Collection of Papers
from the International Academic Conference
21st – 22nd of October 2016

INTERNET AS A SPACE OF POSSIBLE RIGHTS INFRINGEMENT

BRATISLAVA LEGAL FORUM 2016

Zborník príspevkov
z medzinárodnej vedeckej konferencie
21. – 22. októbra 2016

INTERNET AKO PRIESTOR MOŽNÉHO PORUŠOVANIA PRÁV

BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2016

SYMPOSIA, COLLOQUIA, CONFERENCES
SYMPÓZIÁ, KOLOKVIÁ, KONFERENCIE

INTERNET AS A SPACE OF POSSIBLE RIGHTS INFRINGEMENT

BRATISLAVA LEGAL FORUM 2016

INTERNET AKO PRIESTOR MOŽNÉHO PORUŠOVANIA PRÁV

BRATISLAVSKÉ PRÁVNICKÉ FÓRUM 2016

Collection of Papers from the International Academic Conference
Bratislava Legal Forum 2016
organised by the Comenius University in Bratislava, Faculty of Law
on 21st – 22nd of October 2016
under the auspices of Andrej Danko,
the Chairman of the National Council of the Slovak Republic

Zborník príspevkov z medzinárodnej vedeckej konferencie
Bratislavské právnické fórum 2016
organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou
v dňoch 21. – 22. októbra 2016
pod záštitou predsedu Národnej rady Slovenskej republiky Andreja Danka

UNIVERZITA KOMENSKÉHO
V BRATISLAVE
PRÁVNICKÁ FAKULTA
VYDAVATEĽSKÉ ODDELENIE

Univerzita Komenského v Bratislave
Právnická fakulta
2016

Reviewers of Papers / Recenzenti:

- doc. JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA.
- JUDr. Jozef Valuch, PhD
- Mgr. Martin Daňko, PhD

Editors / Zostavovatelia:

- Mgr. Michal Lenhart
- JUDr. Jozef Andraško
- JUDr. Juraj Hamuľák, PhD.

ISBN 978-80-7160-432-7
EAN 9788071604327

CONTENT / OBSAH

BEZPEČNÁ IDENTIFIKÁCIA A AUTENTIFIKÁCIA PRI VYUŽÍVANÍ ELEKTRONICKÝCH SLUŽIEB VEREJNEJ SPRÁVY[1]

Jozef Andraško

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: Author deals with issues relating to identification and authentication as fundamental preconditions for using public administration electronic services. Author analyses the issue from the perspective of Slovak legal order as well as European Union law.

Abstrakt: Autor sa v príspevku zaoberá otázkami identifikácie a autentifikácie ako základných predpokladov využívania elektronických služieb verejnej správy. Autor rozoberá predmetnú problematiku z pohľadu právneho poriadku Slovenskej republiky, ako aj práva Európskej únie.

Keywords: identification, authentication, electronic services, public administration, internet, online

Kľúčové slová: identifikácia, autentifikácia, elektronické služby, verejná správa, internet, online

1 ÚVOD

Orgány verejnej správy vstupujú s rôznymi entitami[2], konkrétne fyzickými osobami, fyzickými osobami podnikateľmi alebo právnickými osobami do rôznych právnych vzťahov. V súčasnej informačnej spoločnosti sa tak už nedeje len v „tradičnom svete“ ale aj vo „virtuálnom svete“[3] prostredníctvom internetu, konkrétne prostredníctvom jeho služby World Wide Web (ďalej len „WWW“). Zvýšená frekvencia využívania elektronických služieb, ktoré poskytujú orgány verenej správy nepochybne znižuje administratívne zaťaženie, zvyšuje efektívnosť verejnej správy, no na druhej strane si treba uvedomiť aj riziká, ktoré sú s poskytovaním takýchto služieb spojené. Orgány verejnej správy[4] sa pri poskytovaní konkrétnych služieb musia spoliehať na to, kto využíva konkrétnu službu, čo v sebe zahŕňa otázky týkajúce sa identifikácie a autentifikácie.

Spoľahlivé zistenie identity konkrétnej entity, ktorá chce využívať elektronickú službu poskytovanú orgánom verejnej správy už nie je len otázkou národnou. Medzinárodný charakter tejto otázky vznikne v situáciách, kedy občan iného členského štátu Európskej únie (ďalej len „EÚ“) pre prístup a využitie elektronickej služby, ktorá je poskytovaná orgánom verejnej správy iného členského štátu, nemôže využiť národné prostriedky elektronickej identifikácie. Kľúčovými aspektmi pre odstránenie bariéry pri cezhraničnom využívaní elektronických služieb a vytvorenie dôvery v online

[1] Tento príspevok vznikol v rámci riešenia vedeckého projektu s názvom „Identifikácia a autentifikácia ako základné predpoklady poskytovania a využívania elektronických služieb verejnej správy“. Grant UK č. UK/270/2016.

[2] Entitou môže byť čokoľvek, človek, zviera, vec, organizácia, dokument, ale aj nehmotný objekt ako myšlienka. Pre účely tohto článku sú entitami fyzické osoby, fyzické osoby podnikatelia a právnické osoby. Bližšie pozri: OLEJÁR, D.: Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. s. 5. [online]. Dostupné na internete: http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s

[3] Pojem „virtuálny svet“ alebo taktiež „virtuálny priestor“ nemajú v slovenskom právnom poriadku legálnu definíciu. Vo všeobecnosti sa tieto pojmy používajú na označenie online prostredia na internete.

[4] Bližšie k pojmu orgán verejnej správy pozri ŠKROBÁK, J. In VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012, s. 18-20.

prostredí sú interoperabilita[5] a bezpečnosť elektronických prostriedkov, ktoré slúžia na identifikáciu a autentifikáciu.

2 ELKTRONICKÉ SLUŽBY VEREJNEJ SPRÁVY

Dôležitú kategóriou v oblasti eGovernmentu[6] predstavujú elektronické služby verejnej správy, v odbornej literatúre označované taktiež ako služby eGovernmentu. V súvislosti s týmto pojmom je viac ako potrebné vymedziť pojem elektronické služby ako také. V zmysle *Metodického pokynu na použitie odborných výrazov pre oblasť informatizácie spoločnosti* (ďalej len „Metodický pokyn“) sú elektronické služby (*e-services*) definované ako: „*služby poskytované v elektronickej podobe pomocou informačných a komunikačných prostriedkov*.“[7]

Napriek skutočnosti, že charakteristiky elektronických služieb sú príznačné pre súkromný sektor, podobné kategórie interakcií možno nájsť aj v súčasných definíciách eGovernmentu. Pojem elektronické služby, ktorý v podmienkach eGovernmentu predstavujú služby verejného záujmu, je používaný pre rôzne podoby zdokonaľovania verejných služieb. Elektronická služba verejnej správy, služba eGovernmentu *(eGovernment service)* je v *Metodickom pokyne* vymedzená ako: *„elektronická forma vecnej komunikácie verejnosti s verejnou správou pri vybavovaní vecí, účasti verejnosti na správe vecí verejných, alebo prístupe verejnosti k informáciám.“*

V zmysle výnosu č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos“) sa elektronické služby verejnej správy rozdeľujú podľa úrovne elektronizácie na šesť úrovní, ktorými sú:

- **Nultá úroveň** (služby offline). Služba nie je online elektronicky dostupná. Občan si musí vybaviť svoju úradnú záležitosť osobne, klasickým papierovým spôsobom.
- **Prvá úroveň** (informatívne služby). Informácia, ktorá je potrebná na začatie alebo vykonanie služby, je dostupná v elektronickej forme. Ide najmä o informácie o mieste, čase, spôsobe a podmienkach vybavenia služby. Samotná služba nie je elektronicky poskytnutá, ani nie je poskytnutý príslušný formulár v elektronickej forme.
- **Druhá úroveň** (jednosmerne interaktívne služby). Ide o jednosmernú elektronickú komunikáciu. Pri jednosmernej elektronickej komunikácii je možné stiahnuť príslušný formulár v elektronickej forme, ale podanie sa nevykonáva elektronickými prostriedkami.
- **Tretia úroveň** (obojstranne interaktívne služby). Ide o obojsmernú elektronickú komunikáciu pri vybavovaní služby. V rámci tejto úrovne prebieha vybavovanie služby elektronicky, avšak pri preberaní výsledku služby sa vyžaduje osobný alebo listinný kontakt.
- **Štvrtá úroveň** (transakčné služby). Táto úroveň umožňuje úplné vybavenie služby elektronickými prostriedkami, najmä vybavenie online, a to vrátane rozhodnutia, zaplatenia a doručenia, ak sa to vyžaduje. V rámci tejto úrovne sa vylučuje akýkoľvek osobný alebo listinný kontakt.
- **Piata úroveň** (proaktívne služby). Táto úroveň obsahuje funkčnosť tretej úrovne alebo štvrtej úrovne, a navyše sa využívajú personalizované nastavenia používateľa, ako aj možnosti proaktívneho automatizovaného vykonávania častí služby. Ide o automatizované poskytovanie služby na základe sociálneho a ekonomického profilu prijímateľa služby, resp. udalostí bez priameho podnetu prijímateľa služby.

Na tomto mieste je potrebné podotknúť, že pre účely identifikácie a autentifikácie identity pre využívanie elektronických služieb verejnej správy majú význam len 3 druhy elektronických služieb verejnej správy, a to konkrétne obojstranne interaktívne služby, transakčné služby a proaktívne

---

5 Vo všeobecnosti možno za interoperabilitu považovať schopnosť informačných systémov verejnej správy vzájomnej komunikácie a spolupráce, najmä pri využívaní a výmene jednotlivých údajov.

6 eGovernment predstavuje „*využívanie informačno-komunikačných technológií on-line vo verejnej správe spojené s organizačnými zmenami a novými zručnosťami s cieľom zlepšiť služby verejnej správy a uplatňovanie demokratických postupov, ako aj posilniť podporu verejných politík.“ MINISTERSTVO FINANCÍ SLOVENSKEJ REPUBLIKY: Stratégia informatizácie verejnej správy. Bratislava, 2008, s. 3.*

7 MINISTERSTVO FINANCÍ SLOVENSKEJ REPUBLIKY: *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti*. Bratislava, 2008, s. 15

služby. V ostatných prípadoch sa pre využitie konkrétnej elektronickej služby verejnej správy pripúšťa aj anonymný prístup, kedy entita nemusí preukazovať svoju identitu.[8]

3 IDENTIFIKÁCIA A AUTENTIFIKÁCIA

Problematika identifikácie a autentifikácie je stará ako ľudstvo samé. Pôvodne fyzické osoby preukazovali svoju totožnosť geografickým názvom svojho miesta narodenia ako napr. Herakleitos z Efezu. Takáto identifikácia osôb v neskorších dobách, kedy vznikali prvé moderné štáty samozrejme nepostačovala. V dôsledku nárastu obyvateľstva, ako aj migračných tendencií bolo potrebné identifikovať osoby oficiálnou cestou. K identifikáciu všetkých občanov bez výnimky došlo až po Francúzskej revolúcii (1789), kedy tamojšie legislatívne orgány mali stanoviť akým spôsobom sa bude overovať narodenie, uzavretie manželstva a smrť, ako aj ktorý orgán bude o týchto skutočnostiach vydávať príslušné dokumenty a tie aj uchovávať.[9]

3.1 Identita

Pred ozrejmením pojmov identifikácia a autentifikácia je potrebné upriamiť pozornosť na kľúčový pojem skúmanej problematiky, ktorým je „identita". Identitu ako koncept, možno chápať z psychologického, sociálneho, ale aj právneho hľadiska. V súvislosti s pojmom identita treba poznamenať, že každá entita sa vyznačuje charakteristickými znakmi, tzv. atribútmi. Množina takýchto atribútov, ktoré nám umožňujú odlíšiť jednu entitu od druhej, tvorí identitu danej entity. Napríklad fyzická osoba je charakterizovaná výškou, vekom, výzorom, váhou, DNA, dátumom a miestom narodenia, bydliskom, alebo zamestnaním. Súbor takýchto vlastností danej entity sa nazýva úplná identita. Na to aby sme mohli entity od seba odlíšiť, bez toho aby sme poznali všetky charakteristické znaky, umelo vytvárame identifikátory. Príkladom takýchto identifikátorov pri fyzických osobách je rodné číslo a v komplexnejšom ponímaní verejné listiny ako občiansky preukaz, alebo rodný list.[10]

Od kedy sa internet, konkrétne jeho služba WWW začala používať ako prostriedok pre komunikáciu v oblasti obchodu, ako aj verejnej správy, začali vznikať debaty o elektronickej, digitálnej alebo kybernetickej identite. Pre účely tohto článku budem z dôvodu konzistentnosti pojmu upravenom v právnom poriadku Slovenskej republiky používať pojem „elektronická identita".

V tradičnom svete vystupuje osoba pod jednou identitou, resp. môže vystupovať anonymne. Vo virtuálnom svete je situácia iná, nakoľko možno hovoriť o viacerých identitách tej istej osoby. Problematika elektronickej identity v akademickom prostredí predstavuje najmä debatu o pôvode ľudskej identity a jej premenách v informačnej spoločnosti. Právnici problematiku elektronickej identity spájajú najmä s otázkami týkajúcimi sa zodpovednosti, ochrany súkromia, ochrany osobných údajov, etiky a morálky. Taktiež sú veľmi dôležité otázky týkajúce sa anonymity a súkromia, kedy právo dovoľuje anonymitu vo virtuálnom priestore, kedy ju prikazuje a kedy zas vyžaduje identifikáciu. Na tomto mieste je potrebné podotknúť, že konanie rôznych entít, ako sú fyzické osoby, fyzické osoby podnikatelia alebo právnické osoby vo virtuálnom priestore môže mať právne následky aj v tradičnom svete. Preto vo vzťahu k elektronickým službám verejnej správy je potrebné, aby poskytovateľ elektronickej služby verejnej správy mal istotu, s kým komunikuje. Vo väčšine prípadov, ak neberieme do úvahy elektronické služby, kde je dovolený aj anonymný prístup, existuje právna podmienka identifikovať sa, aby daná osoba mala prístup a mohla používať konkrétnu službu.

V odbornej literatúre sa stretneme s viacerými definíciami pojmu elektronická identita. Niektorí autori ju vymedzujú ako: *„identita, ktorá je tvorená z informácií uchovávaných a prenášaných v digitálnej forme"*.[11] Elektronická identita je taktiež chápaná ako čiastková identita, ktorá je

---

[8] Bližšie k problematike elektronických služieb verejnej správy pozri: SOPÚCHOVÁ, S: Predpoklady fungovania e-governmentu v Slovenskej republike. In QUAERE 2015 [elektronický zdroj] Hradec Králové: Magnanimitas, 2015, s. 662.

[9] NOIRIEL, G.: The identification of the citizen: the birth of republican civil status in France. In Documenting individual identity, the development of state practices in the modern world. Princeton and Oxford: Princeton University Press, 2001. s. 28.

[10] OLEJÁR, D. a kol.: Manažment informačnej bezpečnosti. Bratislava, 2015. s. 13. [online]. Dostupné na internete: http://informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s.

[11] SULLIVAN, C.: Protecting digital identity in the cloud: Regulating cross border data disclosure. *In* Computer Law & Security Review. 2014, roč. 30, č. 2., s. 139.

v elektronickej forme.[12] Pojem elektronická identita je v slovenskom právnom poriadku vymedzený v zákone č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (ďalej len „zákon o e-Governmente"). V zmysle ustanovenia § 19 ods. 1 zákona o e-Governmente, je elektronickou identitou osoby: „*súbor atribútov, ktoré sú zaznamenateľné v elektronickej podobe a ktoré jednoznačne odlišujú jednu osobu od inej osoby najmä na účely prístupu k informačnému systému alebo na účely elektronickej komunikácie*." Elektronická identita osoby sa v zmysle zákona o e-Governmente deklaruje identifikáciou osoby a overuje sa autentifikáciou osoby.[13]

3.2 Identifikácia

Ako už bolo spomenuté, entity počas svojej existencie vstupujú s inými entitami do rôznych vzťahov. V súvislosti so základnou požiadavkou týchto entít, a teda zistenie, kto je účastníkom týchto vzťahov, budeme hovoriť o identifikácii a autentifikácii identity. Určenie identity možno rozdeliť do dvoch fáz. Prvou fázou je identifikácia. Podstatou identifikácie je, že entita deklaruje svoju identitu. Ide o situáciu, kedy sa napr. fyzická osoba predstaví. Vo virtuálnom svete by analogicky išlo o zadanie prihlasovacieho mena. V zmysle § 3 písm. m) zákona o e-Governmente možno za identifikáciu považovať*: „deklarovanie identity objektu vrátane osoby, a to najmä pri prístupe k informačnému systému verejnej správy alebo pri elektronickej komunikácii."* Inými slovami možno za identifikáciu považovať tvrdenie konkrétnej osoby o tom, kým je. Preukazovanie identity je zabezpečené identifikátorom osoby. Pre účely identifikácie sa využívajú pre rôzne druhy entít rôzne identifikátory. Napr. identifikátorom fyzickej osoby je jej rodné číslo v spojení s menom a priezviskom.[14]

3.3 Autentifikácia

Samotná identifikácia na určenie identity nepostačuje, nakoľko môže dôjsť k situácii, kedy sa entity pokúšajú vystupovať pod falošnou identitou. Takéto aktivity môžu smerovať ku krádeži identity alebo neoprávnenému prístupu k informačnému systému verejnej správy, alebo elektronickej komunikácie. Druhou fázou určenia identity je autentifikácia (autentizácia) identity. V tejto fáze musí entita, ktorá deklarovala svoju identitu, dokázať, že skutočne je tou entitou, ktorej identitu deklarovala. Inými slovami ide o potvrdenie deklarovanej identity. Osoba sa môže autentifikovať rôznymi spôsobmi. V odbornej literatúre možno hovoriť o troch základných prístupoch, ktoré sú založené na tom, čo človek vie (PIN, heslo, rodné priezvisko mamy), na tom, čo človek má (certifikát, čipová karta), alebo na tom, čo človek je (biometrické charakteristiky ako odtlačok prstov, obraz sietnice, hlas, obraz dúhovky).[15]

V súvislosti s autentifikáciou zákon o e-Governmente stanovil, že na autentifikáciu sa môže použiť len úradný autentifikátor, ktorým je občiansky preukaz s elektronickým čipom a bezpečnostný osobný kód alebo doklad o pobyte s elektronickým čipom a bezpečnostný osobný kód. Zákon o e-Governmente taktiež upravuje problematiku alternatívneho autentifikátora, ktorý sa môže použiť na autentifikáciu. V súčasnosti takýto alternatívny autentifikátor (napr. použitie mobilného telefónu na autentifikáciu) ešte nie je dostupný.

3.4 eID

Problematika dôveryhodnosti pri deklarácii svojej identity je vyriešená prenesením tohto procesu na dôveryhodnú tretiu stranu. Takouto dôveryhodnou treťou stranou je štát, ktorý zodpovedá

---

[12] Modinis Study on Identity Management in eGovernment Common Terminological Framework for Interoperable Electronic Identity Management Consultation paper v2.01. 23. november 23. 2005. s. 9. [online]. Dostupné na internete: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf

[13] V zmysle § 3 písm. n) zákona o e-Governmente za osobu možno považovať fyzickú osobu, fyzickú osobu podnikateľa, právnickú osobu, orgány verejnej moci, organizačnú zložku právnickej osoby alebo podnikateľa.

[14] Tamtiež, § 3 písm. n).

[15] OLEJÁR, Daniel a kol.: Manažment informačnej bezpečnosti. Bratislava, 2015. s. 14. [online]. Dostupné na internete: http://informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s.

za vydávanie tokenov, ktorými konkrétne osoby preukazujú svoju identitu.[16] Jedným z hlavných cieľov realizácie elektronických služieb, ktoré sú poskytované orgánmi verejnej správy cez internet, je zabezpečenie efektívnej, bezpečnej a najmä dôveryhodnej identifikácie a autentifikácie identity konkrétnej entity, ktorá chce využiť konkrétnu elektronickú službu verejnej správy. Túto a mnoho ďalších úloh plní občiansky preukaz s elektronickým čipom a bezpečnostným osobným kódom, tzv. elektronická identifikačná karta (ďalej len „eID"). Na jednej strane eID predstavuje fyzický prostriedok v neelektronickom styku pre občanov Slovenskej republiky, ako aj pre cudzincov s povoleným pobytom na území Slovenskej republiky, čiže doklad totožnosti. Na druhej strane eID poskytuje možnosť preukazovania a potvrdenia totožnosti v elektronickom prostredí. Táto funkcia je nevyhnutná pri využívaní elektronických služieb, či už vo verejnom, alebo v súkromnom sektore. eID podľa zákona o e-Govermente zabezpečuje identifikačný a autentifikačný prostriedok pre využívanie elektronických služieb verejnej správy. V Slovenskej republike sa eID vydávajú od decembra 2013 a Ministerstvo vnútra Slovenskej republiky vydalo už viac ako milión kusov.[17]

Možno konštatovať, že nový typ občianskeho preukazu sa stáva dôveryhodným prostriedkom pre identifikáciu a autentifikáciu identity vo virtuálnom prostredí, a to pomocou osobných údajov, ktoré sú uložené na elektronickom čipe.[18] Na čip možno uložiť aj kvalifikovaný certifikát pre kvalifikovaný elektronický podpis a kľúčový pár (súkromný kľúč a verejný kľúč). Údaje z eID je technicky možné prečítať len so súhlasom držiteľa eID zadaním bezpečnostného osobného kódu (ďalej len „BOK") a súčasným priložením eID k čítaciemu zariadeniu kariet. Len oprávnení poskytovatelia elektronických služieb budú môcť požiadať o prečítanie údajov z eID. Ktoré z údajov budú z eID prečítané a odovzdané poskytovateľovi elektronických služieb je určené a zabezpečené príslušným certifikátom.

Podmienkou využívania eID v elektronickej komunikácii s verejnou správou, je jeho aktivácia. Pre aktiváciu elektronického občianskeho preukazu sa vyžaduje zvolenie BOK. V zmysle § 4b ods. 2 zákona č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov je BOK: *„kombináciou najmenej šiestich a najviac desiatich číslic. Občan, ktorý v čase podania žiadosti o vydanie občianskeho preukazu nedovŕšil 65. rok veku, si bezpečnostný osobný kód zvolí pri podaní žiadosti; ostatní občania si môžu bezpečnostný osobný kód zvoliť pri podaní žiadosti alebo neskôr na okresnom riaditeľstve."* BOK s eID slúži na potvrdenie totožnosti držiteľa pri elektronickej komunikácii s informačnými systémami orgánov verejnej správy, alebo s inými fyzickými osobami alebo právnickými osobami.[19] Bezpečnosť citlivých údajov, ktoré sú uložené na čipe, je zabezpečená bezpečnostnými mechanizmami a BOK.

Vďaka elektronickému čipu slúži eID aj ako prostriedok pre vytváranie kvalifikovaného elektronického podpisu. V súvislosti s problematikou elektronického podpisu je potrebné poznamenať, že zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov bol zrušený zákonom č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).[20] Zmeny v tejto oblasti boli zapríčinené prijatím Nariadenie EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS"), ktoré ruší Smernicu

---

16 Token predstavuje akýkoľvek hardvér alebo softvér, ktorý obsahuje informácie potvrdzujúce integritu konkrétnych deklarovaných skutočností (*credentials*). Token môže mať podobu čipovej karty alebo telefónu. Pre účely identifikácie a autentifikácie identity konkrétnej entity sa využívajú napr. eID, cestovný pas a i.

17 [online] Dostupné na internete <http://www.minv.sk/?operacny-program-informatizacia-spolocnosti-tlacove-informacie&sprava=odovzdali-sme-milionty-kus-elektronickeho-obcianskeho-prekazu-s-cipom>

18 Elektronický čip, ktorý sa nachádza na zadnej strane eID obsahuje údaje, ktoré sú zapísané, alebo údaje, ktoré možno zapísať do občianskeho preukazu v zmysle zákona č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov.

19 Ustanovenie § 4b ods.1 zákona č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov.

20 K problematike elektronického podpisu bližšie pozri: DAŇKO, M.: Elektronický podpis ako prejav vôle (v rekodifikačných súvislostiach). In Míľniky práva v stredoeurópskom priestore 2015. Bratislava: Univerzita Komenského v Bratislave, 2015, s. 673-674.

1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy.[21] Zaručený elektronický podpis, ktorý predstavoval najvyššiu úroveň elektronického podpisu v zmysle zákona o elektronickom podpise bol na podobnej úrovni ako kvalifikovaný elektronický podpis podľa Nariadenia eIDAS.[22] V zmysle § 17 ods. 2 zákona o dôveryhodných službách, ak sa vo všeobecne záväzných právnych predpisoch používa pojem zaručený elektronický podpis, rozumie sa tým kvalifikovaný elektronický podpis.[23]

Kvalifikovaný elektronický podpis nám slúži na autentifikáciu totožnosti v elektronickom prostredí a zahŕňa elektronické identifikačné údaje odosielateľa elektronického dokumentu pripojené k nemu. Nariadenie eIDAS definuje niekoľko typov elektronických podpisov podľa úrovne bezpečnosti: elektronický podpis, zdokonalený elektronický podpis, zdokonalený elektronický podpis založený na kvalifikovanom certifikáte a kvalifikovaný elektronický podpis. Kvalifikovaný elektronický podpis ponúka najvyššiu úroveň bezpečnosti.

Úspešná identifikácia a autentifikácia je predpokladom autorizácie. Autorizácia predstavuje povolenie konať v súlade s oprávneniami, ktoré danej entite prislúchajú. Inými slovami, autorizácia je udelenie oprávnení nejakej entite využívať konkrétnu elektronickú službu verejnej správy. V zmysle zákona o e-Governmente, ak sa právny úkon vykonáva v elektronickej podobe alebo ak je náležitosťou právneho úkonu vlastnoručný podpis, osoba, ktorá nie je orgánom verejnej moci, vykoná autorizáciu takého úkonu kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou. Ak je náležitosťou právneho úkonu vlastnoručný podpis, ktorý musí byť úradne osvedčený, pripojí aj kvalifikovanú elektronickú časovú pečiatku. V prípade orgánov verejnej moci sa autorizácia vykonáva kvalifikovaným elektronickým podpisom a mandátnym certifikátom alebo kvalifikovanou elektronickou pečaťou s pripojenou kvalifikovanou elektronickou časovou pečiatkou.[24]

4 BEZPEČNÁ IDENTIFIKÁCIA A AUTENTIFIKÁCIA

Spoľahlivá identifikácia a autentifikácia identity je kľúčovým aspektom vytvorenia dôvery vo virtuálnom svete. V súvislosti s identifikáciou a autentifikáciou vo virtuálnom svete vznikajú nové otázky, ktoré musia byť zodpovedané. Ide najmä o technické aspekty ako bezpečnosť a interoperabilita, ale aj právne otázky, ktoré súvisia s právnou zodpovednosťou, ochranou osobných údajov, ochranou súkromia a i. Vývojom nových technológii sa tieto otázky čím ďalej viac prehlbujú, čoraz častejšie majú interdisciplinárny charakter a taktiež so sebou prinášajú nové problémy.

