dle čl. 2 odst. 16 nařízení o zeměpisném blokování „jakýkoli software, včetně internetové stránky nebo její části a aplikací, včetně mobilních aplikací, provozovaný obchodníkem nebo jeho jménem, který slouží k poskytování přístupu zákazníků ke zboží nebo službám obchodníka za účelem uzavření transakce ve vztahu k tomuto zboží nebo službám".
[130] Srov. čl. 6 nařízení o zeměpisném blokování.
[131] Nařízení o řešení neoprávněného zeměpisného blokování a dalších forem diskriminace založených na státní příslušnosti, místě bydliště či místě usazení zákazníků v rámci vnitřního trhu a o změně nařízení (ES) č. 2006/2004 a (EU) 2017/2394 a směrnice 2009/22/ES.
[132] Rada např. navrhla zakázat pouze *neoprávněné* zeměpisné blokování.
[133] Srov. čl. 1 odst. 3 nařízení o zeměpisném blokování ve spojení s čl. 2 odst. 2 směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. 12. 2006 o službách na vnitřním trhu.
[134] Srov. čl. 18 nařízení o zeměpisném blokování.

o zeměpisném blokování nesmějí být ze stejných důvodů zákazníci bez svého souhlasu přesměrováni na jinou verzi online rozhraní, která se svým obsahem liší od původní verze. Výslovně se dokonce uvádí, že „zákaz diskriminace zákazníků podle tohoto nařízení by neměl být chápán tak, že obchodníkům brání nabízet zboží nebo služby v různých členských státech nebo určitým skupinám zákazníků prostřednictvím cílených nabídek a odlišných všeobecných obchodních podmínek pro přístup, a to i vytvořením online rozhraní pro konkrétní zemi".[135] Provozování různých verzí online rozhraní pro zákazníky z různých členských států a možnost přesměrování zákazníků mezi těmito verzemi tedy zůstávají i pro příště zachovány s tím, že se bude vyžadovat souhlas zákazníků.[136] Do budoucna tak patrně můžeme očekávat podobnou situaci jako v případě udělování souhlasu se zpracováním osobních údajů a instalací souborů cookies na počítač uživatele ve smyslu požadavků směrnice 2002/58/ES,[137] přičemž o významu informovaného souhlasu uživatele lze pochybovat (většina uživatelů upozornění odsouhlasí, neboť jim vadí na ploše). Článek 3 odst. 3 nařízení o zeměpisném blokování pak vylučuje uplatnění zákazu blokovat či přesměrovat zákazníka na jiné online rozhraní pro situace, v nichž obchodník omezuje přístup zákazníka k online rozhraní proto, aby vyhověl právním požadavkům členského státu či EU. V takovém případě stanoví nařízení o zeměpisném blokování toliko požadavek, aby obchodník svůj postup zákazníkovi „jasně a konkrétně" vysvětlil. Tato výjimka ze zákazu blokace, přesměrování či omezení přístupu k online obsahu je sice zdůvodněna rozdílností právní úpravy členských států ohledně svobody projevu a zákazu některých států sdílet určitý druh obsahu,[138] avšak může být zneužívána, neboť obecná formulace umožní blokovat online obsah, který v podstatě nesplní jakékoli právní požadavky, namísto zajištění souladu s právním řádem daného členského státu.

Podle Cleynenbreughela neodstraní nová nařízení o přenosu online služeb a nařízení o zeměpisném blokování překážky jednotného digitálního trhu i proto, že samotné prosazení obou nařízení vůči poskytovatelům on-line služeb a zprostředkovatelům informací ve virtuálním prostředí zůstává na členských státech.[139] Nařízení o zeměpisném blokování poskytuje v čl. 7 prostor pro rozšíření správního dozoru, jehož podobu, včetně ukládaných sankcí, ponechává zcela na dozorčích orgánech členských států, a pouze v odst. 2 stanoví, že jednotlivá opatření (správní sankce) musejí být účinná, přiměřená a odrazující. Nařízení o zeměpisné blokaci se tudíž na jednu stranu snaží unifikovat v rámci vnitřního trhu digitálních služeb pravidla pro použití zeměpisného blokování, na druhou stranu však podmínky jejich vymáhání a sankcionování ponechává zcela na jednotlivých členských státech. Lze se domnívat, že rozdílný přístup jednotlivých členských států může postupem času vést k vyčlenění některých států, které budou v prosazování agendy poněkud laxnější, což by mohlo vést k přesunu sídla části poskytovatelů online služeb na jejich území. V rámci virtuálního prostoru, který nezná hranic, pokud nejde o vymáhání národních právních norem, poskytovatelům online služeb nic nebrání nabízet služby uživatelům mimo stát jejich sídla. Neoprávněné zeměpisné blokování a jiné diskriminační praktiky na základě státní příslušnosti mohou též nadále přetrvávat ze strany poskytovatelů usazených na území třetích států. Otázkou tedy zůstává, zda nebude možné zákaz neoprávněného zeměpisného blokování příliš snadno obcházet.