Otázka bezpečnosti sa stala predmetom novoprijatého Nariadenie eIDAS, ktorého cieľom je posilniť dôveru pri elektronických transakciách na vnútornom trhu. Tento cieľ by sa mal splniť zabezpečením spoločného základu pre bezpečné elektronické interakcie medzi občanmi, podnikmi a orgánmi verejnej správy, čo by malo smerovať k zvýšeniu účinnosti verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v EÚ. Hlasy z jednotlivých inštitúcií EÚ volajú po vytvorení integrovaného jednotného digitálneho trhu, uľahčení cezhraničného používania služieb online a uľahčení bezpečnej elektronickej identifikácie a autentifikácie. Cieľom Nariadenia

[21] Slovenský preklad Nariadenia eIDAS používa pojem „dôveryhodné služby“. Som toho názoru, že anglický pojem „*trust services*“ by mal byť preložený ako „služby dôvery“ resp. „služby vytvárajúce dôveru“, nakoľko hlavnou úlohou služieb poskytovaných v zmysle Nariadenia eIDAS je zabezpečenie dôvery, a tá je obsahom a podstatou týchto služieb. V texte príspevku preto používam pojem „služby dôvery“.

[22] Čo sa týka zaručenej elektronickej pečate, ktorá bola upravená v zákone o elektronickom podpise, tak tej zodpovedá kvalifikovaná elektronická pečať v zmysle Nariadenia eIDAS. V prípade kvalifikovanej elektronickej časovej pečiatky, ktorú upravuje Nariadenie eIDAS je potrebné podotknúť, že zákon o elektronickom podpise upravoval len jednu úroveň časovej pečiatky. Možno ale konštatovať, že je ekvivalentná kvalifikovanej elektronickej časovej pečiatke upravenej v Nariadení eIDAS.

[23] Obdobne, ak sa vo všeobecne záväzných právnych predpisoch používa pojem zaručená elektronická pečať, rozumie sa tým kvalifikovaná elektronická pečať a v prípade ak sa požije pojem časová pečiatka, rozumie sa tým kvalifikovaná elektronická časová pečiatka.

[24] § 23 ods. 1 zákona o e-Governmente.

eIDAS je zabezpečiť, aby bola možná bezpečná elektronická identifikácia a autentifikácia pri prístupe k cezhraničným službám online[25], ktoré ponúkajú členské štáty, aspoň v prípade verejných služieb.[26]

V zmysle ustanovení Nariadenia eIDAS, ktoré upravujú uznávanie služieb dôvery[27] v rámci celej EÚ, ako aj ich právnych účinkov, možno konštatovať, že kvalifikovaný elektronický podpis, kvalifikovaná elektronická pečať[28] a kvalifikovaná elektronická časová pečiatka[29] sú uznávané vo všetkých členských štátoch a v celej EÚ sú s ich použitím spájané rovnaké právne účinky, za podmienky, že sú založené na kvalifikovanom certifikáte vydanom kvalifikovaným poskytovateľom služieb dôvery, ktorý sa nachádza v EÚ.

Osobitne sú upravené ustanovenia týkajúce sa použitia elektronických podpisov a elektronických pečatí vo verejných službách. Predmetné ustanovenia sa týkajú využívania služieb online, ktoré poskytujú subjekty verejného sektora[30], alebo ktoré sú ponúkané v jeho mene. V týchto prípadoch pôjde už o realizáciu elektronických podaní alebo iných právnych úkonov vo vzťahu k verejnej správe, kde sa vyžaduje autorizácia[31], čiže pôjde o využitie elektronického podpisu alebo elektronickej pečate. V zmysle Nariadenia eIDAS platí, ak členský štát vyžaduje v prípade použitia online služby, ktorú poskytuje subjekt verejného sektora alebo v jeho mene, použitie elektronického podpisu alebo elektronickej pečate konkrétnej úrovne, tento členský štát má povinnosť uznať elektronický podpis alebo elektronickú pečať z iných členských štátov, ak sú rovnakej alebo vyššej úrovne. Vyslovene sa zakazuje, aby členský štát pre online službu vyžadoval elektronický podpis alebo elektronickú pečať vyššej úrovne bezpečnosti ako kvalifikovanú úroveň.[32]

Okrem vytvorenia právneho rámca upravujúceho služby dôvery, ktorý by mal zjednotiť právnu úpravu služieb dôvery vo všetkých právnych poriadkoch členských štátov, bola prijatá aj právna úprava týkajúca sa zavedenia povinnosti vzájomne uznávať prostriedky elektronickej identifikácie. Cieľom tejto úpravy je zabezpečiť, aby sa prostriedky elektronickej identifikácie jedného členského štátu dali použiť na identifikáciu a autentifikáciu pri využívaní služieb online, ktoré sú poskytované subjektmi verejného sektora iného členského štátu. Ustanovenia týkajúce sa zásady vzájomného uznávania sa dotknú nie len fyzických osôb, fyzických osôb podnikateľov a právnických osôb, ktorí primárne využívajú služby online, ale najmä orgánov verejnej správy, ktorí poskytujú svoje

---

25 Nariadenie eIDAS nedefinuje, čo možno považovať za služby online. Z textu predmetného nariadenia je však zrejmé, že ide o elektronické služby poskytované či už súkromným sektorom, ako aj subjektmi verejného sektora.

26 Body 5, 12 preambuly Nariadenia eIDAS.

27 V zmysle čl. 3 ods. 16 Nariadenia eIDAS možno za služby dôvery považovať elektronické služby, ktoré sa spravidla poskytujú za odplatu a spočívajú:

„a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo

b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo

c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia.“

28 Elektronickú pečať môžu používať len právnické osoby a pri jej vyhotovení neidentifikuje konkrétnu fyzickú osobu, tak ako pri elektronickom podpise. Preto ani vo forme kvalifikovanej elektronickej pečate nemá právne účinky vlastnoručného podpisu ako je to v prípade kvalifikovaného elektronického podpisu. Základným účelom elektronickej pečate je zabezpečiť integritu dokumentu a správnosť pôvodu dokumentu. Popri autentifikácii dokumentu vydaného právnickou osobou sa elektronické pečate môžu používať aj na autentifikáciu akéhokoľvek digitálneho majetku právnickej osoby, napríklad softvérového kódu alebo serverov.

29 Na kvalifikovanú elektronickú časovú pečiatku sa viaže domnienka správnosti dátumu a času, ktorý uvádza a integrity údajov, s ktorými je dátum a čas spojený.

30 Subjektom verejného sektora je v zmysle čl. 3 ods. 7 Nariadenia eIDAS: *„ústredný, regionálny alebo miestny orgán, verejnoprávny subjekt alebo združenie tvorené jedným alebo viacerými takýmito orgánmi alebo jedným či viacerými takýmito verejnoprávnymi subjektmi, alebo súkromný subjekt, ktorý aspoň jeden z takýchto orgánov, subjektov alebo združení poveril poskytovaním verejných služieb, keď koná na základe takéhoto poverenia.“*

31 Úspešná identifikácia a autentifikácia je predpokladom autorizácie, inými slovami povoleniu konať v súlade s oprávneniami, ktoré danej entite prislúchajú.

32 Čl. 27 a 37 Nariadenia eIDAS.

služby online. Na tomto mieste je nutné podotknúť, že od 1.7.2016 sa aplikuje Nariadenie eIDAS len v rozsahu upravujúcom služby dôvery. Povinnosť vzájomne uznávať prostriedky elektronickej identifikácie vznikne členským štátom až v roku 2018.[33]

Zásada vzájomného uznávania sa uplatňuje vtedy, keď je prostriedok elektronickej identifikácie členským štátom oznámený Komisii v rámci jeho schémy elektronickej identifikácie[34], ktorá musí spĺňať podmienky oznámenia v zmysle čl. 9 Nariadenia eIDAS a oznámenie musí byť uverejnené v Úradnom vestníku EÚ. Taktiež platí, že prístup k službám online a ich konečné poskytnutie žiadateľovi je spojené s právom na využívanie takýchto služieb na základe podmienok, ktoré sú stanovené vo vnútroštátnych právnych predpisoch. Inými slovami možno povedať, že napriek tomu, že sa osoba môže elektronicky autentifikovať pre prístup k službe online iného členského štátu, neznamená to, že automaticky má aj oprávnenie konkrétnu službu online využiť, nakoľko takéto oprávnenie sa môže vzťahovať na podmienku občianstva alebo trvalého pobytu v konkrétnej krajine a i.[35]

Je potrebné podotknúť, že v zmysle Nariadenia eIDAS je na rozhodnutí členských štátov, či oznámia Komisii všetky, niektoré alebo neoznámia žiadne schémy elektronickej identifikácie, ktoré sa používajú na vnútroštátnej úrovni na prístup aspoň k verejným službám online alebo ku konkrétnym službám.[36] V kontexte oznámenia resp. neoznámenia schémy elektronickej identifikácie však treba poznamenať, že členským štátom vznikne v roku 2018 povinnosť vzájomne uznávať prostriedky elektronickej identifikácie, ktoré boli oznámené v súlade s Nariadením eIDAS. Inými slovami, ak napr. občan Českej republiky bude chcieť využiť službu online poskytovanú orgánom verejnej správy Slovenskej republiky a Česká republika v súlade s Nariedením eIDAS oznámila schému elektronickej identifikácie, tak občan Českej republiky má právo sa autentifikovať pre využitie takejto služby.

4.1 Úrovne záruky[37]

Ďalšími podmienkami povinného vzájomného uznávania prostriedku elektronickej identifikácie iným členským štátom, je zaistenie úrovne záruky prostriedku elektronickej identifikácie (čiže úroveň záruky eID alebo iného tokenu osoby, ktorá chce využiť elektronickú službu v inom členskom štáte) vyššej alebo rovnakej ako tá, ktorú vyžaduje príslušný subjekt verejného sektora pre prístup k službe online za predpokladu, že úroveň záruky daných prostriedkov elektronickej identifikácie zodpovedá úrovni záruky „pokročilá“ alebo „vysoká“. Ďalšou podmienkou vzájomného uznávania prostriedku elektronickej identifikácie je, aby príslušný subjekt verejného sektora používal vo vzťahu k prístupu k danej službe online úroveň záruky „pokročilá“ alebo „vysoká“.[38] V prípade ak prostriedok elektronickej identifikácie má nižšiu úroveň záruky, členský štát ho môže, ale nemusí uznať pre potreby identifikácie pre služby online, ktoré poskytuje.[39]

Úrovne záruky by mali vyjadrovať stupeň spoľahlivosti prostriedku pre elektronickú identifikáciu pri určovaní totožnosti osôb, a tým poskytovať záruku, že osoba, ktorá deklaruje konkrétnu totožnosť, je skutočne osobou, s ktorou je táto totožnosť spojená. Úroveň záruky závisí od miery spoľahlivosti, ktorú daný prostriedok pre elektronickú identifikáciu u deklarovanej alebo uvedenej totožnosti osoby poskytuje s prihliadnutím na postup (identifikácia a autentifikácia), riadiacu

---

33 Tamtiež, čl. 52 ods. 2 písm. c).

34 V zmysle čl. 3 ods. 4 Nariadenia eIDAS sa za schému elektronickej identifikácie považuje: *„systém na elektronickú identifikáciu, v rámci ktorého sa fyzickým osobám alebo právnickým osobám alebo fyzickým osobám zastupujúcim právnické osoby vydávajú prostriedky elektronickej identifikácie.“* Podmienky, ktoré musí spĺňať schéma elektronickej identifikácie sú stanovené v čl. 6 ods. 1 Nariadenia eIDAS.

35 Napr. elektronické služby verejnej správy týkajúce sa sociálnych služieb alebo v prípade zavedenia elektronických volieb do Národnej rady Slovenskej republiky, či do orgánov územnej samosprávy.

36 Bod 13 preambuly Nariadenia eIDAS.

37 Slovenský preklad Nariadenia eIDAS používa pojem „úrovne zabezpečenia“. Domnievam sa, že preklad anglického pojmu „*assurance level*“ je v slovenskej verzii nesprávny a mal by sa skôr používať pojem „úroveň záruky“.

38 Čl. 6 písm. b) c) Nariadenia eIDAS. Úrovne záruky schém elektronickej identifikácie sú definované v čl. 8 Nariadenia eIDAS.

39 Bod 13 preambuly Nariadenia eIDAS.

činnosť (subjekt vydávajúci prostriedky pre elektronickú identifikáciu a postup vydávania týchto prostriedkov) a technické kontroly.[40]

Nariadenie eIDAS rozlišuje tri úrovne záruky, konkrétne „nízka", „pokročilá" a „vysoká". Pri definovaní týchto úrovní záruky sa vychádzalo z výsledkov rozsiahlych pilotných projektov financovaných prostriedkami EÚ a normalizačných a medzinárodných činností, ktoré obsahujú rôzne technické vymedzenia a opisy úrovní záruky. Konkrétne ide o projekt STORK *(Secure Identity Across Borders Linked*)[41] a normu ISO 29115 (*Information technology, Security techniques, Entity authentication assurance framework*),[42] kde sa okrem iného odkazuje na úrovne 2, 3 a 4, ktoré by sa mali pri vypracovaní minimálnych technických požiadaviek, noriem a postupov pre úrovne záruky „nízka", „pokročilá" a „vysoká" v zmysle Nariadenia eIDAS, v čo najväčšej miere zohľadňovať. Podrobnosti o jednotlivých úrovniach záruky stanovuje vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015.[43]

Cieľom projektu STORK bolo zabezpečiť jednoduchší prístup občanov EÚ, ako aj podnikateľov k online službám verejnej správy v iných členských štátoch. Autentifikácia pri naplnení tohto cieľa hrá dôležitú úlohu. V rámci naplnenia vyššie uvedeného cieľa bolo potrebné vytvoriť právny rámec pre vzájomné uznávanie národných elektronických identít medzi členskými štátmi, ako aj zabezpečiť interoperabilitu národných riešení elektronickej identity. Prijatím Nariadenia eIDAS a s účinnosťou ustanovení o vzájomnom uznávaní prostriedkov elektronickej identifikácie sa tieto problémy z väčšej časti odstránia. V rámci tohto projektu boli stanovené 4 úrovne záruky, ktoré sa týkajú požiadaviek na potrebnú záruku identity konkrétnej entity. Čím vyššie požiadavky, tým vyššia úroveň záruky. Výsledkom projektu bolo vytvorenie rámca *STORK Quality Authentication Assurance (ďalej len „QAA")*[44]*,* v rámci ktorého sa úrovne záruky určovali na základe organizačných aspektov, kde sa berie do úvahy kvalita identifikačného procesu, procesu vydania tokenu, certifikačnej autority, ako aj technických aspektov, ktorými sú druh a sila tokenu identity a kvalita mechanizmov použitá pri autentifikácii používateľa.[45] Zatiaľ čo sa organizačné aspekty týkajú registračnej fázy, v prípade organizačných aspektov ide o fázu elektronickej autentifikácie.

Ako už bolo spomenuté, úroveň záruky „nízka", „pokročilá" a „vysoká" upravená Nariadením eIDAS zodpovedná STORK QAA úrovni 2,3,4. Vo všeobecnosti pre určenie konkrétnej úrovne rozhoduje spoľahlivosť registračného procesu (subjekt vydávajúci eID, povinnosť fyzickej osoby osobne prevziať eID, a i.), ako aj samotný spôsob autentifikácie (typ autentifikačného nástroja typu heslo, token, PIN, certifikáty a i.). Následne sú jednotlivé úrovne záruky zoradené podľa vážnosti dopadu ujmy, ktorá by mohla nastať v prípade zneužitia identity. STORK QAA úroveň 2 predstavuje úroveň, ktorá by mala byť použitá pri tých službách, kde ujma v dôsledku zneužitia identity má malý dopad. Pri STORK QAA úrovni 3 by služba mohla utrpieť značnú ujmu v dôsledku zneužitia identity. STORK QAA úroveň 4 predstavuje najvyššiu úroveň záruky, kedy zneužitie identity spôsobí ťažkú ujmu. Každá úroveň záruky predstavuje určitý stupeň, v rámci ktorého je spoliehajúca sa strana (napr. poskytovateľ elektronickej služby verejnej správy) presvedčená, že v rámci elektronickej komunikácie

---

[40] Tamtiež, bod 16.

[41] [online]. Dostupné na internete:
https://www.eid-stork.eu/

[42] [online]. Dostupné na internete:
http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138

[43] Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

[44] Bližšie pozri: STORK, D2.3 - Quality authenticator scheme. [online]. Dostupné na: https://www.eid-stork.eu/dmdocuments/public/D2.3_final._1.pdf

[45] V podmienkach právneho poriadku Slovenskej republiky upravuje problematiku úrovne záruky výnos č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky zo 4. marca 2014 o štandardoch pre informačné systémy verejnej správy, konkrétne jeho príloha č. 6 - Úrovne autentifikácie elektronických služieb verejnej správy. Predmetná príloha vychádza z výsledkov projektu STORK. Je otázne nakoľko je táto príloha relevantná, pretože vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015 upravuje problematiku stanovenia úrovne záruky.

informácia o identite naozaj patrí entite, ktorej sa daná informácia týka. Poskytovateľ elektronickej služby verejnej správy bude musieť urobiť analýzu rizík (v prípade poskytnutia služby inej osobe ako oprávnenej osobe) a prideliť konkrétnu úroveň záruky.

5 ZÁVER

Proces elektronizácie verejnej správy a poskytovanie elektronických služieb prostredníctvom internetu prináša so sebou okrem pozitív aj mnohé bezpečnostné riziká. Práve pri otázkach bezpečnosti má problematika týkajúca sa identifikácie a autentifikácie v kontexte využívania elektronických služieb verejnej správy svoje opodstatnenie. Zavádzaním informačných a komunikačných technológií do verejnej správy sa prispelo aj k zmene konceptu identity. Pre spoľahlivé určenie elektronickej identity konkrétnej entity, či už ide o fyzickú osobu, fyzickú osobu podnikateľa alebo právnickú osobu, musia orgány verejnej správy jednoznačne vedieť, s kým komunikujú. Problém s identifikáciou a autentifikáciou identity bol na národnej úrovni do značnej miery vyriešený zavedením občianskych preukazov s elektronickým čipom, ktorý okrem funkcie dokladu totožnosti plní aj funkciu preukazovania a potvrdenia totožnosti v elektronickom prostredí. Možno povedať, že eID je vstupnou bránou k využívaniu elektronických služieb, ktoré sú poskytované orgánmi verejnej správy. Taktiež platí, že eID je založený na elektronickej identite uloženej a bezpečne chránenej v elektronickom čipe. Bezpečnosť eID je zabezpečená najmä tým, že údaje z eID je technicky možné prečítať len so súhlasom držiteľa eID, a to zadaním bezpečnostného osobného kódu.

Podpora idey bezpečného cezhraničného využívania elektronických služieb verejnej správy sa pretavila do prijatia Nariadenia eIDAS. Za základné ciele predmetného nariadenia možno považovať jednak posilnenie dôvery pri elektronických transakciách na vnútornom trhu, ale aj zabezpečenie bezpečnej elektronickej identifikácie a autentifikácie pri prístupe k cezhraničným službám online, ktoré ponúkajú členské štáty, aspoň v prípade verejných služieb. K naplneniu vyššie uvedených cieľov má prispieť vytvorenie právneho rámca upravujúceho služby dôvery vo všetkých členských štátoch, ako aj zavedenie povinnosti vzájomného uznávania prostriedkov elektronickej identifikácie. Neskôr uvedená povinnosť, ktorá vznikne členským štátom v roku 2018, by mala zabezpečiť, aby sa prostriedky elektronickej identifikácie jedného členského štátu dali použiť na identifikáciu a autentifikáciu pri využívaní elektronických služieb, ktoré poskytujú orgány verejnej správy iného členského štátu. Bezpečnú identifikáciu a autentifikáciu vo vzťahu k prístupu k danej službe online zaistia úrovne záruky, ktoré vyjadrujú stupeň spoľahlivosti prostriedku pre elektronickú identifikáciu pri určovaní identity konkrétnej entity, a tým poskytujú záruku, že entita, ktorá deklaruje konkrétnu identitu, je skutočne entitou, s ktorou je táto identita spojená.

Použitá literatúra:

DAŇKO, M.: Elektronický podpis ako prejav vôle (v rekodifikačných súvislostiach). In Míľniky práva v stredoeurópskom priestore 2015. Bratislava: Univerzita Komenského v Bratislave, 2015, s. 673-674.
NOIRIEL, G.: The identification of the citizen: the birth of republican civil status in France. In Documenting individual identity, the development of state practices in the modern world. Princeton and Oxford: Princeton University Press, 2001. S. 28-48.
OLEJÁR, D.: Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. 164 s. [online]. Dostupné na internete:
http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s
SOPÚCHOVÁ, S.: Predpoklady fungovania e-governmentu v Slovenskej republike. In QUAERE 2015 [elektronický zdroj] Hradec Králové : Magnanimitas, 2015. S. 659-668. ISBN 978-80-87952-10-8.
SULLIVAN, C.: Protecting digital identity in the cloud: Regulating cross border data disclosure. In Computer Law & Security Review. 2014, roč. 30, č. 2., s. 137-152.
ŠKROBÁK, J. In VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012, 480 s.
Nariadenie EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
Vykonávacie nariadenie Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej

identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
Zákon č. 224/2006 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov
Zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)
Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách).
Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy
MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY: Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti. Bratislava, 2008.
MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY: Stratégia informatizácie verejnej správy. Bratislava, 2008.
Modinis Study on Identity Management in eGovernment Common Terminological Framework for Interoperable Electronic Identity Management Consultation paper v2.01. 23. november 23. 2005. 18. s. [online]. Dostupné na internete: http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf
[online] Dostupné na internete <http://www.minv.sk/?operacny-program-informatizacia-spolocnosti-tlacove-informacie&sprava=odovzdali-sme-milionty-kus-elektronickeho-obcianskeho-prekazu-s-cipom>
STORK [online]. Dostupné na internete:
https://www.eid-stork.eu/
ISO 29115 [online]. Dostupné na internete:
http://www.iso.org/iso/catalogue_detail.htm?csnumber=45138

Kontaktné údaje:
Mgr. Jozef Andraško
jozef.andrasko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
P. O. Box 313
810 00 Bratislava
Slovenská republika

NEBEZPEČNÉ PRENASLEDOVANIE NA INTERNETE

Martin Daňko, Marek Mezei

Univerzita Komenského v Bratislave, Právnická fakulta

Abstrakt: Paper is dedicated to the actual issue arising on internet – dangerous persecution on internet – the so called cyberstalking. Cyberstalking is a new and widely spread phenomenom. Law enforcement authorities and courts deal with it relatively often. Where is the border between criminal act and misdemeanor? How intense has the cyberstalking has to be to prosecute an individual?.

Abstrakt: Príspevok autorov sa venuje problematike nebezpečného prenasledovania na internete, tzv. cyberstalkingu. Cyberstalking je pomerne novým a rozšíreným fenoménom s ktorým sa orgány činné v trestnom konaní a súdy stretávajú pomerne často. Kde je hranica priestupku a kedy je to už trestný čin? Akú intenzitu musí mať konanie páchateľa na to, aby sme stíhali konkrétnu osobu?

Kľúčové slová: cyberstalking, dangerous persectuion, criminal act, misdemeanor, internet
Kľúčové slová: cyberstalking, nebezpečné prenasledovanie, trestný čin, priestupok, internet

1 ÚVOD

Prudký rozvoj internetu a jeho rozšírenie nielen do domácností ale aj do prenosných zariadení (mobilný telefón, tablet a iné) spôsobil, že sú ľudia v zásade stále online. Komunikácia medzi dvomi osobami čím ďalej tým viac prebieha formou rôznych elektronických správ a sociálnych sietí. Tak ako množstvo iných vecí, tak aj takýto spôsob komunikácie má svoju odvrátenú stránku. Komunikácia prostredníctvom internetu môže byť zneužitá formou rôznych nevyžiadaných správ, obťažujúcich správ, nenávistných komentárov a pod. V rámci nasledujúceho príspevku sme sa venovali jednej konkrétnej forme zneužitia internetovej komunikácie, a to kontaktovaniu druhej osoby bez jej súhlasu. Nebudeme sa však venovať spamu, ktorým je zasielanie rovnakej správy s rovnakým obsahom veľkému okruhu osôb. Pokúsime sa dať odpoveď na otázku, kde je hranica medzi trestným činom a priestupkom a akú intenzitu musí mať takéto konanie, aby sme hovorili o trestnom čine.

2 TRESTNOPRÁVNY ROZMER

Trestné právo ako prostriedok ochrany istých vzťahov nerezignovalo na technologické zmeny v spoločnosti a reagovalo pridaním novej skutkovej podstaty trestného činu do zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej len ako „Tr. zák.“, „TZ“, alebo „Trestný zákon“). Doplnením skutkovej podstaty trestného činu nebezpečného prenasledovania podľa § 360a TZ sa vytvoril priestor pre postihovanie vyššie uvedeného nežiaduceho konania. Zavedenie tejto skutkovej podstaty bolo realizované novelou Trestného zákona, zákonom č. 262/2011 Z. z., ako reakcia na nárast útokov, ktoré jednotlivo nie sú trestnými činmi, ale v súhrne sú tak intenzívnymi zásahmi, že možno hovoriť o trestnoprávnom rozmere.

2.1 Trestný čin nebezpečného prenasledovania podľa § 360a TZ

Trestný čin nebezpečného prenasledovania je v oboch odsekoch prečinom. Trestný čin nebezpečného prenasledovania je pomerne široko koncipovaným trestným činom. Objektom nebezpečného prenasledovania sú medziľudské vzťahy a právo človeka na bezpečnuý a kvalitný život. Útoky sú potom smerované voči osobe v jej fyzickom zhmotnení.

Trestného činu nebezpečného prenasledovania sa podľa § 360a ods. 1 Tr. zák. dopustí ten „*Kto iného dlhodobo prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že (a) sa vyhráža ublížením na zdraví alebo inou ujmou jemu alebo jemu blízkej osobe, (b) vyhľadáva jeho osobnú blízkosť alebo ho sleduje, (c) ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli, (d) zneužije jeho osobné*

údaje za účelom získania osobného alebo iného kontaktu, alebo (e) ho inak obmedzuje v jeho obvyklom spôsobe života."

Samotnú objektívnu stránku trestného činu môžeme rozdeliť do dvoch elementárnych prvkov. Prvým prvkom je všeobecný opis konania, ktorý je následne doplnený alternatívne niektorým druhom špecifického konania. Pre naplnenie objektívnej stránky trestného činu nebezpečného prenasledovania sa vyžaduje naplnenie aspoň jedného konania z alternatívneho výpočtu v spojitosti s naplnením všeobecného opisu konania páchateľa.

Na naplnenie objektívnej stránky sa teda vyžaduje dlhodobé prenasledovanie. Čo si však máme predstaviť pod pojmom *dlhodobo*? Snaha nájsť všeobecnú odpoveď na túto otázku je podľa nášho názoru márna. Podmienka dlhodobosti bude podľa nášho názoru splnená v prípade, ak páchateľ v priebehu niekoľkých dní, niekoľkokrát za deň, fyzicky kontaktuje poškodeného. Nebude však podľa nášho splená za predpokladu, ak ide o kontakt prostredníctvom e-mailu a páchateľ pošle poškodenému dva-tri e-maily denne v priebehu niekoľkých dní.

Pri pojmovom znaku prenasledovanie musíme brať na zreteľ alternatívne vyjadrenie objektívnej stránky. Môže ísť teda o vzbudenie dôvodnej obavy o život alebo zdravie poškodeného alebo jemu blízkej osoby, alebo zhoršenie kvality života podstatným spôsobom. Alternatíva v podobe dôvodnej obavy o život alebo zdravie je pomerne jednoznačná. Ako kvalifikovať zhoršenie kvality života podstatným spôsobom? Zo znenia tejto alternatívy môžeme odvodiť, že nepostačuje akékoľvek zhoršenie kvality života. Za zhoršenie kvality života poškodeného môžeme podľa nášho názoru považovať akýkoľvek negatívny vplyv na život poškodeného. Ako sme už ale uviedli, akékoľvek zhoršenie kvality života nie je postačujúce. Odborná literatúra[1] tvrdí, že za zhoršenie kvality života treba považovať taký posun v kvalite života, ktorý osoba subjektívne vníma ako negatívum. S daným tvrdením sa stotožňujeme a nad rámec dopĺňame, že posúdenie následku v podobe zhoršenia kvality života podstatným spôsobom treba skúmať nielen objektívne, ale aj subjektívne. Zhoršenie kvality života podstatným spôsobom je potrebné klasifikovať ako pojem právny[2], nakoľko ide o jeden zo znakov skutkovej podstaty (následok). Vzhľadom na uvedenú skutočnosť teda o naplnení tohto pojmu rozhoduje orgány činný v trestnom konaní, resp. súd. Zhoršenie kvality života podstatným spôsobom musí byť predmetom podrobného dokazovania a ustálenia, v čom konkrétne malo spočívať a v čom konkrétne zhoršilo kvalitu života poškodeného.

K vyššie uvedenému konaniu musí pristúpiť následne niektoré z alternatívne vyjadrených konaní uvedených pod písmenami a) až e). V prípade cyberstalkingu pôjde o alternatívu uvedenú v § 360a ods. 1 písm c) – kontaktovanie prostredníctvom elektronickej komunikačnej služby.

Uvedenú alineu si ilustrujme na modelovom prípade. Bývala priateľka poškodeného sa nevie zmieriť so skutočnosťou, že poškodený je šťastne zadaný a má dieťa. Z tohto dôvodu začne poškodeného kontaktovať e-mailom na jeho pracovnú adresu. Následne začne takýmto spôsobom kontaktovať aj novú partnerku poškodeného, kolegov poškodeného v práci a pohostinstvo, ktoré poškodený navštevuje. Obsahom e-mailov sú vulgarizmi, oplzlosti a narážky sexuálneho charakteru. Konanie ex-priateľky trvá v zásade viac ako jeden rok, mesačne kontaktuje poškodeného cca. 3 – 4x.

V našom modelovom prípade je možné konštatovať splnenie dlhodobosti prenasledovania poškodeného, nakoľko časový aspekt je viac než postačujúci na to, aby sme mohli hovoriť o dlhodobosti. Zhoršenie kvality života podstatným spôsobom by bolo možné odvodiť z výsluchov poškodeného a jeho priateľky. Ak by napr. poškodený potvrdil, že v dôsledku týchto mailov má v súkromnom živote problémy (priateľka ho upodozrieva, že jej je neverný, kolegovia sa mu vyhýbajú, lebo ich obťažuje intímne detaily zo života poškodeného), tak dochádza podľa nášho názoru k jednoznačnému splneniu kvalitatívnej podmienky v podobe zhoršenia kvality života podstatným spôsobom. V danom prípade by bolo podľa nášho názoru irelevantné, či z e-mailov vyplýva možnosť stupňovania konania podozrivej. Tento náš názor potvrdzuje napríklad aj rozhodovacia činnosť súdov[3], ktorá hovorí, že za vytrvalý kontakt prostriedkami elektronickej komunikácie sa považuje hlavne opakované zasielanie nevyžiadaných e-mailových správ (často s vulgárnym alebo agresívnym obsahom). Samotný časový a kvalitatívny aspekt postačuje na to, aby sme za splnenia ďalších podmienok mohli uvažovať o naplnení skutkovej podstaty podľa § 360a Tr. zák. Naplnenie poslednej

[1] BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J.: Trestný zákon. Komentár. Osobitná časť. Praha: C H. Beck. 2011, s. 1206.

[2] Uznesenie Krajského súdu v Bratislave, sp. zn. 4To/62/2016.

[3] Uznesenie Nejvyššího soudu ČR, sp. zn. 8 Tdo 1107/2013-6.

podmienky, a to kontaktovanie prostredníctvom elektronickej komunikačnej služby je potom ľahko preukázateľné doložením e-mailovej komunikácie.

2.2 Trestný čin alebo priestupok?

Základnou tézou pri posudzovaní trestnej zodpovednosti je posúdenie naplnenia obligatórnych znakov skutkovej podstay. Pre spáchanie akéhokoľvek trestného činu uvedeného v osobitnej časti Trestného zákona sa vyžaduje, aby páchateľ naplnil všetky znaky skutkovej podstaty. Skutkovou podstatou trestného činu sa rozumie súhrn konkrétnych znakov, ktoré charakterizujú určité ľudské správanie a zákonodarca ho „povýšil" na trestný čin.

Podľa § 10 odsek 2 Trestného zákona sa nejedná o prečin, ak vzhľadom na spôsob vykonania činu a jeho následky, okolnosti za ktorých bol čin spáchaný, mieru zavinenia a pohnútku páchateľa je jeho závažnosť nepatrná. Z uvedeného ustanovenia § 10 ods. 2 Trestného zákona vyplýva, že pre trestnosť páchateľa sa vyžaduje okrem naplnenia formálnych znakov (obligatórnych znakov) trestného činu aj naplnenie takzvanej materálnej stránky trestného činu. Práve v ustanovení § 10 ods. 2 Tr. zák. je zakotvená výnimka z formálneho chápania kategórie trestných činov vo vzťahu k prečinu.

Je nevyhnutné konštatovať, že pri rozhodovaní o každom čine vykazujúcom formálne znaky prečinu, musí byť závažnosť prečinu obligatórne zvažovaná a posudzovaná. Nie je na svojvôli orgánov činných v trestnom konaní a súdu, či bude na závažnosť prečinu v konkrétnom prípade prihliadať. Ide o imperatív, ktorý orgánom činným v trestnom konaní a súdu kladie zákon.

V prípade, ak po zvážení všetkých kritérií dospeje orgán činný v trestnom konaní, resp. súd k záveru, že závažnosť spáchaného prečinu je nepatrná, nejde o prečin, a teda nejde o trestný čin.

S poukazom na uvedené je následne nevyhnutné rozmýšlať v intenciách zákona č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov. Konanie, ktoré nie je kvalifikované ako prečin nebezpečného prenasledovania podľa § 360a ods. 1 Trestného zákona z dôvodu aplikácie tzv. materiálneho korektívu je možné kvalifikovať ako úmyselné narušanie občianskeho spolunažívania schválnosťami a hrubm správaním sa voči poškodenému v zmysle § 49 ods. 1 písm. d) zákona o priestupkoch. Citované ustanovenie zákona o priestupkoch chráni občianske spolunažívanie pred jeho narušovaním hrubým spôsobom, resp. konaním, ktoré zasahuje do pokojného, usporiadaného a riadneho spolunažívania.

Vzhľadom na vyššie uvedené môžeme konštatovať, že nie každý kontakt páchateľa s poškodeným je trestným činom. Na to, aby sme mohli hovoriť o trestnom čine nebezpečného prenasledovania podľa § 360a Tr. zák. je potrebné naplniť aj kvalitatívnu stránku tohto trestného činu.

2.3 Aplikačná prax

Ako sme už v úvode príspevku naznačili, nebezpečné prenasledovanie sa relatívne často objavuje v rámci podaných trestných oznámení a orgány činné v trestnom konaní s ním prichádzajú do kontaktu. Na prvý pohľad by sa mohlo zdať, že vzhľadom na častý výskyt skutkov, ktoré by mohli mať znaky tohto trestného činu, bude úroveň rozhodnutí orgánov činných v trestnom konaní a súdov vysoká. Realita je však čiastočne odlišná.

Vzhľadom na to, že trestný čin nebezpečného prenasledovania je prečinom, musia orgány činné v trestnom konaní a súdy obligátorne posudzovať možnosť aplikácie § 10 ods. 2 Tr. zák. – tzv. materiálny korektív. Podľa nášho názoru dochádza k prepínaniu použitia materiálneho znaku v zmysle § 10 ods. 2 TZ, čo má za následok bagatelizovanie takéhoto konania.

V aplikačnej praxi väčšinou dochádza k podaniu trestného oznámenia poškodenou osobou, ktorú prenasleduje jej bývalý partner. Takéto trestné oznámenie je následne posudzované v súlade s ustanoveniami § 196 a nasl. Trestného poriadku. Vo väčšine prípadov je poškodená strana ochotná dodať orgánom činným v trestnom konaní aj dôkazový materiál, napr. vytlačenej e-mailovej komunikácie. Vo väčšine prípadov dochádza k odovzdaniu trestného oznámenia podľa § 197 ods. 1 písm. a) Trestného poriadku príslušnému orgánu na prejednanie priestupku. Orgány činné v trestnom konaní takéto svoje rozhodnutia odôvodňujú najmä materiálnym korektívom, prípadne nesprávne princípom *ultima ratio*.

Odovzdávať trestné oznámenie z dôvodu, že nejde o trestný čin ale o priestupok je samozrejme legitímny spôsob rozhodnutia v rámci postupu pred začatím trestného stíhania. Je však nesprávne, ak orgány činné v trestnom konaní posúdia napr. konanie podozrivej, ktorá niekoľkokrát týždenne v priebehu 2 rokov kontaktuje poškodeného, jeho blízky okruh známych a spolupracovníkov

prostredníctvom e-mailu a takýmto spôsobom ich obťažuje, ako priestupok a odovzdajú vec príslušnému orgánu na jeho prejednanie.

Problém na ktorý sa snažíme poukázať spočíva v uvedenom zľahčovaní situácie, snahy vsugerovať poškodenému myšlienku, že ide v zásade o neškodné konanie zo strany podozrivého, odvolávajúc sa napríklad na skutočnosť, že zo strany podozrivej nedochádza k stupňovaniu takéhoto konania.

2.4 Protiprávne konanie prostredníctvom Internetu

Prečin nebezpečného prenasledovania, ktorý je páchaný prostredníctvom elektronických komunikačných prostriedkov má svoje osobitosti a špecifiká vychádzajúce z použitých prostriedkov či foriem komunikácie. Aj internet je prostriedkom pre uskutočňovanie komunikácie, ale na to, aby sme dokázali pochopiť možnosti jeho využitia a z nich vyplývajúce právne limity, mali by sme sa najprv zamyslieť na pojmom internet a prípadne skúsiť si ho zadefinovať. Slovenský právny poriadok používa pojem internet a internetová komunikácia, ale nikde nenájdeme legálnu definíciu tohto pojmu. V našom poriadku je najrelevantnejšie ustanovenie, z ktorého by sme mohli legálnu definíciu pojmu Internet odvodiť, v zákone č. 351/2011 Z.z. o elektronických komunikáciách (ďalej len „ZEK"), a to konkrétne v ustanovení § 2 ods. 1 definujúce elektronickú komunikačnú sieť. V zmysle obsahu uvedenej definície je internet jeden z technických prostriedkov umožňujúci prenos signálu v elektronickej komunikačnej sieti ako funkčne prepojenej sústave prenosových systémov, a ak je to potrebné, prepájacích alebo smerovacích zariadení, vrátane sieťových prvkov, ktoré nie sú aktívne. Tu je potrebné uviesť, že vymedzenie internetu z technického hľadiska ako „sieť sietí", tzn. funkčne prepojenie všetkých sietí s ohľadom na technologickú neutralitu, slúžiace na prenos signálu, ktorého obsah je možné zobraziť prostredníctvom konkrétnych internetových služieb, nie je totožné s tým, ktoré vyplýva z ustanovenia § 2 ods. 1 ZEK. Predmetná skutočnosť len odôvodňuje požiadavku pojem Internet v právnom poriadku Slovenskej republiky zadefinovať.

Pri vyšetrovaní trestného činu nebezpečného prenasledovania, ktorý bol páchaný prostredníctvom Internetu, je nevyhnutné zohľadniť technicko-komunikačné možnosti Internetu, častokrát prejavujúce sa v intenzite páchateľovho protiprávneho konania. Veď napríklad nebezpečné prenasledovanie môže predstavovať aj zasielanie internetovej elektronickej pošty[4] bez konkrétneho obsahu ale v intenzite, ktorá dokáže vyvolať subjektívnu obavu ohrozenia adresáta[5]. Práve prostredníctvom Internetu resp. jeho služby internetovej elektronickej pošty môže byť intenzita páchania trestného činu výrazne vyššia, ako by to bolo v iných prípadoch (mimo využitia Internetu). Ad absurdum môže páchateľ vytvoriť alebo získať počítačový program, ktorý bude vytvárať a zasielať prostredníctvom internetovej elektronickej pošty vo veľmi veľkých množstvách (napríklad tisíce správ denne) správy poškodenému z obsahom. Autori zastávajú názor, že k naplneniu skutkovej podstaty prečinu nebezpečného prenasledovania by bolo postačujúce len samotné kvantitatívne hľadisko odosielaných správ, pokiaľ by dané konanie vyvolalo u adresáta podstatným spôsobom zhoršenie kvality jeho života.

Páchanie prečinu nebezpečného prenasledovania môže byť realizované na Internete prostredníctvom internetovej elektronickej pošty, ale aj pri využívaní služby WWW, v podobe internetových stránok, ktoré nazývame sociálne siete (napr. Facebook, Twitter, Google+, Linkedin)[6]. Na sociálnych sieťach je poškodený zaregistrovaný pod profilom, ktorý ho dostatočne dokáže identifikovať pred ostatnými používateľmi tejto sociálnej siete. V uvedených prípadoch sa tak vytvára vhodný kybernetický priestor pre páchanie prečinu nebezpečného prenasledovania. Páchateľ má zjednodušenú cestu k poškodenému a prostredníctvom komunikačných možností predmetnej internetovej stránky sociálnej siete (prostredníctvom pošty integrovanej v sociálnej sieti alebo zdieľania neželaných informácií na profile užívateľa) môže napĺňať skutkovú podstatu predmetného prečinu. Funkcionalita užívateľských oprávnený dáva možnosť užívateľovi si na sociálnych sieťach spravovať svoj profil najmä v podobe nastavení rozsahu zobrazenia obsahu tohto profilu pre iných užívateľov, ale aj obmedzenia komunikačných možností s ostatnými užívateľmi tak, aby sa eventualita páchania tohto prečinu mohla značne zredukovať. No v zásade tieto užívateľské oprávnenia

[4] Zákon č. 531/2011 Z.z. v prílohe č. 2 s názvom *Kategória uchovávaných údajov* používa pojem internetová elektronická pošta.

[5] Bližšie pozri: SMEJKAL, V.: Kybernetická kriminalita. Plzeň: Aleš Čenek, 2015, s. 275

[6] Bližšie pozri: SMEJKAL, V.: Kybernetická kriminalita. Plzeň: Aleš Čenek, 2015, s. 157

poškodený využíva v čase, kedy už došlo k protiprávnemu konaniu a poškodený sa voči takémuto protiprávnemu konaniu len bráni. V tejto situácií môže poškodený zabrániť vzniku závažnejších následkov páchateľovho konania, no táto skutočnosť musí byť zohľadnená pri posudzovaní závažnosti páchateľovho konania. Nie je želaný fakt, aby aktívne konanie poškodeného v podobe zablokovania prístupu páchateľa k jeho profilu na sociálnych sieťach, ktorým došlo odvráteniu vzniku závažnejších následkov, viedlo orgány činné v trestnom konaní k zľahčovaniu protiprávneho konania páchateľa a kvalifikáciu jeho protiprávneho konania ako priestupku.

Pri páchaní prečinu nebezpečného sledovania prostredníctvom Internetu by nemala skutočnosť, že poškodení vie blokovať prístup poškodeného k jeho internetovej elektronickej pošte alebo k osobným profilom na internetových stránkach sociálnych sietí, byť dôvodom pre zľahčovanie páchateľovho konania. Poškodení sa obracajú na orgány činné v trestnom konaní aj z dôvodu očakávania rýchleho a efektívneho zásahu proti páchateľovi. Efektívnym zásahom v súvislosti s protiprávnym konaním napĺňajúcim skutkovú podstatu prečinu nebezpečného prenasledovania sú úkony, na základe ktorých je podnik poskytujúci elektronické komunikačné služby povinný v zmysle § 63 ods. 6, ods. 14 písm. c), ods. 15 ZEK poskytnúť súčinnosť pri zisťovania informácií, ktoré sú predmetom telekomunikačného tajomstva.

Internet nám poskytuje slobodu ale zároveň v prípadoch, kedy s jeho využitím dochádza k páchaniu protiprávnej činnosti, aj bezmocnosť, proti ktorej sa dá bojovať len rýchlym a efektívnom konaním orgánov činných v trestnom konaní za súčinnosti podnikov, ktoré poskytujú elektronické komunikačné siete a služby, nakoľko bolo by nesprávne sa domnievať, že pri páchaní trestného činu nebezpečného prenasledovania ide len v prípadoch, kedy je páchateľ poškodenému známy.

3 ZÁVER

V predkladanom príspevku sme sa venovali problematike nebezpečného prenasledovania na internete. Uvedenú problematiku rieši aj zákonodarca v rámci trestného činu nebezpečného prenasledovania v § 360a Trestného zákona. Nie každý nevyžiadaný e-mail alebo správa na sociálnej sieti napĺňa túto skutkovú podstatu. Práve naopak, podľa nášho názoru je potrebné veľmi citlivé a dôsledné posudzovanie konania páchateľa a následku tohto konania orgánmi činnými v trestnom konaní a súdom. Na otázky, ktoré sme si položili v úvode tohto príspevku neexistuje jednoznačná a zovšeobecňujúca odpoveď. Každý jeden prípad, ktorý vykazuje znaky nebezpečného prenasledovania musí byť posudzovaný striktne individuálne a starostlivo. Na prvý pohľad neškodné vynucovanie pozornosti prostredníctvom nevyžiadaných správ môže skončiť s fatálnymi, resp. závažnejšími následkami. Pokiaľ ide o ojedinelý skutok páchateľa, ktorý skončí po uplynutí nejakého časového obdobia, mal by byť podľa nášho názoru posudzovaný skôr ako priestupok. Určite však nie je možné generalizovať a uzavrieť skutok páchateľa odovzdaním veci na prejednanie priestupku s odôvodnením, že v prípade opakovania takéhoto konania nastúpi trestnoprávna represia. Nedôsledným posudzovaním konania a okolností spáchania skutku sa môže pravdepodobnosť páchateľovho ďalšieho pokračovania v tejto činnosti zvyšovať a skončiť spáchaním niektorého z trestných činov proti životu a zdraviu alebo iných závažnejších trestných činov.

Použitá literatúra:

BURDA, E., ČENTÉŠ, J., KOLESÁR, J., ZÁHORA, J.: Trestný zákon. Komentár. Osobitná časť. Praha : C H. Beck. 2011, 1568 s. ISBN: 978-80-7400-394-3.
SMEJKAL, V.: Kybernetická kriminalita. Plzeň: Aleš Čenek, 2015, 636 s. ISBN: 978-80-7380-501-2
Uznesenie Krajského súdu v Bratislave, sp. zn. 4To/62/2016.
Uznesenie Nejvyššího soudu ČR, sp. zn. 8 Tdo 1107/2013-6.

Kontaktné údaje:

Mgr. Martin Daňko, PhD.
martin.danko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Ústav práva informačných technológií a práva duševného vlastníctva
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

JUDr. Marek Mezei
marek.mezei@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Katedra trestného práva, kriminológie a kriminalistiky
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

ONLINE HAZARD A JEHO BLOKOVANIE[1]

Tomáš Gábriš

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The paper analyses the newly proposed amendment to the Slovak Gambling Act and identifies its inconsistencies with the case-law of the CJEU such as that the seat of a gambling service provider to be located in the territory of Slovakia without any acceptable reason, and that the reasons for restricting the freedom to provide gambling services from abroad seem to be of a rather economic nature. Additionally, the proposed regulation will most probably not be efficient and can easily be circumvented.

Abstrakt: Príspevok analyzuje navrhovanú novelu zákona o hazardných hrách a upozorňuje na nesúlad s judikatúrou SDEÚ v dvoch aspektoch: požiadavke sídla poskytovateľa služieb na území SR, a v odôvodnení obmedzenia cezhraničného poskytovania hazardných služieb primárne ekonomickými dôvodmi. Napokon, celkovo možno mať za to, že navrhovaná úprava bude neefektívna a pomerne ľahko obchádzateľná.

Keywords: gambling, online gambling, freedom to provide services

Kľúčové slová: hazard, online hazard, sloboda poskytovania služieb

1 ÚVOD

Príspevok reaguje na v čase odovzdania tohto textu (v októbri 2016) aktuálny legislatívny proces novelizácie zákona č. 171/2005 Z. z o hazardných hrách. Hodnotí navrhovanú novelu vo svetle programových dokumentov a vyjadrení orgánov Európskej únie (EÚ), a osobitne vo svetle judikatúry Súdneho dvora EÚ (SDEÚ) vo vzťahu k regulácii cezhraničného poskytovania služieb hazardu, špeciálne online hazardu. Vo svetle ustálenej judikatúry SDEÚ sa pritom javí, že navrhovaný text novely, obdobne ako ani doterajší stav úpravy poskytovania hazardných služieb v Slovenskej republike nie sú v súlade s právom EÚ a Slovenská republika tak môže potenciálne čeliť žalobe zo strany zahraničných poskytovateľov služieb (online) hazardu.

2 ONLINE HAZARD V PRÁVE EÚ

Podľa aktuálnych odhadov Európskej komisie predstavujú hazardné služby[2] a v rámci nich osobitne služby online hazardu veľmi významný trh, s očakávanými tržbami poskytovateľov online hazardu vo výške 13 miliárd eur za rok 2015.[3] Napriek takémuto významnému ekonomickému rozmeru však predstavuje trh s hazardnými službami jeden z mála príkladov doteraz nejednotného trhu, resp. trhu, ktorý ani v podmienkach ekonomickej a politickej integrácie EÚ nie je „voľným".

[1] Príspevok bol spracovaný v rámci projektu **VEGA č. 1/0136/15** „**Právna úprava správneho trestania**" udeleného Vedeckou grantovou agentúrou Ministerstva školstva, vedy, výskumu a športu SR a Slovenskej akadémie vied.

[2] Podľa staršej správy Európskej komisie pritom asi 30 % z objemu hazardných služieb pripadá na športové stávkovanie, a asi 70% na iný hazard. Pozri Zelená kniha o online hazardných hrách na vnútornom trhu. Dostupné na internete: http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_sk.pdf (navštívené dňa 27.10.2016).

[3] Dostupné na internete: http://ec.europa.eu/growth/sectors/gambling_sk (navštívené dňa 27.10.2016).

Rôznorodé štúdie,[4] rezolúcie,[5] vyjadrenia,[6] správy,[7] zelené knihy,[8] ako aj odporúčania orgánov EÚ,[9] vrátane judikatúry SDEÚ[10] jednomyseľne tento stav akceptujú. Zároveň je však potrebné dodať, že ho neakceptujú bezvýnimočne – nie sú totiž ochotné akceptovať akékoľvek ľubovoľné prekážky voľného trhu, ale iba také obmedzenia, ktoré sú v jednotlivých členských štátoch EÚ opodstatnené osobitnými dôvodmi, a ktoré vo svojej rozhodovacej činnosti podrobne zhrnul a vymedzil SDEÚ ako akceptovateľné.

Z hľadiska primárneho práva EÚ, teda zakladajúcich (a následných) zmlúv,[11] spadajú totiž služby týkajúce sa hazardných hier, ako to potvrdil aj SDEÚ v prípade Schindler, pod článok 56 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ"),[12] a vzťahujú sa teda na ne pravidlá o voľnom pohybe (poskytovaní) služieb. Prevádzkovatelia, ktorým bolo udelené povolenie na poskytovanie týchto služieb v jednom členskom štáte, by preto mali byť oprávnení na základe tohto povolenia poskytovať svoje služby aj v iných členských štátoch, pokiaľ tieto štáty nezavedú obmedzenia z dôvodov vnímaných ako dôvody verejného záujmu, akými sú najmä ochrana spotrebiteľa alebo všeobecná potreba zachovať verejný poriadok.[13] Dané dôvody však nemôžu byť iba predstierané, a tiež platí, že ich treba vykladať reštriktívne.

Ako akceptovateľné dôvody pre obmedzenie trhu s hazardnými službami vo verejnom záujme SDEÚ podľa ustálenej praxe (formulovanej napr. v prípade Gambelli) konkrétne uznáva najmä nasledujúce argumenty:

- verejný poriadok,
- predchádzanie podvodom a iným trestným činom,[14]
- obmedzenie hráčskej vášne, obmedzenie márnotratnosti,
- sociálny poriadok, ochrana morálnych a kultúrnych hodnôt, a
- predídenie tomu, aby hazard predstavoval zdroj súkromného obohatenia.

---

4 Study Of Gambling Services In The Internal Market Of The European Union : Final Report (2006). Dostupné na internete: http://ec.europa.eu/internal_market/services/docs/gambling/study1_en.pdf (navštívené dňa 27.10.2016).

5 Opakované rezolúcie Európskeho parlamentu – European Parliament resolution on the integrity of online gambling (2009, 2011, 2013).

6 Napríklad: European Commission Communication Towards a comprehensive European framework on online gambling (2012).

7 Možno uviesť napr. Správu predsedníctva o súčasnom stave z 1. decembra 2008 (referenčný dokument 16022/08), Správu predsedníctva o súčasnom stave z 3. decembra 2009 (referenčný dokument 16571/09), či Správu predsedníctva o súčasnom stave z 25. mája 2010 (referenčný dokument 9495/10).

8 Zelená kniha o online hazardných hrách na vnútornom trhu (Green Paper on online gambling in the internal market) z roku 2011.

9 Pozri najmä Odporúčanie Komisie č. 2014/478/EÚ o zásadách ochrany spotrebiteľov a hráčov využívajúcich služby online hazardných hier a o predchádzaniu hraniu online hazardných hier (2014).

10 Schindler, C-275/92; Läärä and others, C-124/97; Zenatti, C-67/98; Anomar and others, C-6/01; Gambelli and others , C-243/01; Lindman, C-42/02; Placanica & others, C-338/04, C-359/04 & C-360/04; Liga portuguesa (Santa Casa), C-42/07; Sporting exchange (Betfair) C-203/08; Ladbrokes, C-258/08; Sjöberg and Gerdin, C-447 & 448/08; Winner Wetten, C-409/06; Markus Stoss C-316/07; Carmen media, C-46/08; Engelmann, C-64/08; Stanleybet 2011-2016; Sebat Ince C-336/14.