Závěr

Ať se informace šíří ve virtuálním prostředí, či mimo něj, nejedná se o proces prostý překážek. Některé překážky jsou technického charakteru a pramení z toho, že informace jsou ve virtuálním prostředí propojených počítačových sítí v prvé řadě data proudící v síti, a jiné plynou z chování uživatelů služeb informační společnosti, příjemců informací. Překážky šíření informací ve virtuálním prostředí přináší i právní úprava.

Právní vztahy, kde hraje určitou roli Internet a virtuální (popř. kybernetický) prostor, mívají mezinárodní charakter. Prostředí celosvětově propojených počítačových sítí je decentralizovaným flexibilním prostorem, kde

135 Srov. recitál 27 ve spojení s čl. 4 odst. 1 a odst. 2 nařízení o zeměpisném blokování.
Srov. rovněž recitál 20 nařízení o zeměpisném blokování.

136 Srov. rovněž recitál 20 nařízení o zeměpisném blokování, který předpokládá, že souhlas udělí uživatel pouze napoprvé (což ovšem předpokládá jeho další souhlas s instalací souboru cookies, aby si online rozhraní volbu uživatele pro jeho počítačové zařízení „zapamatovalo").

137 Směrnice Evropského parlamentu a Rady 2002/58/EC ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

138 Srov. recitál 21 nařízení o zeměpisném blokování.

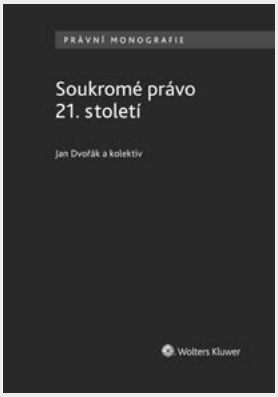
139 Van Cleynenbreughel, P., c. d., str. 49.

tradiční hranice offline světa neexistují, a vztahy v jeho rámci se stávají předmětem mezinárodních debat i sporů, které řeší nadnárodní soudy. Z rozhodovací praxe Evropského soudu pro lidská práva i Soudního dvora Evropské unie, jakož i z nezávazných pravidel a doporučení, lze dovodit některé zásady přípustného omezení svobody přijímat a rozšiřovat informace ve virtuálním prostředí. Například podle doporučení Výboru ministrů Rady Evropy by orgány veřejné moci neměly filtrovat přenášené informace z jiných než taxativně vypočtených hledisek na základě čl. 10 odst. 2 Úmluvy. K filtrování online obsahu nelze přistoupit plošně, nýbrž jen ve vztahu k přesně vymezeným informacím poté, co kompetentní státní orgán rozhodl o jejich protiprávnosti v řízení splňujícím požadavky spravedlivého procesu dle čl. 6 Úmluvy. ESLP ve své judikatuře vnímá virtuální prostředí jako klíčový prvek svobodného přístupu k informacím a odsuzuje praxi států plošně blokujících občanům přístup k internetové platformě využívané ke studiu a šíření informací.[140] Přesto ESLP stále nepovažuje přístup k Internetu za právo zaručené všem bez rozdílu.[141]

SDEU se ve své rozhodovací činnosti ke svobodnému šíření informací ve virtuálním prostředí vyjadřuje skrze maximu zákazu diskriminace na základě státní příslušnosti k jinému členskému státu a zákazu omezení volného trhu služeb. V souvislosti s politikou jednotného digitálního trhu a snahou zamezit neoprávněným zeměpisným blokacím ve virtuálním prostředí lze očekávat rozšíření rozhodovací činnosti SDEU o další otázky. Mnohý z právních zákazů lze však ve virtuálním prostředí obejít a nová právní úprava, jejímž smyslem je přispět ke vzniku jednotného digitálního trhu, má řadu problematických bodů. Otázkou zůstává, zda idea svobodného šíření informací nezůstane jen ideou virtuální.

140 Rozsudek ESLP *Cengíz ad others v. Turkey*, rozsudek *Ahmet Yildirim v. Turkey*.
141 Rozsudek ESLP *Jankovskis v. Lithuania*.

KNIŽNÍ TIP



Soukromé právo 21. století

Jan Dvořák a kolektiv

Monografie vznikla jako výsledek řešitelského úsilí předních odborníků na soukromé právo v rámci Programu rozvoje vědních oborů na Univerzitě Karlově „Soukromé právo XXI. století" (PRVOUK 05).

Cílem řešitelského kolektivu bylo postihnout klíčovou roli soukromého práva v dynamicky se vyvíjející společnosti. Badatelské úsilí se zaměřilo jak na základní soukromoprávní instituty a jejich výklad, tak na vybrané dílčí problémy. Tím se řešitelům otevřel prostor jak pro koncepční úvahy nad dalším směřováním soukromého práva jako celku, tak pro identifikaci aktuálních problémů současné právní úpravy a jejich kritický rozbor. Pro lepší přehlednost je kniha rozdělena do pěti částí, z nichž každá nabízí podnětné úvahy *de lege ferenda*: 1. Kogentní a dispozitivní normy v soukromém právu, 2. Ochrana slabší strany, 3. Subjekty soukromého práva a jejich jednání, 4. Nástroje právní ochrany, 5. Procesní souvislosti.

Monografie je určena odborníkům se zájmem o hlubší studium soukromého práva v jeho širších souvislostech.

Objednat můžete na obchod.wolterskluwer.cz