11 Pokiaľ ide o európske sekundárne právo, teda predpisy vydávané orgánmi Európskej únie, na služby v oblasti hazardných hier sa nevzťahujú žiadne špecifické predpisy o hazarde (smernice, nariadenia).

12 ANDERSON, P. M. – BLACKSHAW, I. P. – SIEKMANN, R. C. R. – SOEK, J.: Sports Betting : Law and Policy. The Hague : T.M.C. Asser Press, 2012, s. 137.

13 Zelená kniha o online hazardných hrách na vnútornom trhu. Dostupné na internete: http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_sk.pdf (navštívené dňa 27.10.2016).

14 Tento argument je osobitne vhodný na obmedzenie voľného poskytovania služieb hazardu. Porovnaj: ROMPUY, B. van: The French "betting right": a legislative Dr. Jekyll and Mr. Hyde. Dostupné na internete: http://www.asser.nl/SportsLaw/Blog/post/the-french-betting-right-a-legislative-dr-jekyll-and-mr-hyde-by-prof-dr-ben-van-rompuy (navštívené dňa 27.10.2016).

SDEÚ má totiž za to, že práve tieto a iné porovnateľné záujmy a argumenty proporcionálne ospravedlňujú obmedzenie voľného trhu služieb hazardu.

SDEÚ pritom výslovne uvádza aj príklady argumentov, ktoré sú neakceptovateľné – vyslovene vylúčený je tak najmä argument predídenia rozpočtovej strate alebo predídenia zníženiu daňových výnosov členského štátu EÚ.

Podobné kritériá zopakoval SDEÚ aj v prípade Carmen media, kde síce akceptoval argument ochranou zdravia (v zmysle predchádzania závislostiam) a verejného poriadku, ale zároveň upozornil na to, že je nutné prihliadať aj na prípadnú vnútroštátnu propagáciu/reklamu hazardu, ktorá môže byť v zjavnom rozpore s inak tvrdenou ochranou zdravia, a môže teda odhaľovať účelovosť argumentu použitého na zabránenie vstupu zahraničných poskytovateľov hazardu na domáci trh.

Nakoniec uvedieme ešte jeden posledný, pre náš príspevok relevantný prípad, a to rozhodnutie SDEÚ vo veci Engelmann, v ktorom SDEÚ skonštatoval, že podmienka, aby mali všetci poskytovatelia služieb hazardu sídlo na území štátu, v ktorom poskytujú svoje služby, je v podmienkach Európskej únie a vzájomného uznávania rozsudkov, ako aj medzinárodnej spolupráce štátnych orgánov disproporčná, a nemôže slúžiť ako akceptovateľný prostriedok obmedzovania voľného trhu služieb hazardu pod zámienkou potreby zvýšenej kontroly poskytovateľov hazardných služieb.

3 PRÁVNA ÚPRAVA (ONLINE) HAZARDU V SLOVENSKEJ REPUBLIKE

Aktuálna právna úprava (online) hazardu v Slovenskej republike, účinná v čase odovzdávania tohto príspevku (k 31.10.2016) obsahuje viaceré obmedzenia voľného trhu v oblasti poskytovania služieb hazardu, vrátane online hazardu. Obmedzenia slobodného trhu predstavujú v podmienkach Slovenskej republiky najmä nasledujúce podmienky poskytovania služieb hazardných hier:[15]

- zákaz prevádzkovania zahraničných hazardných hier na území SR
- licenciu môže získať iba právnická osoba so sídlom na území SR
- právnická osoba musí mať právnu formu akciovej spoločnosti alebo spoločnosti s ručením obmedzeným; akciová spoločnosť musí mať zaknihované akcie
- pri lotériách súčasťou názvu musí byť označenie „národná loterijná spoločnosť"
- prevod akcií spoločnosti na inú právnickú alebo fyzickú osobu sa zakazuje.

V Slovenskej republike teda platí, že na rozdiel od niektorých iných členských štátov EÚ, ktoré uznávajú zahraničné licencie na poskytovanie služieb hazardu, udelené v iných členských štátoch EÚ, o ktorých udelení boli ostatné členské štáty informované prostredníctvom tzv. bielej listiny, Slovenská republika takúto možnosť nepozná. Podobne, hoci niektoré iné členské štáty zvyknú pri udeľovaní svojich vnútroštátnych licencií zohľadniť licencie nadobudnuté v iných členských štátoch, hoci stále uplatňujú režim dvojitej licencie,[16] v prípade Slovenskej republiky neplatí ani táto možnosť zohľadňovania zahraničnej licencie aspoň ako okolnosti prisvedčujúcej udeleniu licencie pre územie Slovenskej republiky. O licenciu sa teda v Slovenskej republike môže uchádzať iba spoločnosť so sídlom na Slovensku (v čom možno konštatovať prvý rozpor s judikatúrou SDEÚ – konkrétne s rozhodnutím Engelmann), bez akéhokoľvek zohľadňovania toho, či je držiteľom licencie v inom členskom štáte EÚ. Navyše cezhraničné poskytovanie hazardu zo zahraničia na územie Slovenskej republiky sa výslovne zakazuje, čo si vyžaduje osobitne skúmať dôvody takéhoto obmedzenia, a ich súlad s dôvodmi akceptovanými SDEÚ v jeho ustálenej judikatúre (k tomu viac nižšie). Napriek výslovnému zákazu poskytovania zahraničných hazardných služieb na území Slovenska však v súčasnosti v Slovenskej republike chýba osobitná, výslovná úprava dôsledkov takéhoto zákazu cezhraničného poskytovania služieb hazardu, ďalej akákoľvek úprava efektívnych spôsobov vynucovania takéhoto zákazu, a napokon vôbec akékoľvek špecifické pravidlá pre cezhraničné poskytovanie služieb „online" hazardu.

Pokusy o výslovnú reguláciu podrobností ohľadom zákazu cezhraničného poskytovania služieb hazardu, osobitne online hazardu, a to konkrétne vo forme jeho blokovania, pritom už v minulosti boli slovenskej verejnosti aj zákonodarnému zboru predložené, ale boli neúspešné – a to

---

15 http://ec.europa.eu/internal_market/services/docs/gambling/study2_en.pdf (navštívené dňa 27.10.2016).

16 Pozri Zelená kniha o online hazardných hrách na vnútornom trhu. Dostupné na internete: http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_sk.pdf (navštívené dňa 14.11.2011).

z viacerých dôvodov: Ministerstvo financií SR tak konkrétne ešte v roku 2010 predložilo do pripomienkového konania návrh zákona, ktorým sa mal zmeniť a doplniť zákon č. 171/2005 Z. z. o hazardných hrách,[17] a ktorým sa sledovali vyššie naznačené ciele. Návrh zákona však bol svojím obsahom viac ako problematický, a to nielen z hľadiska práva EÚ, ale aj z hľadiska základných ústavných princípov a ochrany základných práv a slobôd. O tom, ktoré webové sídla ako sídla poskytovateľov zakázaného cezhraničného online hazardu mali byť blokované, mal totiž rozhodovať samotný Daňový úrad Bratislava a nie súd, čo samo osebe znamenalo neprimeraný zásah do základných práv. Navyše, aj z pohľadu práva EÚ kritici tejto navrhovanej úpravy už v roku 2010 zdôrazňovali, že z odôvodnenia návrhu jednoznačne vyplývalo jeho motivovanie výlučne ekonomickým záujmom Slovenskej republiky – zvýšením príjmov štátneho rozpočtu.[18] Napokon, správne poukazovali aj na pomerne jednoduché spôsoby obchádzania blokovania, a teda celkovú neefektívnosť tejto navrhovanej úpravy.

Najmä pod ťarchou týchto argumentov, ale aj pod argumentom negatívnych vplyvov na podnikateľské prostredie a negatívnych vplyvov na informatizáciu spoločnosti neefektívnym a predpokladane nadmerným (disproporčným) blokovaním služieb elektronických komunikácií (služieb informačnej spoločnosti), a napokon tiež pod argumentom neproporčného obmedzovania slobody pohybu kapitálu[19] Ministerstvo nakoniec od tohto svojho návrhu upustilo.

4 ROK 2016: NAVRHOVANÁ NOVELA ZÁKONA O HAZARDNÝCH HRÁCH

Novela zákona č. 171/2005 Z. z. o hazardných hrách, ktorá sa v súčasnosti (október 2016) nachádza v legislatívnom procese v Národnej rade Slovenskej republiky opäť vykazuje viaceré podobné vady ako doterajšia právna úprava, ale tiež tie isté vady ako mala už kritizovaná úprava navrhovaná v minulosti – stále sa totiž zachováva v prípade Engelmann kritizovaná diskriminačná požiadavka sídla poskytovateľa hazardnej služby na území Slovenska, a okrem toho sa opätovne navrhuje aj zavedenie prísnejšej a podrobnejšej úpravy zameranej proti zahraničným – na Slovensku nelicencovaným – poskytovateľom hazardných hier (prostredníctvom blokovania webových sídiel zahraničných poskytovateľov služieb hazardu), a to opäť s obdobnými nedostatkami, ktoré sa vyčítali už návrhu z roku 2010.

Podľa všeobecnej časti dôvodovej správy k navrhovanej novele, „*V rámci aktuálnej ponuky na trhu hazardných hier prostredníctvom elektronických komunikačných sietí, najmä internetu, sú k dispozícii hazardné hry nielen licencovaných spoločností – prevádzkovateľov hazardných hier, ktorí spĺňajú podmienky platného zákona o hazardných hrách, ale aj ponuka spoločností, ktoré nerešpektujú platnú slovenskú právnu úpravu pre oblasť podnikania vo sfére hazardných hier. Tieto subjekty neplnia rovnaké podmienky na prevádzkovanie hazardných hier, čo vedie k ich nerovnakému postaveniu na trhu a predstavuje tak jednoznačnú konkurenčnú výhodu voči licencovaným subjektom, ktoré zákonné podmienky súvisiace napr. s ochranou verejného poriadku, spotrebiteľa, či prevenciou kriminality plnia. Tieto spoločnosti tým, že nerešpektujú platnú slovenskú právnu úpravu pre oblasť podnikania vo sfére hazardných hier, je ich ponuka pre hráčov častokrát výhodnejšia, ako ponuka licencovaných subjektov. V snahe obmedziť prienik ponuky nelicencovaných operátorov a jeho dostupnosť na území Slovenskej republiky sa navrhuje zadefinovať takúto ponuku ako zakázanú a zároveň zaviesť opatrenia znemožňujúce prístup k poskytovaniu takejto ponuky. Opatrenia by spočívali najmä v možnosti blokovania stránok s nelegálnym obsahom ponuky hazardných hier pri súčasnom blokovaní platieb súvisiacich s hrou na takýchto stránkach a to na základe príkazu súdu*.“

---

17 Pozri http://www.eisionline.org/index.php/sk/10-projekty/novinky-z-aktivit/5-hazardny-navrh-zakona (navštívené dňa 27.10.2016).

18 Tamže.

19 Pozri tamže: „*Prijatie článku III by vo svojich dôsledkoch mohlo znamenať aj porušenie článku 63 Zmluvy o fungovaní Európskej Únie. Ten totiž zakazuje všetky obmedzenia pohybu kapitálu a platieb medzi členskými štátmi navzájom ako aj členskými štátmi a tretími krajinami. Podľa tohto návrhu zákona má však práve k takémuto obmedzeniu dôjsť, keďže poskytovateľovi platobnej služby sa ukladá povinnosť neposkytnúť platobné služby alebo nevykonať platobnú operáciu vo vzťahu k platobnému účtu uvedenému v zozname zakázaných ponúk. Blokovanie platieb sa môže zakladať na „kóde kategórie obchodníka“ (MerchantCategory Code – MCC). Zákaz spracovania platieb spojených s určitým kódom však môže zablokovať zákonné obchodné transakcie, ktoré nepredstavujú platby v súvislosti so stávkami a výhrami*.“

Táto argumentácia pritom znie akokoľvek inak, len nie ako argumentácia ochranou verejného poriadku, zdravia, či predchádzaním trestnej činnosti. Skôr má bližšie k argumentácii primárne ekonomickej, chrániacej slovenských poskytovateľov služieb hazardu.

Osobitná časť dôvodovej správy k bodu 30 v tejto línii argumentácie pokračuje ďalej: „*Ich ponuka pre hráčov hazardných hier, na území Slovenskej republiky je častokrát výhodnejšia ako ponuka licencovaných subjektov z dôvodu neplnenia zákonných podmienok a je v rozpore s dobrými mravmi, čím predstavuje nežiaduci prvok v podnikaní v oblasti hazardu. V snahe zamedziť pokračovaniu uvedenej situácie sa navrhuje úprava, ktorá je zameraná na obmedzenie dostupnosti hazardných hier, na prevádzkovanie ktorých nebola udelená alebo vydaná príslušná licencia podľa slovenských právnych predpisov a ktoré prostredníctvom elektronických komunikačných sietí a služieb (internetu) ponúkajú predovšetkým zahraničné spoločnosti*.“

Za týmto účelom sa navrhuje inštitút tzv. zakázanej ponuky, t.j. ponuky zahraničných poskytovateľov bez slovenskej licencie (bez ohľadu na to, či majú zahraničnú licenciu), a to konkrétne v § 2 zákona o hazardných hrách, do ktorého sa má doplniť písmeno u) definujúce zakázanú ponuku ako: „...*propagovanie hazardnej hry alebo prevádzkovanie hazardnej hry dostupnej na území Slovenskej republiky bez licencie podľa tohto zákona prostredníctvom elektronickej komunikačnej siete.*“ K tomu novonavrhovaný § 3 ods. 3 posledná veta zákona dopĺňa: „*Prevádzkovať hazardnú hru a propagovať hazardnú hru, na ktorú nebola udelená alebo vydaná licencia podľa tohto zákona, sa zakazuje*.“ Týmito dvoma ustanoveniami by tak zrejme mala byť vylúčená aj akákoľvek reklama ilegálnych poskytovateľov hazardných (online) hier na území Slovenska.

Podľa novonavrhovaného znenia § 11 ods. 2 ďalej platí, to bude „*Finančné riaditeľstvo Slovenskej republiky*“ kto „*vykonáva dozor nad poskytovaním zakázaných ponúk, ...*“ Ak v zmysle dôvodovej správy k bodu 30, „*Navrhovaným ustanovením sa vymedzuje pôsobnosť orgánu dozoru, t.j. Finančnému riaditeľstvu SR v oblasti dozoru nad poskytovaným zakázaných ponúk a určuje sa obsah zoznamu subjektov poskytujúcich zakázané ponuky*.“ Zoznam zakázaných ponúk teda má primárne vytvárať Finančné riaditeľstvo ako rozpočtová organizácia Ministerstva financií SR, ktoré má zároveň za úlohu prípadne komunikovať s prevádzkovateľmi takýchto služieb, a podávať návrhy na súd za účelom súdneho blokovania webového sídla ilegálneho poskytovateľa hazardných služieb: „*stanovuje povinnosť orgánu dozoru komunikovať s fyzickou alebo právnickou osobou s cieľom ukončenia jej činnosti v oblasti poskytovania zakázaných ponúk. Stanovuje sa postup vyradenia zakázaných ponúk zo zoznamu subjektov poskytujúcich zakázané ponuky, resp. ich nezaradenia v prípade, ak sa preukáže, že nie sú/nepoužívajú sa na poskytovanie zakázanej ponuky alebo bola zakázaná ponuka odstránená (prevádzkovanie a propagovanie hazardnej hry bez licencie prestalo byť dostupné z územia Slovenskej republiky). V tejto súvislosti sa stanovuje kompetencia orgánu dozoru vyžadovať od poskytovateľa platobných služieb identifikáciu používateľa platobných služieb a ďalšie informácie o používateľovi platobných služieb, ktorý je dozorovaným subjektom. V prípade, ak nedôjde k odstráneniu poskytovania zakázanej ponuky, Finančné riaditeľstvo Slovenskej republiky požiada Krajský súd v Banskej Bystrici o vydanie príkazu súdu na zamedzenie prístupu k webovému sídlu, prostredníctvom ktorého je zakázaná ponuka poskytovaná a zamedzenie vykonaniu platobnej operácie a inej platobnej služby v prospech účtu, ktorý používa osoba poskytujúca zakázanú ponuku na účely prijímania vkladu pri poskytovaní zakázanej ponuky. Príkaz súdu zverejní Finančné riaditeľstvo Slovenskej republiky na svojom webovom sídle a doručí ho osobám určeným v tomto príkaze. Ak pominú dôvody pre vydanie príkazu súdu, Finančné riaditeľstvo Slovenskej republiky požiada tento súd o zrušenie príkazu*.“ Novela teda predpokladá blokovanie webových sídiel rovnako ako aj blokovanie platobných operácií, obdobne ako to predpokladal už návrh z roku 2010, avšak tentokrát na základe rozhodnutia súdu.

Zásadná otázka tu však stále zostáva nezodpovedaná – ohľadom súladu takejto navrhovanej úpravy s ustálenou judikatúrou SDEÚ. Už sme pritom poukázali na fakt, že novela neodstraňuje doterajšiu požiadavku, aby poskytovateľ služieb mal sídlo na území Slovenskej republiky, čo SDEÚ odmietol v prípade Engelmann. To je však iba prvý z problémov, ktorý v súvislosti s navrhovanou novelou vidíme. Ďalším problémom je odôvodnenie, ktoré novela v súvislosti so sprísňovaním zákonnej úpravy obmedzenia voľného trhu uvádza. Kým totiž SDEÚ jasne vyslovil (v prípade Gambelli), že ekonomické dôvody nie sú akceptovateľnými, súčasná slovenská úprava v jej stave k dnešnému dňu (31.10.2016), rovnako ako aj pôvodná dôvodová správa k zákonu č. 171/2005 Z. z. o hazardných hrách (z roku 2005), a obdobne aj dôvodová správa k aktuálne prerokúvanej novele

(október 2016) dávajú dôvody pochybovať o súladnosti argumentov, ktoré Slovenská republika používa na obmedzenie poskytovania služieb hazardu zahraničnými poskytovateľmi.

Ak sa totiž zameriame na samotný text zákona č. 171/2005 Z. z. o hazardných hrách, ten dôvody regulácie trhu s hazardnými hrami uvádza len veľmi stručne vo svojom § 1 ods. 2: „*Účelom tohto zákona je vo verejnom záujme vytvoriť podmienky na ochranu verejného poriadku pri prevádzkovaní hazardných hier a zabezpečenie spoločenskej kompenzácie rizík vyplývajúcich z prevádzkovania hazardných hier a účasti na nich*.“ Ako máme možnosť vidieť, spomína sa tu iba veľmi všeobecne verejný poriadok, a pritom žiadne z konkrétnych dôvodov, ktoré by pre obmedzenie voľného trhu hazardných služieb uznával SDEÚ. Ak ďalej nazrieme do pôvodnej dôvodovej správy k zákonu č. 171/2005 Z. z. o hazardných hrách, zistíme, že táto uvádza dôvody úpravy hazardu predsa len podrobnejšie – sledované ciele sú podľa nej nasledujúce: zodpovednosť v hazarde; ochrana spotrebiteľa; predchádzanie trestným činom; prevencia závislosti; ochrana verejného poriadku; využitie príjmov na verejné účely, a ochrana príjmov SR. V tomto výpočte sa teda síce nachádzajú dôvody, ktoré by SDEÚ mohol akceptovať ako relevantné dôvody pre obmedzenie voľného poskytovania služieb hazardu, zároveň však aj dôvody, ktoré by určite SDEÚ neakceptoval – využitie príjmov na verejné účely, či ochrana príjmov SR, čo sú výlučne ekonomické dôvody, ktoré SDEÚ v doterajších rozhodnutiach odmietal. Legitímne otáznym pritom môže byť, ako by asi SDEÚ hodnotil takúto kombináciu argumentov neekonomických a ekonomických – či by nemal za to, že neekonomické argumenty sú príliš všeobecné oproti konkrétnym ekonomickým dôvodom, ktoré by mohli v očiach sudcov SDEÚ znehodnotiť celú právnu úpravu regulácie prístupu na slovenský trh s hazardom. Jednoznačnú odpoveď na túto otázku naporúdzi nemáme.

Takáto je teda situácia vo vzťahu k doterajšiemu zneniu zákona, resp. k terajšej právnej úprave. Možno pritom predpokladať, že zákonodarca, poučený predchádzajúcou judikatúrou SDEÚ zvolí v prípade aktuálne predloženej novely, zavádzajúcej oveľa prísnejšie pravidlá pre zákaz cezhraničného poskytovania služieb hazardu na územie Slovenskej republiky dôkladnú argumentáciu podčiarkujúcu práve význam ochrany občanov Slovenskej republiky a prípadne aj ich zdravia pred nekontrolovanými zahraničnými subjektmi dopúšťajúcimi sa podvodov a inej trestnej činnosti, a to ideálne aj v prepojenosti na novozavádzaný inštitút tzv. registra vylúčených osôb,[20] ktoré budú nespôsobilé využívať služby hazardu vrátane online hazardu,[21] a ktorých ochrana zdravia si vyžaduje prísnu kontrolu poskytovania služieb hazardu na území Slovenska (a následné správne sankcie),[22] čo by bolo pri zahraničných poskytovateľoch niekoľkonásobne komplikovanejšie. Ak však máme takéto očakávanie, budeme novelou a jej dôvodovou správou sklamaní. Už vyššie sme totiž naznačili, že dôvodová správa používa skôr argument znevýhodňovania slovenských poskytovateľov služieb hazardu oproti zahraničným, keďže slovenskí podliehajú licencovaniu a iným druhom dozoru a kontroly, a zahraniční nie.[23] Takéto argumentovanie ekonomickými (konkurenčnými) dôvodmi sa

---

[20] Podľa navrhovaného § 35a ods. 2: „*Fyzické osoby vylúčené z účasti na hazardných hrách sú fyzické osoby,*

a) ktoré sú evidované ako príjemcovia pomoci v hmotnej núdzi,

b) ktoré sami požiadali o vylúčenie,

c) ktorým bola diagnostikovaná choroba patologického hráčstva.“

[21] Za týmto účelom má podľa § 35 ods. 6 štvrtá veta zákona znieť: „*Prevádzkovateľ hazardnej hry prevádzkovanej prostredníctvom telekomunikačných zariadení, prevádzkovateľ hazardnej hry prevádzkovanej prostredníctvom internetu a prevádzkovateľ hazardnej hry, ktorý prenos a zber údajov a informácií súvisiacich s prevádzkovaním hazardnej hry realizuje prostredníctvom internetovej siete, je na tieto účely povinný požadovať údaje z preukazu totožnosti a z ďalšieho dokladu, kópie ktorých mu na tieto účely zasiela fyzická osoba, ktorá má záujem zúčastniť sa na hazardnej hre*.“

[22] V § 35 sa za odsek 6 vkladá nový ods. 7: „*Účasť na hazardných hrách podľa § 3 ods. 2 písm. b) a d) až g) a § 4 ods. 3 písm. d) a na hazardných hrách, pri ktorých je prenos a zber údajov a informácií súvisiacich s prevádzkovaním hazardnej hry realizovaný prostredníctvom internetovej siete, je zakázaná aj fyzickým osobám zaevidovaným v registri fyzických osôb vylúčených z hrania hazardných hier (ďalej len „register vylúčených osôb“). Prevádzkovateľ hazardnej hry uvedenej v prvej vete nesmie týmto fyzickým osobám umožniť účasť na takejto hazardnej hre*.“

[23] „*Tieto subjekty neplnia rovnaké podmienky na prevádzkovanie hazardných hier, čo vedie k ich nerovnakému postaveniu na trhu a predstavuje tak jednoznačnú konkurenčnú výhodu voči*

pritom vyčítalo už predchádzajúcej, neúspešnej novele v roku 2010.[24] Navyše, príklon dôvodovej správy a novely v prospech skôr ekonomických než iných dôvodov na obmedzenie poskytovania zahraničných hazardných služieb možno preukazovať aj tým, že samotný dozor je zverený finančnému orgánu, akým je Finančné riaditeľstvo.

A napokon, už iba stručne možno argumentovať proti navrhovanej novele aj tretím problémom, ktorým je okrem obmedzenia voľného trhu poskytovania služieb aj obmedzenie voľného pohybu kapitálu, keď novela v § 15b ods. 7 predpokladá nasledujúcu reguláciu: „*Právnická osoba alebo fyzická osoba, ktorá poskytuje platobné služby, je povinná na základe príkazu súdu vydaného na základe žiadosti Finančného riaditeľstva Slovenskej republiky zamedziť vykonaniu platobnej operácie alebo inej platobnej služby v prospech účtu, ktorý používa osoba poskytujúca zakázanú ponuku na účely prijímania vkladu pri poskytovaní zakázanej ponuky*.“ Rovnaká výčitka pritom bola adresovaná už aj predchádzajúcemu pokusu o takúto úpravu v roku 2010.

5 ZÁVER – ROZPOR S JUDIKATÚROU EÚ A NEEFEKTÍVNOSŤ?

V príspevku sme venovali pozornosť viacerým výhradám, ktoré možno voči navrhovanej úprave (resp. zákazu) poskytovania zahraničných služieb online hazardu vysloviť. Nebolo pritom naším cieľom zlomyseľne kritizovať. Naopak, účelom príspevku a snahou jeho autora bolo poukázať na limity a slabiny navrhovanej úpravy a jej odôvodnenia, ktoré môžu byť zneužité proti Slovenskej republike v prípade potenciálneho sporu o nesúlad slovenskej úpravy s právom EÚ, resp. s ustálenou judikatúrou SDEÚ vo veci cezhraničného poskytovania služieb (online) hazardu.

Okrem nedostatku v podobe požiadavky sídla poskytovateľa služieb na území Slovenskej republiky sme totiž identifikovali problém tiež v obmedzení voľného trhu v EÚ – pohybu kapitálu a cezhraničného poskytovania služieb, čo by síce samo osebe nebolo úplne vylúčené, na to by však Slovenská republika musela omnoho dôraznejšie argumentovať ochranou zdravia, bezpečnosti a verejného poriadku v Slovenskej republike, a zároveň sa (v duchu rozhodnutia Carmen media) vzdať takých argumentov proti zahraničnému hazardu, ktoré by boli inkonzistentné s vnútroštátnou podporou slovenských poskytovateľov služieb (ako to robí dôvodová správa k novele).

Okrem uvedených právnych problémov však napokon máme pred očami aj iné aspekty celej problematiky obmedzovania poskytovania služieb zahraničného (cezhraničného) online hazardu. Máme totiž pochybnosti o samotnej efektívnosti navrhovanej úpravy – jednak tým, že blokovanie webových sídiel poskytovateľmi služieb elektronickej komunikácie dokáže bežný užívateľ online hazardu pomerne jednoducho obchádzať napríklad s využitím proxy serverov alebo VPN sietí, ale rovnako možno mať pochybnosti aj o efektívnom vyhľadávaní takýchto webových sídiel zamestnancami Finančného riaditeľstva, ako aj o pohotovosti súdneho rozhodovania o blokovaní takýchto sídiel. A napokon, aj samotné blokovanie bankových platieb zrejme nemožno vo svete elektronických platobných služieb ako je PayPal považovať za neprekonateľnú prekážku pre stredne šikovného užívateľa služieb informačnej spoločnosti.

Okrem všetkých doteraz uvedených pripomienok možno napokon našu úvahu zavŕšiť ešte poslednou kritickou otázkou – bolo v súvislosti s navrhovanou úpravou dostatočne zvážené ekonomické hľadisko tejto novely v zmysle zohľadnenia všetkých s ňou spojených nákladov (prenesených na Finančné riaditeľstvo, súd a poskytovateľov služieb elektronickej komunikácie)?

Použitá literatúra:

ANDERSON, P. M. – BLACKSHAW, I. P. – SIEKMANN, R. C. R. – SOEK, J.: Sports Betting : Law and Policy. The Hague: T.M.C. Asser Press, 2012.

---

licencovaným subjektom, ktoré zákonné podmienky súvisiace napr. s ochranou verejného poriadku, spotrebiteľa, či prevenciou kriminality plnia. Tieto spoločnosti tým, že nerešpektujú platnú slovenskú právnu úpravu pre oblasť podnikania vo sfére hazardných hier, je ich ponuka pre hráčov častokrát výhodnejšia, ako ponuka licencovaných subjektov. V snahe obmedziť prienik ponuky nelicencovaných operátorov a jeho dostupnosť na území Slovenskej republiky sa navrhuje zadefinovať takúto ponuku ako zakázanú a zároveň zaviesť opatrenia znemožňujúce prístup k poskytovaniu takejto ponuky.“

[24] Pozri http://www.eisionline.org/index.php/sk/10-projekty/novinky-z-aktivit/5-hazardny-navrh-zakona (navštívené dňa 27.10.2016).

European Commission Communication Towards a comprehensive European framework on online gambling.
European Parliament resolution on the integrity of online gambling.
http://ec.europa.eu/growth/sectors/gambling_sk (navštívené dňa 27.10.2016).
http://ec.europa.eu/internal_market/services/docs/gambling/study2_en.pdf (navštívené dňa 27.10.2016).
http://www.eisionline.org/index.php/sk/10-projekty/novinky-z-aktivit/5-hazardny-navrh-zakona (navštívené dňa 27.10.2016).
ROMPUY, B. van: The French "betting right": a legislative Dr. Jekyll and Mr. Hyde. Dostupné na internete: http://www.asser.nl/SportsLaw/Blog/post/the-french-betting-right-a-legislative-dr-jekyll-and-mr-hyde-by-prof-dr-ben-van-rompuy (navštívené dňa 27.10.2016).
Správy predsedníctva o súčasnom stave.
Study Of Gambling Services In The Internal Market Of The European Union : Final Report (2006). Dostupné na internete: http://ec.europa.eu/internal_market/services/docs/gambling/study1_en.pdf (navštívené dňa 27.10.2016).
Zelená kniha o online hazardných hrách na vnútornom trhu. Dostupné na internete: http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_sk.pdf (navštívené dňa 27.10.2016).

Kontaktné údaje:
doc. JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA
tomas.gabris@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. 6, P.O.Box 313
810 00 Bratislava 1
Slovenská republika

PRÁVNE ASPEKTY SPAMU A MOŽNOSTI OCHRANY PROTI NEMU

Marek Ivančo

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The author of the paper analyzes seemingly already common, but in many cases dangerous, phenomenon of the 21st century called "spam" in the context of the legislation of the Slovak Republic. The author brings into focus the description of legal means of protection against spam in general terms with relevant emphasis on selected atypical private law practices including damages and unfair competition proceedings as the consequences of a spam use. Such a method also implies the need of hypotheses reasoning the application of the abovementioned means. In this respect, the aim of this paper is to point out theoretical and practical framework of this issue and to identify problematic aspects of protection against spam along with its potential solutions.

Abstrakt: Autor v príspevku analyzuje zdanlivo už prirodzený, avšak v mnohých prípadoch nebezpečný fenomén 21. storočia nazývaný „spam", a to v kontexte právnej úpravy Slovenskej republiky. Zameriava sa pritom na právne prostriedky ochrany proti spamu vo všeobecnosti s náležitým akcentom na vybrané atypické súkromnoprávne postupy vrátane možnosti náhrady škody a nekalosúťažného postihu ako dôsledku využívania spamu. Uvedený postup zároveň predpokladá uvedenie hypotéz dôvodiacich potrebu aplikácie týchto prostriedkov. S ohľadom na to je cieľom príspevku poukázať na nielen teoretický, ale aj praktický rámec tejto tematiky spolu s uvedením problematických aspektov ochrany proti spamu a ich prípadných riešení.

Key words: spam, legal means of protection against spam, damages, unfair competition sanction

Kľúčové slová: spam, právne prostriedky ochrany proti spamu, náhrada škody, nekalosúťažný postih

1 ÚVOD

S rozvojom internetu dochádza dennodenne k sprostredkovaniu množstva informácií ako aj s nimi spätého širokého spektra možností pre milióny ľudí. Rastúcim vplyvom tejto komplexnej globálnej siete nastáva o. i. vzrast potenciálnych neduhov, ktoré so sebou táto sieť obnáša. V tomto smere možno na túto skutočnosť nahliadať ako na dvojsečnú zbraň, prostredníctvom ktorej je možné rýchlejšie a efektívnejšie než kedykoľvek predtým postihnúť mnohonásobne väčšie kvantum osôb. Jedným z týchto neduhov asociovaných s použitím moderných komunikačných prostriedkov je fenomén zvaný „spam" javiaci sa ako bežná súčasť našich životov. Napriek zdanlivej neškodnosti možno spamom spôsobiť značné problémy, ktorých riešenie však ponúka aj právna úprava *de lege lata.* Uvedené možno ilustrovať na situácii, keď skrz spam dôjde k preťaženiu telekomunikačných kanálov určitej obchodnej spoločnosti a následne k prípadným prestojom spôsobujúcim ušlý zisk.

S ohľadom na túto naznačenú relevanciu danej problematiky sa autor zameriava práve na predostretie právnych prostriedkov ochrany proti spamu v slovenskej právnej úprave s akcentom na atypické súkromnoprávne postupy spolu s objasnením základného právneho rámca tejto tematiky. Črtajúca sa aktuálnosť takéhoto postupu je, podľa názoru autora, podčiarknutá absenciou akéhokoľvek súdneho výkladu či minimom doktrinálneho výkladu. Účelom tohto príspevku pritom nie je hĺbková analýza každého do úvahy spadajúceho právneho prostriedku ochrany voči spamu ako ani vyčerpanie všetkých so spamom súvisiacich aspektov vrátane technickej stránky veci. Autor, naopak, sústreďuje svoju pozornosť na tie vybrané právne inštitúty, ktoré sa podľa jeho názoru v boji proti spamu javia byť kľúčové, pričom vyústením tejto snahy má byť predostretie určitých aplikačných problémov týkajúcich sa právnej úpravy spamu ako takej.

2 NIEKOĽKO POZNÁMOK KU KONCEPTU SPAMU A K JEHO PRÁVNYM ASPEKTOM

2.1 Pojem spam, jeho dôvody šírenia a ciele za ním

Predtým, než uvedieme právnu úpravu, ktorá sa vzťahuje na spam a reguluje ho, je úvodom potrebné vymedziť tento samotný pojem ako predmet uvádzanej regulácie. Pojem spam ako taký

však v právnej úprave Slovenskej republiky (ďalej aj ako „SR“) nie je priamo vymedzený v žiadnej zákonnej norme, a to aj napriek tomu, že určitá právna regulácia, ako naznačuje zameranie tohto príspevku, existuje. Priama definícia spamu je totiž obsiahnutá iba na úrovni interného normatívneho aktu v metodickom pokyne Ministerstva financií SR, v zmysle ktorého je spamom „*nevyžiadaná elektronická správa (najmä email) obťažujúca príjemcu, ktorý nemá s odosielateľom nijaký konsenzuálny vzťah, obvykle ako reklama nejakého výrobku alebo služby, rozosielaná zvyčajne naraz na väčší počet adries s vyššou frekvenciou výskytu*.“[1] Takáto definícia však z povahy interného normatívneho aktu, prirodzenie, nie je všeobecne záväzná, určitú právnu relevanciu jej však nemožno uprieť. Výklad plynúci z tejto definície sa totiž prelína s doktrinálnym výkladom, podľa ktorého je spam, ako široký pojem s nejasnými hranicami, možné vymedziť jednak prostredníctvom kvalitatívneho a jednak prostredníctvom kvantitatívneho kritéria. V zmysle tejto dichotómie napĺňa znaky spamu konanie spočívajúce v rozosielaní správ so zanedbateľnou informačnou hodnotou alebo ich zjavnou neúčelnosťou, resp. bez súhlasu recipienta spamu (*kvalitatívne kritérium*), alebo konanie tkvejúce v hromadnom šírení správ negatívne ovplyvňujúcich infraštruktúru siete (*kvantitatívne kritérium*).[2]

Nahliadajúc na spam ako na vyššie vymedzený komunikačný prostriedok, resp. formu šírenú obvykle prostredníctvom elektronickej pošty, medzi hlavné dôvody jeho šírenia možno zaradiť nízke náklady na jednu odoslanú správu pri relatívne vysokej úspešnosti doručenia tejto správy.[3] V pozadí nezaostáva ani možnosť postihu obrovskej množiny osôb, ktorým je prostredníctvom spamu možné tieto správy doručiť, a to z pohodlia domova.

V nadväznosti na tieto dôvody šírenia, cieľom a snahou odosielateľov spamu je obvykle navýšenie objednávok pri predaji tovarov a služieb prostredníctvom hromadne šírenej nevyžiadanej reklamy, a teda získanie vyššieho obnosu finančných prostriedkov, získanie finančných prostriedkov od príjemcu vplyvom podvodného konania (tzv. *scam*), získanie osobných údajov ako aj prístupových údajov k rôznym službám, získanie údajov z kreditných či debetných kariet (tzv. *phishing*) či šírenie nepravdivých a často poplašných správ (tzv. *hoax*).[4]

Dôsledkami týchto dôvodov sú zvýšené náklady adresátov spamu na zavedenie protispamových opatrení, prípadne časová záťaž adresátov spamu spôsobená mazaním veľkého množstva nevyžiadaných správ a iné. V porovnaní s bežnou listinnou poštou teda spam ako forma elektronickej pošty nezaťažuje iba šíriteľa správ, ale aj recipienta týchto správ. Vzhľadom na tieto naznačené riziká spamu je žiaduce, aby bol spam legislatívne upravený, pričom aspektom právnej úpravy sa venujeme v nasledujúcej podkapitole.

2.2 Východiská a požiadavky regulácie spamu v právnej úprave SR

Úvodom tohto príspevku sme konštatovali, že priama, resp. všeobecná definícia spamu v právnej úprave SR absentuje, dôsledkom čoho sme pre účely tohto príspevku pristúpili k určitému doktrinálnemu vymedzeniu tohto pojmu. Na druhej strane, absencia akejkoľvek úpravy či definície (nepriamej) tohto fenoménu súčasnosti by však reálne predstavovala nemožnosť legislatívno-právneho postihu pomerne závažných, vyššie uvedených dôsledkov jeho nekalého využívania, čo by v konečnom dôsledku znamenalo o. i. aj bezúčelnosť akejkoľvek už existujúcej, avšak iba čiastkovo uplatniteľnej, právnej úpravy.[5]

Aj to opodstatňuje prijatie Smernice o súkromí a elektronických komunikáciách, ktorá najprv v článku 2 písm. h) vymedzuje pojem elektronickej pošty a následne upravuje podmienky jej

---

1 Metodický pokyn Ministerstva financií SR č. 42/2008 na použitie odborných výrazov pre oblasť informatizácie spoločnosti.

2 Korene samotného pojmu spam možno nachádzať v šunkovej konzerve (obdoba tzv. *lunchmeatu*) s názvom Hormel Spiced Ham (neskôr už iba „SPAM“), ktorá bola počas obdobia druhej svetovej vojny často jediným dostupným zdrojom potravy. Bližšie pozri POLČÁK, R. Právo na internetu: spam a odpovědnost ISP, s. 106 – 108.

3 RAMBOUSEK, K., MIČUDOVÁ, T. Za spam hrozí pokuta až do 66 tisíc eur. In: Finančný manažment, 2012, č. 5, s. 52.

4 Tamtiež, s. 52.

5 Bližšie pozri HANUŠ, L. Argumentace nebo svévole. Úvahy o právu, spravedlnosti a etice, s. 90 – 91.

používania v článku 13 pojednávajúcom o nevyžiadaných správach.[6] Uvedená smernica je pritom odrazovým mostíkom pre slovenskú právnu úpravu. Predmetné vyššie spomenuté články tejto smernice totiž boli transponované do ust. § 62 zákona č. 351/2011 Z. z. o elektronických komunikáciách (ďalej aj ako „ZEK").[7]

V zmysle ust. § 62 ods. 1 ZEK je elektronickou poštou akákoľvek „*textová, hlasová, zvuková alebo obrazová správa zaslaná prostredníctvom verejnej siete, ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu, kým ju príjemca nevyzdvihne*." Ak teda doposiaľ okrem emailu neboli konkretizované iné formy spamu, predmetné ustanovenie rozširuje efektívne využitie problematiky spamu aj na radu ďalších foriem, ako napríklad blogy, diskusné príspevky, komentáre, príspevky na sociálnych sieťach či krátke textové správy (tzv. *SMS*).

Následne ust. § 62 ods. 2 a ods. 3 ZEK ďalej vymedzujú podmienky šírenia elektronickej pošty. V zmysle týchto ustanovení (na ktoré sa z dôvodu ich komplexnosti a za účelom prehľadnosti ďalej bližšie pozrieme v osobitných bodoch) právna regulácia spamu vyžaduje, aby predmetná elektronická pošta:

a) nebola nevyžiadaná (ust. § 62 ods. 2 prvá veta ZEK a ust. § 62 ods. 3 prvá veta ZEK);
b) spĺňala rámec priamej marketingovej povahy (ust. § 62 ods. 2 prvá veta ZEK a ust. § 62 ods. 3 prvá a tretia veta ZEK);
c) umožňovala kedykoľvek ukončiť zasielanie týchto správ (ust. § 62 ods. 3 druhá veta ZEK);
d) obsahovala totožnosť a adresu jej odosielateľa (ust. § 62 ods. 2 tretia veta ZEK);
e) nenabádala k návšteve webového sídla v rozpore s osobitným predpisom (ust. § 62 ods. 2 tretia veta ZEK).

Z uvedeného výpočtu kumulatívnych požiadaviek na používanie elektronickej pošty vyplýva, že už introdukované kvantitatívne kritérium nehrá pri regulácii spamu žiadnu rolu.[8] Naopak, prednosť tu dostalo kritérium kvalitatívne, nelimitujúce spam iba na hromadne zasielanú elektronickú poštu. To znamená, že právny rámec spamu bude za predpokladu nesplnenia niektorej z vyššie uvedených podmienok naplnený aj v prípade, ak pôjde o nedovolené použitie, resp. zaslanie singulárnej elektronickej pošty podľa definície obsiahnutej v ust. § 62 ods. 1 ZEK. Žiada sa však spomenúť, že púha protiprávnosť konania opretá o vyššie spomenuté kvalitatívne požiadavky, je do istej miery korigovaná ust. § 73 ods. 6 ZEK, podľa ktorého Úrad pre reguláciu elektronických komunikácii a poštových služieb (ďalej aj ako „Úrad") prihliada aj na „*závažnosť, spôsob, trvanie a dôsledky porušenia povinnosti*".

Vracajúc sa k objasneniu vyššie zmienených požiadaviek, podľa prvej z nich (písm. a) by elektronická pošta nemala byť nevyžiadanou. Právna úprava ZEK na tomto mieste umožňuje používanie elektronickej pošty buď len s preukázateľným predchádzajúcim súhlasom príjemcu tejto pošty (ust. § 62 ods. 2 prvá veta ZEK), alebo bez tohto predchádzajúceho súhlasu, ak ide o kontakt elektronickej pošty získaný od zákazníka v súvislosti s predajom výrobku alebo služby (ust. § 62 ods. 3 prvá veta ZEK).

V prípade podmienky preukázateľného predchádzajúceho súhlasu ide o situáciu postavenú na tzv. *princípe opt-in,* v zmysle ktorého je potrebné aktívne konanie (potenciálneho) príjemcu elektronickej pošty, ktorým okrem potrebného súhlasu pred samotným zaslaním elektronickej pošty, udelí aj ľubovoľný elektronický kontaktný údaj.[9] V kontexte ust. § 62 ods. 1 ZEK možno argumentom *a similio* vyabstrahovať, že takýmto elektronickým kontaktným údajom bude email, telefónne číslo či užívateľský profil na sociálnej sieti. Zároveň má takýto súhlas spĺňať podstatné náležitosti vyplývajúce

---

6 Smernica Európskeho parlamentu a Rady 2002/58/ES zo dňa 12.07.2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách).

7 Bližšie pozri Tabuľka zhody smernice o súkromí a elektronických komunikáciách s právnymi predpismi SR. Dostupné na: <https://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=356724>.

8 Inak je tomu v podmienkach právnej úpravy Českej republiky, ktorá v ust. § 10a v spojitosti s ust. § 11 zákona č. 480/2004 Sb. o některých službách informační společnosti, vyžaduje pre sankcionovanie spamu hromadné alebo opakované šírenie týchto správ.

9 JANSA, L., OTEVŘEL, P., MATĚJKA, M., ČERMÁK, J., MALIŠ, P., HOSTAŠ, P., MATEJKA, J. Internetové právo : Praktický průvodce, s. 267.

z ust. § 37 ods. 1 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej aj ako „OZ") ako aj z ust. § 62 ods. 2 ZEK, a teda musí ísť o preukázateľný súhlas daný slobodne, vážne, určito a zrozumiteľne.[10] V rámci týchto podmienok na margo uvádzame, že s ohľadom na podmienku preukázateľnosti tohto súhlasu sa javí vhodné, aby odosielateľ elektronickej pošty disponoval či už presným časom, kedy bol súhlas udelený, alebo IP adresou, z ktorej bol súhlas udelený, prípadne potvrdzujúcou informačnou správou zaslanou príjemcovii elektronickej pošty o tom, že jej odosielateľ obdržal súhlas na použitie elektronickej pošty.[11] Rovnako dodávame, že o tento súhlas je možné potenciálneho príjemcu elektronickej pošty požiadať emailom, ktorý nebude koncipovaný za účelom priameho marketingu, ba naopak, bude mať iba informatívny charakter bez uvedenia akéhokoľvek konkrétneho produktu. V takom prípade nepôjde o nevyžiadanú elektronickú poštu obchodnej povahy.

V prípade zákonne súladného použitia elektronickej pošty bez predchádzajúceho súhlasu ide o situáciu založenú na tzv. *princípe opt-out*. Podľa tohto princípu postačuje pre splnenie zákonných medzí použitia elektronickej pošty kvázi pasívne konanie, v zmysle ktorého odosielateľ elektronickej pošty získal elektronický kontakt na potenciálneho príjemcu elektronickej pošty v súvislosti s realizáciou nejakého predošlého obchodu, pri ktorom tento potenciálny príjemca vyslovil súhlas s obchodnými podmienkami odosielateľa obsahujúcimi súhlas so zasielaním marketingovej elektronickej pošty. V tomto prípade sa teda súhlas príjemcu potenciálnej elektronickej pošty prezumuje, a to s ohľadom na neúčelnosť požadovania osobitného súhlasu pre zaslanie elektronickej pošty od štandardných zákazníkov odosielateľa elektronickej pošty.[12] Je však potrebné, aby išlo o nadobudnutie elektronického kontaktu odosielateľom od svojho zákazníka ako subjektu, s ktorým už tento odosielateľ v minulosti bol zaangažovaný do obchodu týkajúceho sa vlastného obdobného tovaru či služby. Z tohto dôvodu nejde odosielať marketingové ponuky v prospech tretích strán. Zároveň však právna úprava ZEK vyžaduje, aby mal príjemca tejto elektronickej pošty možnosť pri každej ním obdržanej správe, ako aj pred obdržaním vôbec prvej správy, jednoducho a bezplatne ďalšie zasielanie správ odmietnuť.

Podľa druhej z vyššie uvedených podmienok (písm. b) sa právna úprava ZEK dotýka elektronickej pošty, a to zasielanej na účely priameho marketingu. Z uvedeného dôvodu zákonná úprava ZEK (ani iná zákonná úprava v tomto príspevku ďalej uvádzaných správnoprávnych predpisov, ktoré sa dotýkajú problematiky spamu) nepostihuje politický, náboženský či iný spam, keďže nie sú odosielané za účelom priameho marketingu.[13]

Pre plný zákonný súlad odosielania elektronickej pošty za účelom priameho marketingu je v zmysle tretej vyššie zmienenej podmienky (písm. c) potrebné, aby predmetná odoslaná správa umožňovala príjemcovi elektronickej pošty kedykoľvek ukončiť zasielanie týchto správ ich odosielateľom. Uvedené v praktickej rovine znamená, že príjemcovi elektronickej pošty by malo byť umožnené ďalšie zaslanie elektronickej pošty jednoducho odmietnuť, a to napríklad kliknutím na hypertextový link v dolnej časti emailu či odoslaním bezodplatnej SMS správy na určené číslo. Dôležité pritom v zmysle zákonnej dikcie je, aby takéto odmietnutie ďalšieho príjmu elektronickej pošty nebolo spoplatnené.

Štvrtá spomínaná podmienka vyžadujúca obsiahnutie totožnosti a adresy jej odosielateľa (písm. d) v zasielanej elektronickej pošte znamená, že príjemcovi elektronickej pošty musí byť vždy zrejmé, kto mu ju zaslal a na akú adresu môže tento príjemca zaslať svoj nesúhlas s ďalším zasielaním elektronickej pošty jej odosielateľom. Požiadavka uvedenia adresy odosielateľa

---

[10] Na tomto mieste si dovolíme poznamenať, že spracúvaním súhlasu s najvyššou pravdepodobnosťou dôjde k spracúvaniu osobných údajov a okrem podmienok podľa ust. § 37 ods. 1 OZ bude potrebné ďalej naplniť ostatné požiadavky podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Vzhľadom na zameranie tohto príspevku sa tým však bližšie nezaoberáme.

[11] JANSA, L., OTEVŘEL, P., MATĚJKA, M., ČERMÁK, J., MALIŠ, P., HOSTAŠ, P., MATEJKA, J. Internetové právo : Praktický průvodce, s. 268 - 269.

[12] Tamtiež, s. 269.

[13] V tejto súvislosti porovnaj ust. § 2 ods. 1 písm. a) zákona č. 147/2001 Z. z. o reklame v znení neskorších predpisov (ďalej aj ako „ZR"), podľa ktorého je reklamou „*predvedenie, prezentácia alebo iné oznámenie v každej podobe súvisiace s obchodnou, podnikateľskou alebo inou zárobkovou činnosťou s cieľom uplatniť produkty na trhu*".

elektronickej pošty sa pochopiteľne vzťahuje na platnú adresu, na ktorej je možné zo strany príjemcu účinne vyjadriť spomínaný nesúhlas. Môže pritom ísť či už o emailovú adresu, na ktorú môže príjemca elektronickej pošty zaslať svoj nesúhlas s jej ďalším zasielaním, ako aj adresu webovej stránky, ktorej načítaním dôjde k automatickému odhláseniu zo zoznamu recipientov elektronickej pošty.[14]

Piatou uvádzanou podmienkou zákonnej súladnosti elektronickej pošty je podmienka, aby elektronická pošta nenabádala k návšteve webového sídla v rozpore s osobitným predpisom, ktorým sa rozumie zákon č. 22/2004 Z. z. o elektronickom obchode v znení neskorších predpisov (ďalej aj ako „ZEO"). Spresnenie tejto podmienky ponúka ust. § 4 ods. 6 ZEO, z ktorého vyplýva, že odosielateľ elektronickej pošty nesmie nabádať k návšteve webového sídla práve v prípade, ak si to príjemca elektronickej pošty priamo vopred nevyžiadal.

2.3 Ďalšie právne predpisy regulujúce spam a kategorizácia právnych prostriedkov ochrany proti spamu

Navzdory vyššie analyzovanej relatívne samostatnej právnej úprave týkajúcej sa spamu obsiahnutej v ZEK je problematika spamu pomerne roztrieštená.

Okrem kľúčového ZEK je potrebné zmieniť aj zákon č. 147/2001 Z. z. o reklame v znení neskorších predpisov, v zmysle ktorého ust. § 3 ods. 3 ZR sa reklama „*nesmie šíriť automatickým telefonickým volacím systémom, telefaxom a elektronickou poštou bez predchádzajúceho súhlasu ich užívateľa, ktorý je príjemcom reklamy."* Predmetný zákon sa teda rovnako týka problematiky spamu. Na rozdiel od ZEK však tento predpis pokrýva aj situácie, kedy dochádza k rozosielaniu správ inými ako elektronickými prostriedkami.[15] V praxi pôjde o nevyžiadanú reklamu v podobe letákov či inej formy poštovej kampane. Zároveň v prípade aplikácie ZR je orgánom kompetentným na vykonávanie dozoru a uloženie sankcií Slovenská obchodná inšpekcia, ak vo veci nie je kompetentný iný orgán podľa ust. § 10 ZR.[16] V nadväznosti na takúto roztrieštenosť kompetencie prešetriť prípadný spam vo všeobecnosti, rozdiel v porovnaní s právnou úpravou ZEK možno bádať aj vo výške zákonných sankcií a v kategórií osôb, ktorým je možné udeliť sankciu. Podľa ust. § 73 ods. 3 písm. a) ZEK totiž možno za porušenie ustanovení regulujúcich spam uložiť pokutu od 200 eur do 5 % z obratu podniku, a to právnickej osobe, prípadne fyzickej osobe – podnikateľovi. Naopak, podľa ust. § 11 ods. 3 písm. c) ZR možno udeliť sankciu do 66 400 eur, a to šíriteľovi reklamy, ktorým sa v zmysle ust. § 2 ods. 1 písm. c) ZR rozumie akákoľvek fyzická či právnická osoba šíriaca reklamu.

Doplnkom tejto správnoprávnej úpravy spamu je zákon č. 22/2004 Z. z. o elektronickom obchode v znení neskorších predpisov, na ktorý odkazuje aj východisková právna úprava ZEK. Podľa ust. § 4 ods. 6 ZEO „*poskytovateľ služieb nesmie doručovať informácie komerčnej komunikácie elektronickou poštou, ak si ich príjemca služby vopred nevyžiadal*." Dohľad nad dodržiavaním tohto ustanovenia však vykonáva opätovne Slovenská obchodná inšpekcia alebo Národná banka Slovenska, a to navyše podľa osobitných predpisov. Sankcionovateľným subjektom je v tomto prípade, obdobne ako pri právnej úprave ZEK, iba právnická osoba alebo fyzická osoba – podnikateľ, teda poskytovatelia služieb definovaný v ust. § 2 písm. b) ZEK. Ani tento právny predpis teda nenapomáha jednotnosti sankčného postupu voči prípadným odosielateľom spamu.

Mimo rámec správnoprávnych predpisov si dovolíme zaradiť zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov upravujúci situáciu, kedy je prostredníctvom spamu spôsobená škoda, ktorú si možno žiadať titulom náhrady škody spôsobenej prevádzkovou činnosťou či titulom náhrady škody spôsobenej úmyselným konaním proti dobrým mravom. V určitých prípadoch možno spamom dokonca zasiahnuť do ochrany osobnosti (napríklad v prípade vyššie spomínaného tzv. hoaxu).

Táto súkromnoprávna úprava je doplnená zákonom č. 513/1991 Zb. Obchodný zákonník v znení neskorších právnych predpisov (ďalej aj ako „OBZ"), upravujúci možnosť nekalosúťažného postihu voči spamu.

---

[14] MATEJKA, J. Anti-Spam Legislation in Consideration of Personal Data Protection and Other Legal Instruments. In: The Lawyer Quarterly, 2016, č. 2, s. 100.

[15] Uvedené vyplýva z definície reklamy v ust. § 2 ods. 1 písm. a) ZR ako aj z vymedzenia všeobecných požiadaviek na reklamu v ust. § 3 ZR.

[16] Ide napríklad o Štátny ústav na kontrolu liečiv nad reklamou liekov, Úrad verejného zdravotníctva SR či Národnú banku Slovenska, a to v závislosti od druhu regulovanej reklamy.

Posledným dôležitým právnym predpisom uzatvárajúcim triádu kategórií právnych prostriedkov ochrany proti spamu je zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej aj ako „TZ“) upravujúcim situáciu, kedy vplyvom spamu dôjde k naplneniu skutkovej podstaty trestného činu ohováraniu, šírenia pornografie, šírenia toxikománie, prípadne trestného činu neoprávneného nakladania s osobnými údajmi či iného trestného činu. Vzhľadom na zásadu subsidiarity a pomerne komplexnú úpravu spamu v správnoprávnej rovine sa možno domnievať, že aplikácia TZ bude skôr výnimočná.

Vzhľadom na vyššie zmienené predpisy je možné vyčleniť nasledovné kategórie právnych prostriedkov ochrany proti spamu:

a) správnoprávne prostriedky ochrany vychádzajúce predovšetkým z právnej úpravy obsiahnutej v ZEK či ZR;
b) súkromnoprávne prostriedky ochrany vychádzajúce z OZ a OBZ;
c) trestnoprávne prostriedky ochrany vychádzajúce z TZ.

3 SÚKROMNOPRÁVNE PROSTRIEDKY OCHRANY PROTI SPAMU

Nadväzujúc na vyššie zmienenú triádu právnych prostriedkov ochrany proti spamu, dovolíme si opätovne podotknúť, že právna úprava spamu je relatívne samostatne upravená práve vo vyššie analyzovanom ZEK ako aj v ZR. Tieto právne predpisy tak podľa nášho názoru predstavujú prvotné piliere pre úvod do nami skúmanej problematiky, ktoré sme zároveň s prihliadnutím na väčšiu efektívnosť z nich plynúcich správnoprávnych postupov (v komparácii s tými súkromnoprávnymi či trestnoprávnymi) nepovažovali za vhodné opomenúť. Naopak, žiadalo sa na ne v uvedenom kontexte upriamiť náležitú pozornosť.

Napriek tomu, ako poukazujeme v tejto kapitole, svoje zastúpenie v boji proti spamu patrí aj atypickým súkromnoprávnym prostriedkom ochrany. Nevýhodu týchto prostriedkov však možno bádať práve v ich súkromnoprávnej povahe a v priemete *zásady vigilantibus iura scripta sunt*, ktorá vyžaduje väčšiu aktivitu jednotlivých subjektov zrkadliacu v nesení dôkazného bremena ako aj všetkých nákladov konania. Možno aj z tohto dôvodu nie je táto forma obrany proti spamu v našom právnom systéme vôbec bežná a teda absentuje aj úvodom spomínaný súdny výklad. Iný dôvod atypickosti týchto právnych prostriedkov v našom právnom systéme možno vidieť v nemožnosti preukázania škody, či nehmotnej ujmy, prípadne nemožnosti odhalenia totožnosti odosielateľa spamu, ako aj v demotivácii oprávneného subjektu domáhať sa náhrady minimálnej škody z titulu spamu.[17]

Z týchto dôvodov sa preto na tomto mieste ďalej pokúsime opísať prípadný právny postup ochrany voči spamu spočívajúci v uplatnení nároku na náhradu škody spôsobenej prevádzkovou činnosťou či škody spôsobenej úmyselným konaním proti dobrým mravom. Okrem týchto prostriedkov ochrany podľa OZ, spomenieme aj nekalosúťažný postih podľa OBZ.

3.1 Náhrada škody za spam z titulu zodpovednosti za škodu spôsobenú prevádzkovou činnosťou podľa ust. § 420a OZ

V zmysle uvedeného ustanovenia OZ „*každý zodpovedá za škodu, ktorú spôsobí inému prevádzkovou činnosťou*.“ Uplatnenie tohto nároku pri škode spôsobenej spamom právna doktrína prirovnáva k situácii, keď niekto porušením dopravných predpisov spôsobí inému škodu na majetku.[18] Nehodu vyšetrí a o pokute rozhodne policajt, škodu však musí na delikventovi vymáhať samotný poškodený. Obdobne aj v prípade škody spôsobenej spamom totiž dôjde k porušeniu právnej povinnosti podľa ZEK či podľa ZR a odosielateľ spamu bude okrem správnej sankcie zodpovedať aj za akúkoľvek ďalšiu škodu, ktorú svojím konaním spôsobí. Uvedené zároveň nachádza svoj podklad v definovaní prevádzkovej činnosti, ktorou sa v zmysle judikatúry rozumie „*akákoľvek činnosť súvisiaca s predmetom činnosti danej osoby, ktorá však nemusí byť vždy vymedzená v predmete činnosti tejto osoby; znamená to, že prevádzkovou činnosťou je preto akákoľvek činnosť súvisiaca s činnosťou danej osoby*“, teda aj činnosť, ktorá nie je vymedzená v predmete činnosti tejto osoby.[19]

---

17 MATEJKA, J. Anti-Spam Legislation in Consideration of Personal Data Protection and Other Legal Instruments. In: The Lawyer Quarterly, 2016, č. 2, s. 105.
18 POLČÁK, R. Právo na internetu: spam a odpovědnost ISP, s. 132.
19 Rozhodnutie Najvyššieho súdu SR, sp. zn. 3 M Cdo 7/2005.

Podstatná bude teda tá okolnosť, či vplyvom spamu došlo ku škodnej udalosti. Akékoľvek bližšie judikatórne či doktrinálne závery však k tomuto nároku absentujú.

Okruh pasívne legitimovaných subjektov je v tomto prípade identický so subjektmi podľa ZEK, a to vzhľadom na to, že subjektom zodpovednosti podľa ust. § 420a OZ môže byť len podnikateľ.[20]

3.2 Náhrada škody za spam z titulu zodpovednosti za škodu spôsobenú porušením dobrých mravov podľa ust. § 424 OZ

Keďže podľa predmetného ustanovenia zodpovedá za škodu „*aj ten, kto ju spôsobil úmyselným konaním proti dobrým mravom*“, je potrebné, obdobne ako v prvom prípade, preukázať existenciu a výšku škody. Tá je pri jednotlivcovi mnohokrát iba zanedbateľná. Pokiaľ ide o väčšie korporácie, môže však ísť o značnú čiastku.

Na rozdiel od predošlej situácie podotýkame, že v tomto prípade je možné si uplatniť náhradu škody aj v situácii, keď nejde o spam, resp. nedôjde k porušeniu právnej úpravy ZEK či ZR. Bude však potrebné preukázať neetický aspekt materiálneho spamu (spam, ktorý nemusí byť v rozpore so ZEK či ZR).[21] Výhodou tohto postupu je teda možnosť uplatnenia si nároku voči odosielateľovi spamu aj v prípade nemožnosti aplikácie správnoprávnych prostriedkov. Okrem preukázania rozporu s dobrými mravmi spočívajúcom v preukázaní neetického aspektu spamu bude potrebné preukázať aj úmysel.

3.3 Nekalosúťažný postih spamu

Ak chceme uplatniť voči odosielateľovi spamu určitý nekalosúťažný postih, je potrebné, aby posudzované konanie napĺňalo znaky tzv. generálnej klauzuly obsiahnutej v ust. § 44 ods. 1 OBZ, podľa ktorého je nekalou súťažou „*konanie v hospodárskej súťaži, ktoré je v rozpore s dobrými mravmi súťaže a je spôsobilé privodiť ujmu iným súťažiteľom alebo spotrebiteľom.“*

V zmysle tejto definície je teda možné tento nekalosúťažný postih uplatniť aj voči akejkoľvek fyzickej osobe, pokiaľ táto osoba bude svojím konaním vytvárať určitý efekt na hospodárske súťažné prostredie, a teda spadať pod definičný rozsah konania v hospodárskej súťaži.

Rozpor s dobrými mravmi, ako druhý definičný znak nekalej súťaže, bude možné preukázať odkazom na už spomínaný tzv. *netiquette* ako v prípade preukazovania rozporu s dobrými mravmi podľa ust. § 424 OZ.[22] V prípade nekalosúťažného postihu však nebude potrebné preukazovať zavinenie.

Tretí definičný znak plynúci z generálnej klauzuly spočíva v spôsobilosti privodiť ujmu. Nekalosúťažný postih teda nie je limitovaný iba na náhradu škody, ktorej vznik a výšku je potrebné podľa ust. § 420a OZ a ust. § 424 OZ preukázať. Naopak, nekalosúťažným postihom je možné si uplatniť okrem nároku na náhradu škody aj nárok na primerané zadosťučinenie, ktorého posúdenie závisí od úvahy súdu.

4 ZÁVER

Záverom by sme si dovolili s pokorou konštatovať, že právna úprava týkajúca sa spamu podľa nášho názoru nie je úplne bezproblémová a ponúka širší priestor na zlepšenie. Už úvodom sme načrtli, že neexistuje priama definícia spamu. Práve existujúca priama definícia tohto pojmu môže byť tým faktorom, ktorý môže prispieť k uplatňovaniu nárokov plynúcich zo spamu.

Okrem toho je pozoruhodné, že vykonávať dozor a sankcionovať na úseku problematiky spamu môže hneď niekoľko subjektov verejnej správy. Roztrieštenosť kompetencií podľa nášho názoru prípadnému uplatneniu si nároku zo spamu rovnako neprospieva.

Na druhej strane by mohlo zo strany zákonodarcu dôjsť k zavedeniu kvantitatívneho hľadiska, ktorým by sa znížil nápad bagatelizovaných vecí. Rovnako konštatujeme, že prípadnému širšiemu

---

[20] ŠTEVČEK, M., DULAK, A., BAJÁNKOVÁ, J., FEČÍK, M., SEDLAČKO, F., TOMAŠOVIČ, M. a kol. Občiansky zákonník I. Komentár, s. 1360.

[21] Pôjde o skutkovo náročnejšie dokazovanie, pričom je možné vychádzať aj tzv. *netiquette* – pravidiel slušného správania na internete, ktoré boli súdom bližšie rozobraté napríklad v rozhodnutí Ontario Superior Court of Justice vo veci Ontario Inc. v. Nexx Online Inc., Ref. No. C20546/99. Bližšie pozri POLČÁK, R. Právo na internetu: spam a odpovědnost ISP, s. 133.

[22] POLČÁK, R. Právo na internetu: spam a odpovědnost ISP, s. 134.

uplatňovaniu nárokov plynúcich z titulu spamu by určite prospela aj osveta zo strany kompetentných orgánov. Ako bolo totiž konštatované, jedným z hlavných dôvodov neuplatňovania si prostriedkov ochrany voči spamu je práve nevedomosť oprávnených subjektov o tejto možnosti.

Veríme však, že dynamická povaha spamu podnieti zákonodarcu k náprave aspoň časti tu uvedených nedostatkov.

Použitá literatúra

HANUŠ, L. Argumentace nebo svévole. Úvahy o právu, spravedlnosti a etice. Praha: C.H.Beck, 2008. 221 s. ISBN 978-80-7400-035-5.

JANSA, L., OTEVŘEL, P., MATĚJKA, M., ČERMÁK, J., MALIŠ, P., HOSTAŠ, P., MATEJKA, J. Internetové právo : Praktický průvodce. Praha: Computer Press, 2016. 432 s. ISBN 978-80-2514-664-4.

POLČÁK, R. Právo na internetu: spam a odpovědnost ISP. Praha: Computer Press, 2007. 150 s. ISBN 978-80-2511-777-4.

MATEJKA, J. Anti-Spam Legislation in Consideration of Personal Data Protection and Other Legal Instruments. In: The Lawyer Quarterly, 2016, č. 2, s. 90-114. ISSN 1805-8396.

RAMBOUSEK, K., MIČUDOVÁ, T. Za spam hrozí pokuta až do 66 tisíc eur. In: Finančný manažment, 2012, č. 5, s. 52 – 57. ISSN 1338-7065.

Súdne rozhodnutia

Rozhodnutie Najvyššieho súdu SR, sp. zn. 3 M Cdo 7/2005

Rozhodnutie Ontario Superior Court of Justice vo veci Ontario Inc. v. Nexx Online Inc., Ref. No. C20546/99

Legislatíva

Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

Zákon č. 147/2001 Z. z. o reklame v znení neskorších predpisov

Zákon č. 22/2004 Z. z. o elektronickom obchode v znení neskorších predpisov

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov

Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov

Zákon č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov

Zákon č. 480/2004 Sb. o některých službách informační společnosti v znení neskorších predpisov

Smernica Európskeho parlamentu a Rady 2002/58/ES zo dňa 12.07.2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách)

Metodický pokyn Ministerstva financií SR č. 42/2008 na použitie odborných výrazov pre oblasť informatizácie spoločnosti

Tabuľka zhody smernice o súkromí a elektronických komunikáciách s právnymi predpismi SR

Kontaktné údaje:

Mgr. Marek Ivančo
marek.ivanco@flaw.uniba.sk
Katedra občianskeho práva
Právnická fakulta Univerzity Komenského v Bratislave
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava 1
Slovenská republika

OCHRANA DUŠEVNÉHO VLASTNÍCTVA DIZAJNÉROV[1]

Petra Janská

Univerzita Komenského v Bratislave, Právnická fakulta

Abstrakt: The phenomenon of the Internet as a global system of interconnected computer networks offers many advantages, but also negatives. One of them is to facilitate the procedure of counterfeiters who violate intellectual property rights worldwide. The contribution will be given legal way for designers whose rights are being violated more and more just "thanks" website.

Abstrakt: Fenomén internet ako globálny systém vzájomne prepojených počítačových sietí predstavuje mnoho výhod, avšak aj negatív. Jedným z nich je uľahčenie konania falšovateľov, ktorí celosvetovo porušujú práva duševného vlastníctva. Predmetný príspevok sa bude venovať spôsobom právnej ochrany pre dizajnérov, ktorých práva sú čoraz viac porušované práve „vďaka“ webu.

Kľúčové slová: counterfeiting - Design - Intellectual Property – legal protection

Kľúčové slová: falšovanie – dizajn – duševné vlastníctvo – právna ochrana

1 ÚVOD

Podnetom na zvýšený záujem o danú tému mi bolo niekoľko článkov z prostredia dizajnu.[2] Vzhľadom na charakter duševného vlastníctva je v súčasnom období rozmáhajúceho sa internetu čoraz viac lákavé pre falšovateľov pristúpiť ku porušovaniu práv nie len dizajnérov. Dané zásahy do nehmotných práv tvorcov predstavujú výrazný zásah do ich finančnej sféry a môžu mať dokonca vplyv na zhoršenie ich značky, či povesti. Vzhľadom na to, že na Slovensku som sa doposiaľ príliš nestretla s „veľkými“ spormi v oblasti dizajnov, rozhodla som sa zmapovať situáciu dizajnérov na Slovenku a následne ponúknuť možnosti ochrany s prihliadnutím na porušovanie ich práv na internete. Na dosiahnutie účelu som prostredníctvom e-mailu oslovila desiatky dizajnérov, najmä z oblasti grafického a textilného dizajnu, pričom zhrnutiu ich odpovedí sa budem venovať v podkapitole 3.1.

Vo všeobecnosti za dizajnéra považujeme osobu, ktorá robí dizajn[3]. Širšie definovanie ponúka psychológ Herbert Simon: „Dizajnuje každý, kto navrhuje a cielene koná k zmene existujúcich situácií na svoje vlastné.“[4] Dizajnér ako taký môže pôsobiť vo viacerých odvetviach, a to napríklad: grafický dizajn, typografia, interiérový dizajn, produktový dizajn, web dizajn, módny, textilný, odevný dizajn, transport dizajn, šperk, keramika, sklo, porcelán a iné.

2 VÝZNAM DIZAJNU

Jednoducho možno konštatovať, že dizajn možno nájsť všade. Čokoľvek, čoho sa dotkla ľudská ruka, má dizajn. Na účely zákona o dizajnoch[5] sa rozumie dizajnom vonkajšia úprava výrobku

1 Tento príspevok vznikol v rámci riešenia vedeckého projektu s názvom „Ochrana priemyselného vlastníctva na Univerzite Komenského“. Grant UK č. UK/400/2016.

2 napr.: *From Runway to Replica: Intellectual Property Strategies for Protecting Fashion Designs* [online]. Natasha Reed, 2016 [cit. 2016-11-06]. Dostupné z: http://www.trademarkandcopyrightlawblog.com/2016/02/from-runway-to-replica-intellectual-property-strategies-for-protecting-fashion-designs/

3 J. Kačala – M. Pisárčiková – M. Považaj. Krátky slovník slovenského jazyka 4 Bratislava: Veda, 2003

4 SIMON, H. A. (1996). The Sciences of the Artificial (third ed.). Cambridge, MA: MIT Press (s. 111)

5 Zákon č. 444/2002 Z.z. o dizajnoch v znení neskorších predpisov (čl. 3 nariadenia Rady EÚ č. *6/2002* z 12. decembra 2001 o dizajnoch)

alebo jeho časti spočívajúca v znakoch, ktorými sú najmä línie, obrysy, farby, tvar, štruktúra alebo materiál samého výrobku alebo jeho zdobenia, pričom výrobkom možno rozumieť akúkoľvek priemyselne alebo remeselne zhotovenú hmotnú vec vrátane obalu, úpravy, grafických symbolov, typografických znakov alebo z častí určených na zostavenie zloženého výrobku s výnimkou počítačových programov.

V dnešnej stratégii Európskej únie tzv. Únii inovácií 2020 sa považuje dizajn za ťažisko hybnej sily inovácií. Možno ho označiť za strategický nástroj inovácie zameranej na používateľa, čo znamená, že má priestor pri transformácii výskumu a vývoja. Dizajn je umením aj vedou, formuje naše domovy a naše pracoviská, a je všade okolo nás, nech sme kdekoľvek. V podnikaní ako takom je dizajn základom úspechu. Najideálnejšie sa dizajn zameriava priamo na používateľa, kombinuje estetické, ekonomické a praktické hodnoty a pre zákazníkov je znakom, podľa ktorého identifikujú geniálnosť inovácie. Na základe stratégie EÚ možno konštatovať, že v Európe sa uznáva potreba podpory európskych dizajnérov a európskych podnikov pri vývoji ich stratégie dizajnu. Zároveň o dizajne možno uviesť, že je majetkom spoločnosti, s ktorým možno obchodovať alebo ho použiť ako zábezpeku. Prakticky funguje ako podpis duševného vlastníctva. EUIPO[6] triedi dizajny nasledovne:

- Obaly výrobkov
- Výrobok/súprava výrobkov
- Zložené výrobky
- Časti výrobkov
- Logá
- Počítačové ikony
- Typy písma
- Kresby a umelecké diela
- Úpravy
- Zdobenie
- Dizajn webových stránok
- Mapy[7]

Na Slovensku má problematika dizajnu dlhú tradíciu. Nebudem sa jej v predmetnom príspevku venovať obsiahlejšie, ale je upravená na webstránke Slovenského centra dizajnu (SCD)[8]. SCD je štátna príspevková organizácia Ministerstva kultúry SR. Avšak spomeniem, že za pioniera rodiacej sa dizajnérskej profesie sa považuje Michael Thonet z firmy Thonet (rakúska firma pôsobiaca na území Slovenska v časoch Rakúsko-Uhorska a zameriavala sa na výrobu nábytku z ohýbaného dreva. V oblasti sklárstva bola veľmi úspešná skláreň firmy Schreiber založená v roku 1892 v Lednických Rovniach. Ako prvá v Európe používala na dekorovanie skla pantograf, no aj v ostatných ohľadoch patrila medzi najmodernejšie vybavené sklárne. Táto skláreň existuje podnes a kvalita dizajnu predstavuje základ jej obchodných úspechov. Pre čitateľa bude pravdepodobne známa značka Sandrik v Dolných Hámroch, ktorej podnik bol založený v roku 1895 a ich kuchynské príbory sú používané ešte v súčasnosti. Pri výrobe príborov a stolového riadu podnik využíval progresívnu technológiu galvanického pokovovania. Výrobky v roku 1900 na svetovej výstave v Paríži získali zlatú medailu a následne začala firma Sandrik dodávať riad pre najvýznamnejšie európske hotely. Konkurencieschopnosť a životnosť tejto firmy sa udržala práve vďaka progresívnym výrobným technológiám a kvalitnému dizajnu. Z uvedeného je evidentné, že na dizajn produktov dbali firmy už v minulosti a práve to im zabezpečilo úspech značky.

3 POTREBA OCHRANY DIZAJNU A ČO NA TO PRAX

Naproti minulosti však nastalo „obdobie internetu“, ktoré znamená nielen pre dizajnérov riziko pri ochrane ich tvorby. To znamená, že hoci aj v súčasnosti mnohí výrobcovia dbajú na kvalitný dizajn,

6 European Union Intellectual Property Office = Úrad Európskej únie pre duševné vlastníctvo

7 Pozri zatriedenie aj podľa obrázkov na Definícia dizajnu. *EUIPO - Úrad Európskej únie pre duševné vlastníctvo* [online]. [cit. 2016-10-28]. Dostupné z: https://euipo.europa.eu/ohimportal/sk/design-definition

8 KOLESÁR, Z.: Dizajn na Slovensku - začiatky. In: *Slovenské centrum dizajnu* [online]. Bratislava [cit. 2016-11-14]. Dostupné z: http://www.sdc.sk/?dizajn-na-slovensku

ktorý by mal potenciálneho zákazníka presvedčiť, že sa má rozhodnúť práve pre jeho výrobok, no vytvoriť skvelý a pútavý dizajn už nestačí.

V podstate súčasnú situáciu môžeme pomenovať ako začarovaný kruh, keďže internet dobre slúži na zviditeľnenie značky, rozšírenie predaja aj do zahraničia, ale na druhej strane otvára možnosti pre falšovateľov, ktorý za veľmi lacné vstupné náklady dokážu produkovať podobné, prípadne celkom rovnaké a pre laika nerozoznateľné falzifikáty, čím sa výrazne zasahuje do práva duševného vlastníctva dizajnérov.

Čo sa týka slovenskej praxe, tak v júni roka 2014 sa vtedajší predseda Úradu priemyselného vlastníctva SR Ľuboš Knoth k slovenskej realite vyjadril tak, že sa nástroje priemyselného vlastníctva využívajú viac-menej iba v dvoch rovinách. Jedna rovina je právo ochrannej známky, ktoré sú už húfne využívané, v oveľa menšej miere sa využívajú technické patenty a keďže domáci podnikatelia často preferujú krátkodobú realizáciu plánov, tak inštitút ochrany dizajnu ignorujú.[9] Posledná výročná správa ÚPV označuje rok 2015 rokom, keď sa prebudil inovátorský duch krajiny a posilnilo sa vedomie o priemyselnoprávnej ochrane riešení. Zároveň však uvádza, že hoci je na Slovensku veľmi veľa talentovaných dizajnérov, dokonca úspešných šéfdizajnérov známych značiek a výnimočných dizajnov, tak význam ochrany dizajnu stále nie je úplne docenený a počet prihlášok dizajnov nestúpol.[10] Na ilustráciu uvádzam tabuľku z danej výročnej správy týkajúcu sa počtov prihlásených dizajnov.

Dizajny	2011	2012	2013	2014	2015
Prihlášky dizajnov	108	120	125	100	95
z toho domáce	96	97	101	82	84
z toho zahraničné	12	23	24	18	11
Zapísané dizajny	73	117	128	102	94
z toho domáce	60	102	100	77	85
z toho zahraničné	13	15	28	28	9

Tabuľka 1: Počty prihlásených dizajnov

3.1 POSTREHY OD SLOVENSKÝCH DIZAJNÉROV

V rámci prieskumu reality v oblasti dizajnu som oslovila desiatky dizajnérov z adresáta zverejneného Slovenským centrum dizajnu. To znamená, že oslovená vzorka bola pestrá, odpovedali dizajnéri z prostredia akadémie, väčších firiem, či pracujúcich jednotlivo. Čo sa týka vnímania porušovania duševného vlastníctva, tak toto vnímajú takmer všetci. Podľa ich vyjadrení, keď sa vytvorí niečo vizibilné, tak sa to často odkopíruje. Tiež by mali záujem o ochranu nie len loga, ale taktiež konceptov celých riešení značiek. Mnohí prezentovali, že by prijali zriadenie združenia obdobného SOZA-e, ktoré by zastupovalo ich práva, resp. nejakú komoru ako samosprávnu stavovskú právnickú osobu. Jednou so skúseností dizajnérov bolo, že logo slovenského dizajnéra určené pre časopis, bolo ukradnuté zahraničným dizajnérom, a to paradoxne pre právnickú firmu. Taktiež dizajnérom vytvorené písmo sa nachádza voľne na internete na pirátskych stránkach, kde sú voľne stiahnuteľné kýmkoľvek. Jeden z dizajnérov prezentoval

[9] Ako podporiť ekonomiku cez duševné vlastníctvo? In: *Slovenské centrum dizajnu* [online]. Bratislava: EurActiv.sk, 2014 [cit. 2016-11-01]. Dostupné z: https://euractiv.sk/clanky/veda-a-inovacie/ako-podporit-ekonomiku-prostrednictvom-dusevneho-vlastnictva-022614/

[10] Výročná správa ÚPV za rok 2015. Dostupné z: http://www.indprop.gov.sk/swift_data/source/dokumenty_na_stiahnutie/vyrocne_spravy/VS_2015.pdf

skúsenosti z tendrov a výberových konaní, kedy dizajnér ako účastník nie je vybratý, ale s jeho návrhmi sa naďalej pracuje a sú editované. Tiež sa stáva, že potenciálnemu klientovi predloží dizajnér svoj návrh, klient odmietne alebo prestane komunikovať a neskôr sa ukáže, že tento návrh používa, občas trochu modifikovaný. Mnohí majú problém pri dokazovaní falšovania ich duševného vlastníctva. Pozitívnym momentom je, že medzinárodné koncerny, resp. väčšie firmy si svoje produkty starostlivo strážia a častokrát nechávajú dokonca patentovať. V otázke druhov využívanej ochrany možno konštatovať, že je využívaná minimálne, a to najmä z dôvodov nedôvery vo vymožiteľnosť práva na Slovensku. Niektorí z dizajnérov priamo napísali adminom, ktorí spravovali webstránky s ich dizajnami, čomu admin môže a nemusí vyhovieť a vtedy bude rozhodujúce dokázať, že ide o tvorbu dizajnéra, ktorý sa domáha odstránenia. Nútene možno stiahnutie z webstránky dosiahnuť iba súdnou cestou.

Všetky postrehy od dizajnérov budú pre mňa podnetom pre ďalší výskum a snahu o zlepšenie prostredia v oblasti dizajnérov, nakoľko jednoznačne môžem vyhodnotiť, že záujem o poradenstvo tu existuje a daná téma si zaslúži komplexnú úpravu aj pre laikov, ktorí mnohokrát oželejú pár stovák eur pri porušení ich duševného vlastníctva naproti tomu, aby sa domáhali svojich práv u orgánov ochrany štátu.

4 AKO MOŽNO DIZAJNY CHRÁNIŤ

Pri vytváraní ochrany ako takej je potrebné mať na zreteli, že existuje ochrana vytvorená momentom vzniku nehmotného statku (tzv. **neformálna ochrana** – autorské právo), ďalej ochrana priemyselného vlastníctva zabezpečená Úradom priemyselného vlastníctva SR so sídlom v Banskej Bystrici (ďalej len „ÚPV“) vo fáze, kým sa nehmotné statky, či výsledky tvorivej duševnej činnosti nestanú predmetom subjektívneho absolútneho práva (tzv. **formálna ochrana** - napr. právo majiteľa patentu, právo majiteľa osvedčenia o zápise dizajnu v registri dizajnov, právo osvedčenia o zápise ochrannej známky v registri ochranných známok). Ochrana týchto práv znamená ich ochranu proti nelegálnemu obchodu a falšovaniu. Ak však dôjde k porušeniu po vytvorení takejto formálnej ochrany, je možné sa svojich práv domôcť prostredníctvom občianskoprávneho konania na súde a v takom prípade pôjde o **súdnu ochranu** (taktiež prichádza do úvahy aj trestnoprávne konanie). Pri porušení práva, v dôsledku ktorého vznikne škoda, má poškodený právo na jej náhradu. Poškodený môže požadovať náhradu skutočnej škody a tiež ušlý zisk, ktorý mu vznikol v dôsledku porušenia jeho práv. Ak bolo poškodené dobré meno dizajnéra, jeho česť alebo dôstojnosť, môže sa domáhať aj náhrady nemajetkovej ujmy, najmä formou ospravedlnenia alebo zverejnenia rozsudku súdu na náklady osoby, ktorá porušila alebo ohrozila jeho právo duševného vlastníctva. Pokiaľ by takýto spôsob vzhľadom k spôsobenej ujme nebol dostatočný, môže súd priznať aj náhradu v peniazoch. Poškodený má tiež nárok domáhať sa, aby porušovanie či ohrozovanie práva bolo zakázané a následky odstránené. Vzhľadom na potrebu rozsahového obmedzenia príspevku sa však autorka súdnej ochrane ďalej v predmetnom článku nevenuje. Je tiež potrebné uviesť, že efektívnou ochranou pred porušovateľmi duševného vlastníctva prostredníctvom internetu môže byť aj využitie riešenia, ktoré nemá právnický charakter. Príkladom je ochrana webstránky pred kopírovaním. Ak dizajnér umiestňuje svoju tvorbu na internete, tak sa môže aspoň priblížiť ku zamedzeniu kopírovania textu a obrázkov, vytlačeniu a uloženiu webovej stránky, ale celkom zabrániť tomu nie je možné. Neskúseného používateľa však takýto druh ochrany môže rýchlo odradiť. Príkladom takejto neprávnej ochrany je použitie CSS ochrany alebo Javascript ochrany.[11] Vzhľadom na neustály rozvoj informačných technológií možno predpokladať, že takýto druh ochrany bude mať opodstatnenie aj v budúcnosti avšak nie je ochranou, ktorej vymoženie by zabezpečoval štát.

4.1 PRÁVNE FORMY OCHRANY

Spektrum právnych prostriedkov ochrany je pomerne široké. Medzi právne formy ochrany možno zahrnúť autorské právo ako typické právo duševného vlastníctva, ktoré vzniká momentom vzniku bez potreby registrácie v konkrétnom registri. Ďalšou možnosťou právnej ochrany dizajnu môže byť aj spísanie zmluvy v zmysle Obchodného zákonníka. V oblasti priemyselných práv existuje na vytvorenie ochrany formálny proces, ktorý je upravený normami vereného práva a pred vznikom

[11] LIPTÁK, M.: *Ochrana web stránky pred kopírovaním* [online]. In: . 2010 [cit. 2016-11-06]. Dostupné z: https://martinliptak.wordpress.com/2010/01/28/ochrana-web-stranky-pred-kopirovanim/

ochrany týchto predmetov duševného vlastníctva je potrebná registrácia v príslušnom registri. Bez toho, aby bol predmet duševného vlastníctva (napr. logo) zapísaný v registri vedenom ÚPV (register dizajnov), nie je možné očakávať ochranu štátom. Registrácia do príslušného registra je pri týchto predmetoch nevyhnutnou pri vytváraní ochrany. Na registrovanie do toho konkrétneho registra je potrebné podať prihlášku a zaplatiť správny poplatok. V prípade tvorby dizajnérov v mnohých prípadoch nebude postačovať iba ochrana dizajnu, ale je treba myslieť aj na ochranu technickej stránky veci a častokrát je náležité podať prihlášku aj do registra patentov, príp. ochranných známok. Zvolenie si správnej kombinácie foriem ochrany prináleží tvorcovi, ktorý sa v danej problematike môže poradiť s odborníkom v oblasti duševného vlastníctva, napr. s patentovým zástupcom.

4.1.1 AUTORSKÉ PRÁVO

Autora (napr. dizajnéra) autorské právo chráni pred nepovoleným zhotovovaním kópií, no nechráni nápad samotný. Autorské právo vzniká automaticky bez potreby registrácie a nevyžaduje žiadne poplatky. Neposkytuje žiadnu ochranu proti komukoľvek, kto nezávisle na dizajnérovi prišiel s rovnakou alebo podobnou myšlienkou. Konkurent môže tvrdiť, že jeho nápad je podobný náhodou, respektíve situáciu otočiť. Originalitu riešenia (autorstvo) možno preukázať rôznymi spôsobmi. Dizajnér by si mal spraviť písomný popis, fotografiu či nákres svojho nápadu a tieto umiestniť na CD, DVD či USB alebo takto vytlačené dokumenty zapečatiť do obálky aj s písomným prehlásením nezávislého svedka s dátumom podpisu na preukázanie dňa zapečatenia obálky. Danú obálku by dizajnér mal doporučene zaslať na miesto úschovy, prípadne sebe a uschovať si doručenku z pošty, na ktorej je jednoznačne vyznačený dátum odoslania. Neotvorená a zapečatená obálka pre súd predstavuje dôkaz priority autorského práva. Miestom úschovy môže byť napríklad aj notár, ktorý koná vo veciach úschov v zmysle zákona č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) a o zmene a doplnení ďalších predpisov.

4.1.2 ZMLUVA O MLČANLIVOSTI

Zmluvné strany môžu v súlade s § 269 ods. 2 Obchodného zákonníka uzatvoriť aj zmluvu, ktorú Obchodný zákonník neupravuje ako zmluvný typ, a to konkrétne zmluvu o mlčanlivosti (označovanú tiež za zmluvu o utajení, dohodu o (zachovaní) mlčanlivosti, zmluva/dohoda o zachovaní tajomstva, po anglicky non-disclosure agreement, skratka NDA). Túto zmluvu je možné uzatvoriť samostatne alebo je možné jej ustanovenia zakomponovať do inej zmluvy. Aby bol záväzok mlčanlivosti dostatočne určitý je potrebné vymedziť predovšetkým rozsah povinnosti zachovávať mlčanlivosť, a to uvedením všetkých dôverných informácií, skutočností alebo dokumentov, o ktorých majú zmluvné strany zachovávať mlčanlivosť.[12] Pre zabezpečenie záväzku môže byť zmluvnými stranami dohodnutá zmluvná pokuta. V prípade porušenia takejto zmluvy riskuje zmluvná strana, ktorá zmluvu porušila, súdnu žalobu. Uvedené zmluva chráni dizajnéra v každej fáze vývoja nápadu, t.j. bez ohľadu na ďalšie použité formy práv duševného vlastníctva a dokonca aj dlho potom, čo bol dizajn uvedený na trh. Problematickým môže byť presvedčiť iné osoby, aby zmluvu o mlčanlivosti podpísali bez toho, aby im bol nápad predstavený, preto by mal dizajnér vedieť už pred podpisom zmluvy predostrieť napríklad obchodné výhody jeho nápadu bez konkretizovania daného nápadu. Zmluva o mlčanlivosti bráni tretím osobám iba v zverejnení alebo využití konkrétnych a jedinečných tajných informácií, ktoré sa dozvedeli od tvorcu. Informácie, ktoré sú už všeobecne známe, však môže voľne používať ktokoľvek bez ohľadu na existujúcu zmluvy o mlčanlivosti. Akonáhle sa dôverné informácie, ktoré sú zmluvou chránené, stanú všeobecne známe akýmkoľvej iným spôsobom, tak zmluvné strany už touto zmluvou viazané nie sú.

4.1.3 PRÁVO K NEZAPÍSANÉMU DIZAJNU

Právo k nezapísanému dizajnu je podobné autorskému právu tým, že je bezplatné a poskytuje právo dlhoročnej ochrany proti nedovolenému kopírovaniu. Neexistuje žiaden oficiálny register práv k takýmto dizajnom. Preto nemusí byť pre tretie osoby samozrejmé sa o dizajne dozvedieť a preto treba opäť myslieť na zabezpečenie dôkazu novosti nápadu pre prípad sporu. Právo k nezapísanému dizajnu nechráni kopírované alebo zvyčajné dizajny, ktoré na prvý pohľad pripomínajú iné dizajny. V rámci uplatnenia „voľnosti“ dizajnu môže dizajnér pretvoriť akýkoľvek

[12] Zmluva o mlčanlivosti (§ 269 ods. 2 zákona č. 513/1991 Zb.). In: *Epi.sk* [online]. [cit. 2016-11-06]. Dostupné z: http://www.epi.sk/vzor-zmluvy-a-pravneho-podania/zmluva-o-mlcanlivosti.htm

predmet, ktorý nie je súčasťou iného výrobku. Napríklad brzdová doštička môže mať iba jeden tvar, aby sa hodila do brzdového obloženia. Tu sa teda „voľnosť" dizajnu uplatniť nedá a výrobok z hľadiska dizajnu ochranu nemá.[13]

Právo k nezapísanému dizajnu vzniká pri vytvorení dizajnu automaticky. Mal by však byť použitý postup zapečatenej obálky tak, ako bol konkretizovaný vyššie pre dôkaz autorského práva, čím dizajnér získa dôkaz o prioritnom dátume. Žalobu na určitú osobu je možné podať iba ak je žalobca (dizajnér) schopný dokázať, že porušovateľ duševného vlastníctva vytvoril podobný dizajn na základe „nedovolenej inšpirácie".

Aj napriek skutočnosti, že takáto forma ochrany je užitočná (lepšia ako žiadna samozrejme), tak v rámci efektívnejšej stratégie ochrany duševného vlastníctva je istejšie využiť formálne vytvorenie ochrany prostredníctvom registrácie na ÚPV.

4.1.4 REGISTRÁCIA DIZAJNU

Dizajnom sa prostredníctvom formálneho zápisu chráni vonkajšia úprava výrobku. Predmet ochrany predstavuje vyobrazený vzhľad výrobku alebo jeho časti a rozsah ochrany určuje vyobrazenie dizajnu v zmysle zápisu v registri dizajnov na ÚPV. Je potrebné dať do pozornosti, že inštitút zapísaného dizajnu nechráni technickú, konštrukčnú, funkčnú, materiálovú alebo inú podstatu výrobku, aj v prípade ak by bola z vyobrazení zrejmá v konkrétnom vyhotovení alebo i zovšeobecnená. Tvorbu dizajnéra možno takto ochrániť ak ide o nový dizajn, ktorý má osobitý charakter. Novosť dizajnu sa posudzuje tak, že pred dňom podania prihlášky alebo pred dňom vzniku práva prednosti nebol sprístupnený verejnosti zhodný dizajn, ktorý by a líšil len nepodstatne. Osobitosť dizajnu je dodržaná vtedy, ak celkový dojem, ktorý vyvoláva u informovaného užívateľa, sa líši od celkového dojmu, ktorý u takého užívateľa vyvoláva dizajn, ktorý bol sprístupnený verejnosti pred dňom podania prihlášky alebo pred dňom vzniku jeho práva prednosti.

Na ochranu duševného vlastníctva dizajnom sa vyžaduje podanie prihlášky na ÚPV, a to pôvodcom alebo jeho právnym zástupcom. Ak pôvodca vytvoril dizajn v rámci plnenia úloh vyplývajúcich z pracovnoprávneho pomeru (tzn. podnikový dizajn), prechádza právo na dizajn na zamestnávateľa, ak nie je zmluvou ustanovené inak (tzv. zamestnanecké diela). Podaním prihlášky vzniká prihlasovateľovi právo prednosti. Vlastníkovi zapísaného dizajnu vydá ÚPV osvedčenie o zápise. Zápis oznámi vo vestníku úradu.

Vlastník zapísaného dizajnu má výlučné právo využívať dizajn, poskytovať súhlas na využívanie dizajnu iným osobám (licenciu) alebo na nich dizajn previesť. Licencia sa udeľuje prostredníctvom licenčnej zmluvy, ktorá nadobúda účinnosť voči tretím osobám zápisom do registra dizajnov. Zápis dizajnu platí päť rokov odo dňa podania prihlášky dizajnu. Vlastník dizajnu môže túto dobu ochrany opakovane obnoviť, a to vždy o 5 rokov, až na celkovú dobu 25 rokov od dátumu podania prihlášky dizajnu.

V prípade, že je duševné vlastníctvo takto chránené, tak môže dizajnér podať žalobu na kohokoľvek, kto vyrába, dováža, predáva alebo využíva výrobky podobné zapísanému dizajnu bez udelenia súhlasu - licencie. Rozdiel s právom k nezapísanému dizajnu je, že v tomto prípade nie je potrebné dokazovať, že iný dizajn vznikol skopírovaním, stačí dokázať, že sa podobá hoci len náhodou na dizajn zapísaný v registri.

4.1.5 OCHRANNÁ ZNÁMKA

Dielo dizajnéra, ktoré bude obsahovať označenie, ktoré možno graficky znázorniť a ktoré tvoria najmä slová vrátane osobných mien, písmená, číslice, kresby, tvar tovaru alebo jeho obal, prípadne ich vzájomné kombinácie bude možné zaregistrovať ako ochrannú známku v prípade, že takéto označenie je spôsobilé rozlíšiť tovary alebo služby jednej osoby od tovarov alebo služieb inej osoby.[14] Ide o formálnu registráciu do registra ochranných známok, ktorý vedie ÚPV a v prípade, že majiteľ takejto ochrannej známky bude pravidelne platiť udržiavacie poplatky, tak môže mať časovo neobmedzenú platnosť. Dizajn chránený ochrannou známkou tak môže byť časom najcennejšou formou duševného vlastníctva, nakoľko ak sa stane obľúbenou značkou, tak bude majiteľa ochrannej

[13] Formy práv DV. In: *Úrad priemyselného vlastníctva: Patentovat.sk* [online]. [cit. 2016-11-06]. Dostupné z: http://www.patentovat.sk/vynalezy-patenty-a-dodatkove-ochranne-osvedcenia/prirucka-vynalezcu/ochrana-vasho-napadu/formy-prav-dv/

[14] § 2 zákona č. 506/2009 Z. z. o ochranných známkach v znení neskorších predpisov

známky odlišovať výrazným spôsobom od iných subjektov na trhu, čím bude mať značnú konkurenčnú výhodu. Vďaka ochrannej funkcie ochrannej známky môže predovšetkým plniť pre spotrebiteľa úlohu identifikácie pôvodu či očakávanú kvalitu tovarov alebo služieb a jej majiteľovi zabezpečiť odbyt pre jeho tovary respektíve služby.[15] Ochranné známky avšak nechránia nápady alebo výrobky ako také.

4.1.6 PATENT

V prípade, že výrobok, ktorý môže vytvoriť aj dizajnér, disponuje okrem špeciálneho dizajnu aj novým a priemyselne využiteľným riešením, možno ho považovať za vynález a stáva sa tak možným predmetom registrácie do registra patentov vedeného ÚPV. Patent predstavuje formu legálneho monopolu, čo jednoducho znamená, že nikto nemôže tento patent používať bez toho, aby majiteľovi patentu za jeho využitie zaplatil odmenu. Patent je udeľovaný štátom ako protihodnota možnosti zverejnenia príslušného vynálezu. Patentovanie nápadu nemusí nutne zvýšiť jeho obchodnú hodnotu. Pokiaľ má vynález komerčný potenciál, môže patent predstavovať výlučný spôsob ako zabezpečiť, aby z neho tvorca mal aj finančný prospech. Je fakt, že získanie ochrany patentom je spomedzi všetkých druhov duševného vlastníctva najnákladnejšia a proces je najzložitejší, preto je nevyhnutné si také rozhodnutie dôkladne zvážiť. Za predpokladu platenia udržiavacích poplatkov platí patent maximálne 20 rokov.[16]

4.1.7 AKO OCHRÁNIŤ DIZAJN V ZAHRANIČÍ

Formálna ochrana registráciou v registroch ÚPV (patentom, dizajnom, ochrannou známkou) má teritoriálny charakter, čo znamená, že platí len na území Slovenskej republiky, kde bola táto ochrana priznaná. Ak je predpoklad, že dizajnový produkt sa bude predávať, vyrábať, resp. distribuovať do iných krajín, kde sa očakáva obchodný úspech, tak je potrebné zvážiť získanie ochrany aj v týchto štátoch. Podľa medzinárodného dohovoru (Parížsky dohovor na ochranu priemyselného vlastníctva z roku 1883) je možné podať prihlášku dizajnu takmer v každej krajine. Ochranu dizajnu v zahraničí môže slovenský subjekt získať podaním prihlášky dizajnu na príslušnom zápisnom mieste priamo v krajine, v ktorej sa ochrana požaduje.

Medzinárodnú ochranu dizajnov upravuje Haagska dohoda o medzinárodnom prihlasovaní priemyselných vzorov a modelov z roku 1925. Hoci Slovenská republika priamo nie je jej zmluvnou stranou, pristúpením Európskej únie k Ženevskému aktu Haagskej dohody sa otvorila možnosť využívania výhod medzinárodného systému aj pre slovenských prihlasovateľov. Na registráciu dizajnu v zahraničí je teda možné využiť podanie jedinej jednotnej medzinárodnej prihlášky a získať tak ochranu na území EÚ a na území Ženevského aktu, tzn. aj v iných krajinách mimo územia EÚ. Nevýhodou však je, že odmietnutie prihlášky v jednej z krajín spôsobuje zamietnutie prihlášky dizajnu vo všetkých krajinách.[17] Prostredníctvom Haagskeho systému medzinárodnej registrácie priemyselných dizajnov je možné jedinou prihláškou získať ochranu až v 55 zmluvných stranách. Z podaných prihlášok je možné využiť prioritné právo pre ďalšie podania. Prihláška sa podáva priamo v sídle Svetovej organizácie duševného vlastníctva v Ženeve (WIPO).

Ak má dizajnér záujem o ochranu prostredníctvom ochrannej známky vo viacerých krajinách, môže si podať prihlášku buď na zápis medzinárodnej ochrannej známky podľa madridského systému, a to vo Svetovej organizácii duševného vlastníctva (WIPO) so sídlom v Ženeve, alebo prihlášku ochrannej známky Spoločenstva (za účelom ochrany iba v EÚ), a to v EUIPO.

5 ZÁVER

Po niekoľkonásobnom zamyslení sa nad reakciami slovenských dizajnérov a celkovo nad hodnotením využívania prostriedkov ochrany pre výsledky duševnej činnosti mi prichádza na myseľ zásada, ktorá platila už v rímskom práve, podľa ktorej „vigilantibus iura scripta sunt", t. j. „práva patria

---

[15] MARUNIAKOVÁ, I. a kol.: *Komentár k zákonu o ochranných známkach*. Banská Bystrica: ÚPV SR, 2012. S. 69. ISBN 978-80-88994-79-4.

[16] zákon č. 435/2001 Z. z. o patentoch, dodatkových ochranných osvedčeniach a o zmene a doplnení niektorých zákonov (patentový zákon)

[17] MAJLINGOVÁ, M.: Praktické skúsenosti firiem s ochranou dizajnu mimo územia Slovenskej republiky. In: *Duševné vlastníctvo na Slovensku VII: k Svetovému dňu duševného vlastníctva*. Banská Bystrica: ÚPV SR, 2007, s. 101. ISBN 978-80-88994-56-5.

len bdelým" (pozorným, opatrným, starostlivým). To znamená tým, ktorí sa aktívne zaujímajú o ochranu a výkon svojich práv a ktorí svoje procesné oprávnenia uplatňujú včas a s dostatočnou starostlivosťou a predvídavosťou. Je fakt, že stagnujúci počet prihlášok dizajnu u nás kopíruje aj dlhodobo zachovanú mieru podávaných prihlášok registrovaného dizajnu Európskej únie v EUIPO. EUIPO uvádza, že čím viac pozornosti venujú podniky dizajnu, tým sú úspešnejšie. Rast spoločností, ktoré si cenia dizajn, je o 22 % vyšší než tých, ktoré na dizajn nedbajú. Dobrý dizajn je dôležitým pilierom úspechu podnikov.

Uvedené skutočnosti sú nesporne dôvodom, prečo by mali slovenskí dizajnéri venovať viac pozornosti ochrane svojej tvorby, svojho duševného vlastníctva, pokiaľ chcú byť svetoví a zachovať si konkurencieschopnosť. Je fakt, že úroveň právneho povedomia v danej oblasti má ešte rezervy, ale aktivity ÚPV a taktiež mnoho projektov, ktoré sa na Slovensku realizujú s podporou nadnárodných organizácií ochrany duševného vlastníctva, najmä na podporu malých a stredných podnikov, sú nádejou na zmenu.

Použitá literatúra:

Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

Zákon č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) a o zmene a doplnení ďalších predpisov

Zákon č. 444/2002 Z.z. o dizajnoch v znení neskorších predpisov

Zákon č. 506/2009 Z. z. o ochranných známkach v znení neskorších predpisov

MARUNIAKOVÁ, I. A kol.: *Komentár k zákonu o ochranných známkach*. Banská Bystrica: ÚPV SR, 2012. ISBN 978-80-88994-79-4. 305 s.

Zákon č. 435/2001 Z. z. o patentoch, dodatkových ochranných osvedčeniach a o zmene a doplnení niektorých zákonov (patentový zákon)

From Runway to Replica: Intellectual Property Strategies for Protecting Fashion Designs [online]. Natasha Reed, 2016 [cit. 2016-11-06]. Dostupné z: http://www.trademarkandcopyrightlawblog.com/2016/02/from-runway-to-replica-intellectual-property-strategies-for-protecting-fashion-designs/

KAČALA, J. – PISARČÍKOVÁ, M. – POVAŽAJ, M.: Krátky slovník slovenského jazyka. 4. dopl. a upr. vyd. Bratislava: Veda 2003. 985 s. ISBN 80-224-0750-X

SIMON, H. A. (1996). The Sciences of the Artificial (third ed.). Cambridge, MA: MIT Press (s. 111)

MAJLINGOVÁ, M.: Praktické skúsenosti firiem s ochranou dizajnu mimo územia Slovenskej republiky. In: Duševné *vlastníctvo na Slovensku VII: k Svetovému dňu duševného vlastníctva*. Banská Bystrica: ÚPV SR, 2007, ISBN 978-80-88994-56-5. 134 s.

Definícia dizajnu. *EUIPO - Úrad Európskej únie pre duševné vlastníctvo* [online]. [cit. 2016-10-28]. Dostupné z: https://euipo.europa.eu/ohimportal/sk/design-definition

KOLESÁR, Z.: Dizajn na Slovensku - začiatky. In: *Slovenské centrum dizajnu* [online]. Bratislava [cit. 2016-11-14]. Dostupné z: http://www.sdc.sk/?dizajn-na-slovensku

Ako podporiť ekonomiku cez duševné vlastníctvo? In: *Slovenské centrum dizajnu* [online]. Bratislava: EurActiv.sk, 2014 [cit. 2016-11-01]. Dostupné z: https://euractiv.sk/clanky/veda-a-inovacie/ako-podporit-ekonomiku-prostrednictvom-dusevneho-vlastnictva-022614/

Výročná správa ÚPV za rok 2015. Dostupné z: http://www.indprop.gov.sk/swift_data/source/dokumenty_na_stiahnutie/vyrocne_spravy/VS_2015.pdf

LIPTÁK, M.: *Ochrana web stránky pred kopírovaním* [online]. In: . 2010 [cit. 2016-11-06]. Dostupné z: https://martinliptak.wordpress.com/2010/01/28/ochrana-web-stranky-pred-kopirovanim/

Zmluva o mlčanlivosti (§ 269 ods. 2 zákona č. 513/1991 Zb.). In: *Epi.sk* [online]. [cit. 2016-11-06]. Dostupné z: http://www.epi.sk/vzor-zmluvy-a-pravneho-podania/zmluva-o-mlcanlivosti.htm

Formy práv DV. In: *Úrad priemyselného vlastníctva: Patentovat.sk* [online]. [cit. 2016-11-06]. Dostupné z: http://www.patentovat.sk/vynalezy-patenty-a-dodatkove-ochranne-osvedcenia/prirucka-vynalezcu/ochrana-vasho-napadu/formy-prav-dv/

Kontaktné údaje:
Mgr. Petra Janská
petra.janska@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Katedra občianskeho práva
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovenská republika

OCHRANA OSOBNÝCH ÚDAJOV NA INTERNETE A PORUŠOVANIE PRÁV S TÝM SPOJENÝCH

Protection of Personal Data on Internet and the Breach of the Rights Connected with the Topic

Daniela Ježová

Univerzita Komenského v Bratislave, Právnická fakulta

Abstrakt: Článok sa zaoberá otázkou ochrany osobných údajov na internete a to v členských krajinách EÚ a prípadmi porušovanie práv s tým spojených. Reforma, ktorú článok popisuje je pre súčasný digitálny vek kľúčovou a zásadnou. Spolu s jej prijatím a uvedením do praxe bude porušovanie práv jednotlivcov v oblasti ochrany osobných údajov ťažšie ako doteraz.

Abstrakt: The article deals with privacy issues on the Internet and in the EU Member States and infringement cases related to it. The reform, which the article describes is for today's digital age a key and essential. Along with the adoption and putting into practice the violation of individual rights of privacy will more difficult than before.

Kľúčové slová: reforma ochrany osobných údajov, jednotný digitálny trh, všeobecné nariadenie o ochrane osobných údajov, smernica o všeobecnej ochrane osobných údajov.

Key words: : reform of the personal data protection, digital single market, general directive on data protection, general regulation on data protection

1 ÚVOD

Tri hlavné inštitúcie EÚ, Európsky parlament, Rada a Európska komisia, začali 24. júna 2015 rokovania v rámci spolurozhodovacieho postupu o navrhovanom všeobecnom nariadení o ochrane údajov, ktorý je známy pod názvom neformálny „trialóg“[1]. Základom pre tento trialóg je návrh Komisie z januára 2012, legislatívne uznesenie Parlamentu z 12. marca 2014 a všeobecný prístup Rady prijatý 15. júna 2015[2]. Tieto tri inštitúcie sa zaviazali zaoberať sa všeobecným nariadením o ochrane osobných údajov v rámci širšieho reformného balíka pre ochranu údajov, ktorý zahŕňa navrhovanú smernicu o všeobecnej ochrane údajov. Tento bol ukončený dňa 27.04.2016 prijatím tzv. balíka reforiem ochrany osobných údajov. Nová právna úprava ochrany osobných údajov v Európskej únii si stanovila za cieľ vytvoriť jednotné pravidlá v celej Európskej únii, posilniť právnu istotu a podporiť dôveru občanov a podnikov v jednotlivý digitálny trh.

Reformný balík obsahuje dva právne predpisy a to :

Nariadenie európskeho parlamentu a rady (EÚ) 2016/679[3] (ďalej len ako „Všeobecné nariadenie o ochrane údajov“ alebo „Nariadenie“) a

---

1 Spoločné vyhlásenia Európskeho parlamentu, Rady, Komisie, Spoločné vyhlásenie o praktických opatreniach pre spolurozhodovací postup (článok 251 Zmluvy o ES) (2007/C 145/02) (Ú. v. EÚ C 145, 30.6.2007).

2 COM(2012)11 final; legislatívne uznesenie Európskeho parlamentu z 12. marca 2014 k návrhu nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov), P7_TA(2014)0212; návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov) – Príprava všeobecného prístupu, dokument Rady 9565/15, 11.6.2015.

3 Nariadenie európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), L 119/1

Smernica európskeho parlamentu a rady (EÚ) 2016/680[4] (ďalej len ako „smernica o ochrane osobných údajov v oblasti justície a súdnictva“ alebo „Smernica“)

Prijatie reformného balíka je míľnikom vo vývoji prinášajúcom širokú škálu počítačovej bezpečnosti súvisiacej implementácie pre členské štáty EÚ a súkromný sektor. Cieľom balíka je zjednotenie právnej úpravy ochrany osobných údajov v členských štátoch Európskej únie so zameraním sa na zvýšenie práv dotknutých osôb ako aj zjednodušenie pravidiel spracúvania osobných údajov pre prevádzkovateľov pôsobiacich v Európskej únii.

Reforma pravidiel ochrany údajov je legislatívny balík navrhnutý za účelom aktualizácie a modernizácie princípov Smernice o ochrane údajov z roku 1995. Unifikovaná a aktuálna legislatíva ochrany údajov je nevyhnutná pre zaručenie základných práv jednotlivcov na ochranu ich osobných údajov, podporu vývoja digitálnej ekonomiky a zefektívnenie boja proti transnacionálnemu zločinu a terorizmu. Jedným z hlavných dôvodov snahy o reformu ochrany osobných údajov je práve rozvíjajúci sa kyberpriestor a putovanie osobných údajov v kyberpriestore. O uvedenom svedčí aj cieľ reformy - posilniť právo na súkromie v online prostredí a podporiť digitálnu ekonomiku Európy. Reformný balík pre ochranu údajov bol navrhnutý predovšetkým ako prostriedok na posilnenie práv na ochranu súkromia online zabezpečením, aby ľudia boli lepšie informovaní o svojich právach a viac si kontrolovali svoje informácie.

Reforma ochrany osobných údajov je základ pre vytvorenie jednotného digitálneho trhu, ktorý je prioritou Únie a má za cieľ slobody spojené s jednotným trhom EÚ rozšíriť na digitálny svet a tým podporiť rast a zamestnanosť v EÚ. V nadväznosti na Lisabonskú stratégiu[5] sa stratégiou Európa 2020[6] zaviedla digitálna agenda pre Európu ako jedna zo siedmich hlavných iniciatív, pričom sa uznala kľúčová úloha využívania informačných a komunikačných technológií, aby EÚ uspela vo svojom úsilí do roku 2020.

Nový právny základ stanovený v článku 16 ZFEÚ a skutočnosť, že v článku 8 Charty základných práv[7], sa právo na ochranu osobných údajov uznáva za samostatné právo a rovnako sa v jej článku 7 za samostatné právo uznáva právo na rešpektovanie súkromia a rodinného života, plne vyžadujú a podporujú komplexný prístup k ochrane údajov vo všetkých oblastiach, v ktorých sa osobné údaje spracúvajú.

Účinný európsky a medzinárodný režim na ochranu údajov je nevyhnutným základom pre cezhraničný tok osobných údajov a súčasné rozdiely v právnych predpisoch na ochranu údajov a v ich presadzovaní ovplyvňujú ochranu údajov a osobné slobody, právnu istotu a jasnosť v zmluvných vzťahoch, rozvoj elektronického obchodu a elektronického podnikania, dôveru spotrebiteľov v systém, cezhraničné transakcie, svetové hospodárstvo a jednotný európsky trh a v tejto súvislosti je výmena údajov dôležitá, keď umožňuje a zaisťuje verejnú bezpečnosť na vnútroštátnej i medzinárodnej úrovni.

2 VŠEOBECNÉ NARIADENIE O OCHRANE OSOBNÝCH ÚDAJOV

Dňa 27.04.2016 Európsky parlament schválil znenie Všeobecného nariadenie o ochrane údajov, ktoré sa stane platným v 20-ty deň odo dňa jeho zverejnenia v Úradnom vestníku Európskej únie (dňa 04.05.2016 bolo zverejnené v Úradnom vestníku). Nariadenie sa začne uplatňovať 25.05.2018. Nariadenie nahrádza pôvodnú smernicu o ochrane osobných údajov č. 95/46/EHS ešte z roku 1995. Táto jednotná právna úprava na úrovni Európskej únie nahradí aktuálnu nejednotnú národnú úpravu členských štátov Únie. Toto nové nariadenie zabezpečí občanom väčšiu kontrolu nad ich súkromnými

[4] Smernica európskeho parlamentu a rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, L 119/89

[5] Cieľom Lisabonskej stratégie bolo urobiť z EÚ „najkonkurencieschopnejšiu a najdynamickejšiu znalostnú ekonomiku na svete, schopnú nepretržitého hospodárskeho rastu s väčším počtom lepších pracovných príležitostí a väčšou sociálnou súdržnosťou“.

[6] Európa 2020 – Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu (COM(2010)2020)

[7] „1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú. 2. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu. 3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.

informáciami vo svete plnom digitalizácie a smartfónov, sociálnych médií a sietí, internet bankingu a pod. Ako uviedol spravodajca Nariadenia Jan Philipp Albrecht (Zelení/EFA,DE): „Všeobecné nariadenie o ochrane údajov zreálňuje vysokú a jednotnú úroveň ochrany dát naprieč EÚ. Ide o veľký úspech Európskeho parlamentu a jednoznačné európske 'áno' silným právam spotrebiteľov a konkurencieschopnosti v digitálnom veku. Občania sa budú môcť sami rozhodnúť, o ktoré osobné informácie sa budú chcieť podeliť s ostatnými. Nariadenie tiež vytvorením jednotného právneho rámca v celej EÚ zabezpečí firmám jednoznačnú právnu zrozumiteľnosť. Nová legislatíva podporuje dôveru, právnu istotu a spravodlivejšiu konkurenciu."

Nariadenie je prioritne zamerané na posilnenie práv fyzických osôb na ochranu ich osobných údajov a na zníženie administratívnej záťaže spojenej s ich ochranou. Ďalším zo zámerov novej legislatívy je umožnenie voľného toku osobných údajov v priestore jednotného digitálneho trhu, čo má značne odbremeniť nadnárodné spoločnosti od administratívnej záťaže súvisiacej so zabezpečovaním súladu s právnymi poriadkami rôznych európskych štátov. Nariadenie má mať pozitívny dopad aj na zvýšenie právnej istoty spotrebiteľov a zlepšenie hospodárskej súťaže v Európskej únii. [8]

Cieľom nariadenia je zaručiť konzistentnú úroveň ochrany fyzických osôb v celej Únii a zabrániť rozdielom, ktoré sú prekážkou voľného pohybu osobných údajov v rámci vnútorného trhu. Nariadením sa poskytne právna istota a transparentnosť pre hospodárske subjekty vrátane malých a stredných podnikateľov. Nariadením sa tiež poskytne fyzickým osobám rovnaká úroveň ochrany práv vo všetkých členských štátoch a na druhej strane sa stanovia rovnocenné sankcie vo všetkých členských štátoch. Naopak nariadenie sa nevzťahuje na spracúvanie osobných údajov právnických osôb.

EÚ musí byť vybavená komplexným, súdržným, moderným a kvalitným rámcom, schopným účinne chrániť základné práva jednotlivcov, predovšetkým súkromie, v súvislosti s každým spracovaním osobných údajov jednotlivcov v rámci EÚ i mimo nej a za každých okolností, aby mohla riešiť početné problémy spojené s ochranou údajov, ako sú problémy spôsobené globalizáciou, technologickým rozvojom, nárastom činností uskutočňovaných na internete, používaním v súvislosti so stále väčším množstvom aktivít, ako aj otázky bezpečnosti (t. j. boj proti terorizmu). Zámerom Nariadenia je preto harmonizovať národné zákony na ochranu osobných údajov po celej EÚ za súčasného oslovenia nového technologického rozvoja bez potreby implementácie do národných poriadkov.[9]

2.1. Definícia osobných údajov

Osobné údaje sú definované v Nariadení ako akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Pod týmto termínom je možné rozumieť napríklad aj online identifikátor ako je IP adresa fyzickej osoby. Ide o rozširujúcu definíciu osobných údajov za účelom zabezpečenia ochrany akejkoľvek identifikovateľnosti fyzickej osoby.

Citlivé osobné údaje ako sú napr. spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby je možné spracovať len v prípade ak ide

[8] http://www.epravo.sk/top/clanky/reforma-ochrany-osobnych-udajov-v-eu-podstatne-ovplyvni-aj-slovensku-legislativu-3356.html, vzhliadnuté dňa 30.10.2016

[9] Hunton & Williams: EU General Data Protection Regulation. A guide for in-house lawyers. June 2015, str. 6, dostupné na https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf (30.10.2016)

o stanovenú výnimku v Nariadení. Jednou z výnimok je aj prípad ak dotknutá osoba tieto údaje preukázateľne zverejní (ako napr. na sociálnej sieti).

Spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby.

2.2. Princípy a zásady Nariadenia

Medzi zásady spracúvania osobných údajov patria: zákonnosť, spravodlivosť a transparentnosť; správnosť; obmedzenie účelu; minimalizácia uchovávania; minimalizácia údajov; integrita a dôvernosť.

Zásada transparentnosti si vyžaduje, aby všetky informácie určené verejnosti alebo dotknutej osobe boli stručné, ľahko prístupné a ľahko pochopiteľné, formulované jasne a jednoducho, a navyše ak je to vhodné, ľahko zrakovo vnímateľné. Takéto informácie by sa mohli poskytnúť v elektronickej podobe, napríklad pri oslovení verejnosti prostredníctvom webového sídla. Týka sa to najmä situácií, ako je napríklad online reklama, v ktorých veľký počet účastníkov a technologická zložitosť činnosti sťažujú dotknutej osobe zistiť a pochopiť, či osobné údaje, ktoré sa jej týkajú, boli získané, kým a na aké účely. Keďže deťom prislúcha osobitná ochrana, všetky informácie a každá komunikácia, pri ktorej sa spracúvanie zameriava na dieťa, by mali byť formulované jasne a jednoducho, aby ich dieťa mohlo ľahko pochopiť.

Zásady spravodlivého a transparentného spracúvania si vyžadujú, aby dotknutá osoba bola informovaná o existencii spracovateľskej operácie a jej účeloch. Prevádzkovateľ by mal dotknutej osobe poskytnúť všetky ďalšie informácie, ktoré sú potrebné na zaručenie spravodlivého a transparentného spracúvania, pričom sa zohľadnia konkrétne okolnosti a kontext, v ktorom sa osobné údaje spracúvajú. Dotknutá osoba by okrem toho mala byť informovaná o existencii profilovania a následkoch takéhoto profilovania. Ak sa osobné údaje získavajú od dotknutej osoby, dotknutá osoba by mala byť informovaná aj o tom, či je povinná osobné údaje poskytnúť, a o následkoch v prípade, že tieto údaje neposkytne. Tieto informácie možno poskytnúť v kombinácii so štandardizovanými ikonami s cieľom poskytnúť dobre viditeľným, zrozumiteľným a čitateľným spôsobom zmysluplný prehľad zamýšľaného spracúvania. Ak sú ikony uvedené v elektronickej podobe, mali by byť strojovo čitateľné.

Najdôležitejším prínosom Nariadenia je nová zásada zodpovednosti podľa ktorej je prevádzkovateľ zodpovedný za súlad so všetkými zásadami a tento súlad musí vedieť preukázať. Čiže dôkazné bremeno je prenesené na prevádzkovateľa.

2.3. Územná pôsobnosť Nariadenia:

Nariadenie sa vzťahuje na spracúvanie osobných údajov v rámci činnosti prevádzky prevádzkovateľa alebo sprostredkovateľa v Únii, a to bez ohľadu na to, či sa spracúvanie vykonáva v Únii alebo nie. Nariadenie sa teda vzťahuje na každého, kto spracúva osobné údaje na území Európskej únie, ale i mimo nej, ak spĺňa nariadením stanovené podmienky. Nariadenie sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Únii, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, pričom spracovateľská činnosť súvisí s ponukou tovaru alebo služieb bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie. Pre potreby naplnenia predchádzajúceho bodu je prevádzkovateľ alebo sprostredkovateľ povinný písomne určiť svojho zástupcu v Únii.

2.4. Práva jednotlivca podľa Nariadenia:

Právo byť informovaný zahŕňa povinnosť poskytovať "spravodlivé procesovanie informácií", typicky prostredníctvom oznámenia o ochrane osobných údajov. Zdôrazňuje potrebu transparentnosti nad tým, ako budete používať osobné údaje.

Právo prístupu k osobným údajom spočíva v práve získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a vymedzené informácie.

Právo na opravu osobných údajov ak sú tieto nesprávne alebo na doplnenie neúplných údajov.

Právo na vymazanie (tzv. právo na zabudnutie) je založené na princípe umožniť osobe požiadať o zmazanie a odstránenie osobných údajov a ta tam, kde neexistuje žiadny dôvod na ich ďalšie spracovanie. Každý môže požadovať, aby boli jeho osobné údaje vymazané pokiaľ osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo osoba nechce, aby boli tieto údaje ďalej spracúvané, odvolá svoj súhlas a nie je iný právny základ alebo legitímny dôvod na ich spracúvanie a uchovanie. V praxi to znamená napríklad, že ak niekto požiadal internetovú spoločnosť o vymazanie svojich osobných údajov, táto spoločnosť je povinná postúpiť túto požiadavku ďalším firmám, ktorým boli poskytnuté tieto osobné údaje. Toto právo je dlhodobo diskutované z hľadiska reálnej technologickej možnosti úplného vymazania osobných údajov. Nariadenia definuje povinnosť prevádzkovateľa *vymazať osobné údaje, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení podnikne primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.*

Právo na obmedzenie spracúvania je povinnosť obmedziť Ďalšie spracovanie dát, avšak nie je povinnosť vymazať existujúce dáta. Čiže prevádzkovateľ si môže ponechať také množstvo údajov aby sa ubezpečil, že obmedzenie spracúvanie do budúcna bude zabezpečené.

Právo na prenosnosť osobných údajov k inému poskytovateľovi služieb znamená, že: *„dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil*“[10] Dotknuté osoby majú mať možnosť vymeniť poskytovateľa služieb vrátane prenosu ich osobných údajov priamo od jedného prevádzkovateľa druhému prevádzkovateľovi, pokiaľ je to technicky možné a to bez straty údajov (napríklad kontaktov či predchádzajúcich e-mailov) a potreby ich opätovného zadávania.

Profilovanie je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom. Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú. Nové pravidlá, ktoré Nariadenie prináša, obmedzujú použitie profilovania bez predchádzajúceho súhlasu dotknutej osoby. Profilovaním nesmie dochádzať k diskriminácii osoby, ktorej údaje sú spracúvané a takisto profilovanie nesmie byť založené na údajoch, ktoré sú definované ako.

Právo vedieť o porušení ochrany osobných údajov. Dotknutá osoba má právo byť informovaná, že došlo k ohrozeniu bezpečnosti jej osobných údajov. Samotné oznámenie porušenia ochrany osobných údajov dozornému orgánu je upravené v článku 33 Nariadenia, ktorý uvádza

[10] článok 20 ods. 1 Všeobecného nariadenia o ochrane osobných údajov

v odsekoch 1 a 2: *„V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania. Sprostredkovateľ podá prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel.“*[11] Prevádzkovateľ zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu. Uvedená dokumentácia musí umožniť dozorným orgánom overiť súlad s týmto článkom.

Osobitná ochrana pre deti a podmienky týkajúce sa súhlasu dieťaťa sú upravené v čl. 8 ods. 1 Nariadenia: *„Ak sa uplatňuje článok 6 ods. 1 písm. a), v súvislosti s ponukou služieb informačnej spoločnosti adresovanou priamo dieťaťu je spracúvanie osobných údajov dieťaťa zákonné, len ak má dieťa aspoň 16 rokov. Ak má dieťa menej než 16 rokov, takéto spracúvanie je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil nositeľ rodičovských práv a povinností. Členské štáty môžu právnym predpisom stanoviť na tieto účely nižšiu vekovú hranicu za predpokladu, že takáto nižšia veková hranica nie je menej než 13 rokov.“* [12] Uvedené znamená, že deti pod určitou vekovou hranicou budú potrebovať súhlas rodiča alebo iného zákonného zástupcu, aby si mohli napríklad zriadiť účty na jednotlivých sociálnych sieťach ako Facebook, Instagram, pričom stanovenie vekovej hranice je ponechané vôli zákonodarcov členských štátov a to v rozmedzí veku dieťaťa od 13 do 16 rokov. Týmto spôsobom je zabezpečené, aby si štáty mohli nechať v platnosti súčasnú úpravu o súhlase zákonného zástupcu. Cieľom tejto úpravy je ochrana detí pred zdieľaním svojich osobných údajov bez uvedomovania si následkov takéhoto konania. Treba však podotknúť, že cieľom nie je obmedziť deťom prísun informácií, ktoré získavajú prostredníctvom internetu.

3. SMERNICA O OCHRANE OSOBNÝCH ÚDAJOV V OBLASTI JUSTÍCIE A SÚDNICTVA

Špecifická povaha policajných a súdnych činností vyžaduje špecifické pravidlá ochrany osobných údajov, aby bolo možné zabezpečiť voľné prúdenie údajov a spoluprácu medzi členskými štátmi v týchto oblastiach. Smernica sa zameriava na ochranu práv jednotlivcov na ochranu ich osobných údajov za súčasnej garancie vysokej úrovne verejnej bezpečnosti.

Cieľom smernice je nahradiť rámcové rozhodnutie o ochrane údajov 2008/977/SVV, ktoré v súčasnosti upravuje spracúvanie osobných údajov v oblasti policajnej a justičnej spolupráce v trestných veciach, avšak pre členské štáty z neho vyplýva povinnosť aplikovať určenú úroveň ochrany osobných údajov len v súvislosti s ich cezhraničnou výmenou.[13]

V porovnaní s rámcových rozhodnutím z roku 2008 prináša smernica komplexnú právnu úpravu, keďže sa má vzťahovať aj na ochranu osobných údajov pri ich spracúvaní na vnútroštátnej úrovni, čím by sa mala dosiahnuť minimalizácia rozdielov medzi jednotlivými úpravami a z toho vyplývajúca posilnená úroveň ochrany údajov.[14]

Smernica bola prijatá s cieľom zabezpečiť vysokú úroveň ochrany osobných údajov pri súčasnom zlepšení spolupráce v boji proti terorizmu a inej závažnej trestnej činnosti. Potom, čo Lisabonská zmluva nadobudla platnosť, ochrana fyzických osôb v súvislosti so spracovaním osobných údajov je výslovne uznaná ako základné právo. Článok 8 (1) Charty základných práv Európskej únie (ďalej len

11 článok 33 ods. 1 a 2 Všeobecného nariadenia o ochrane osobných údajov

12 článok 8 ods. 1 Všeobecného nariadenia o ochrane osobných údajov

13 Predbežné stanovisko Slovenskej republiky k Návrhu smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov.

14 Predbežné stanovisko Slovenskej republiky k Návrhu smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov.

"Charta") a článku 16 (1) Zmluvy o fungovaní Európskej únie (ZFEÚ) stanovuje, že každý má právo na ochranu osobné údaje, ktoré sa ho týkajú. Avšak vyhlásenie 21 pripojené k záverečnému aktu medzivládnej konferencie, ktorá prijala Lisabonskú zmluvu, uznáva, že špecifická povaha oblasti bezpečnosti zaslúžia osobitnú legislatívna úprava. Podľa prístupu európskych orgánov, spracovanie v radoch polície a trestného súdnictva kontexte treba odlíšiť od všetkých ostatných spracovaním osobných údajov. Európsky zákonodarca má na prvý pohľad rozlišovala medzi poľami výberom dva rôzne druhy právnych nástrojov (nariadenie a smernica). Ochrana a voľný pohyb údajov spracovaných príslušnými orgánmi na účely prevencie, vyšetrovania, odhaľovania a stíhania alebo výkonu trestov bola regulovaná smernicou, ktorý umožňuje členským štátom istú mieru flexibility a zároveň začlenením do svojich vnútroštátnych právnych predpisov, zatiaľ čo nariadenie bolo prijaté pre reguláciu všeobecné spracovanie osobných údajov. Týmto spôsobom by EÚ uznala proces dvojrýchlostný v snahe harmonizovať každé spracovanie osobných údajov v EÚ.

Jedným z hlavných rozdielov medzi všeobecným nariadením a smernicou o ochrane osobných údajov v oblastiach policajnej a justičnej (regulujúce ochranu dát v rámci pôsobnosti trestného práva) je v podstate práva na informácie a na prístupu k osobným údajom. Ak práva stanovené v nariadení sú vykonávané v čo najväčšej možnej miere v prípade trestného práva, to by zamedzilo vykonať vyšetrovanie trestných činov. To je dôvod, prečo musia byť uvedené v texte smernice osobitné ustanovenia týkajúce sa oblasti policajnej a justičnej. Smernica sa usiluje o vyváženie cieľov v oblasti ochrany údajov s cieľmi a bezpečnostnej politiky, zatiaľ čo určite prispeje k vytvoreniu menej roztriešteného všeobecného rámca.

Členské štáty v súlade s touto smernicou chránia základné práva a slobody fyzických osôb, najmä ich právo na ochranu osobných údajov, a zabezpečia, aby výmena osobných údajov medzi príslušnými orgánmi v rámci Únie, ak sa takáto výmena vyžaduje podľa práva Únie alebo práva členského štátu, nebola obmedzená ani zakázaná z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov.

Spracovanie osobných údajov podľa tejto smernice je prípustné len za účelom prevencie, vyšetrovania, odhaľovania či stíhania trestných činov alebo výkonu trestov, vrátane ochrany pred hrozbami pre verejnú bezpečnosť. V prípade, ak sú osobné údaje spracovávané pre iné účely, použije sa Všeobecné nariadenie o ochrane údajov. Smernica sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému. Zo smernice je vyňaté aj spracovanie osobných údajov uskutočňované pri výkone činností, ktoré nespadajú do oblasti pôsobnosti práva Únie (napr. činnosti týkajúce sa národnej bezpečnosti), ako aj spracovanie osobných údajov uskutočňované orgánmi, inštitúciami a inými subjektami Európskej únie.

Účelom smernice je zabezpečiť ochranu osobných údajov vo vzťahu k obetiam, svedkom, podozrivým osobám a obžalovaným v trestnom konaní. Jednotnou právnou úpravou na európskej úrovni dôjde k zjednodušeniu medzištátnej spolupráce orgánov činných v trestnom konaní a prokurátorov, čo zabezpečí efektívnejší a rýchlejší boj proti závažným formám zločinu a terorizmu v celej Európe. Smernica sa týka cezhraničných prenosov dát v rámci Európskej únie a sú ňou stanovené minimálne štandardy pre spracúvanie a výmenu údajov policajným a justičnými orgánmi

Členským štátom EÚ však je ponechané právo stanoviť si vo svojich národných právnych poriadkoch vyššiu mieru ochrany takto prenášaných údajov, čo hovorí aj článok 1 ods. 3 smernice a to, že táto smernica členským štátom nebráni, aby stanovili prísnejšie záruky, ako sú záruky stanovené v tejto smernici na ochranu práv a slobôd dotknutých osôb, pokiaľ ide o spracúvanie osobných údajov príslušnými orgánmi.

Dohľad má vykonávať národný orgán pre ochranu osobných údajov (na Slovensku je takýmto orgánom Úrad na ochranu osobných údajov), s dostatočnými právomocami na vynútenie plnenia

pravidiel. Policajné a justičné orgány sa v zásade budú riadiť rovnakými pravidlami ochrany osobných údajov ako tými, ktoré sú špecifikované Nariadením, avšak s potrebou úprav pre túto sféru.

Smernica nadobúda účinnosť dňom nasledujúcim po jej uverejnení v Úradnom vestníku Európskej únie. Členské štáty prijmú a uverejnia do 6. mája 2018 zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou.

4. PORUŠOVANIE PRÁV NA OCHRANU OSOBNÝCH ÚDAJOV

Porušovanie práv spojených s ochranou osobných údajov bude po zavedení opisovaného reformného balíka ťažšie. Reformný balík predstavuje jednotnú úpravu vo všetkých členských štátoch únie a preto bude potrebné túto právnu úpravu dodržiavať v celej EÚ a to aj prevádzkovateľmi, ktorý nemajú sídlo v rámci členských štátov EÚ. Sankcie za porušovanie práv sú stanovené jednotne a nebude možné vyhľadávať si priaznivejšiu jurisdikciu pre to ktoré porušenie. Reformný balík predstavuje garancie a záruky pre fyzické osoby a dodržiavanie ich práv na ochranu osobných údajov.

5. ZÁVER

Je nepochybné, že výzvy a nároky, ktoré sú kladené na ochranu údajov a súkromia jednotlivcov sa budú zvyšovať exponenciálne s ďalším vývojom technológií. Preto je potrebné si uvedomiť, že ako sa nezastaví vývoj digitalizácie a informatizácie spoločnosti, práca na zdokonaľovaní systémov ochrany dôstojnosti človeka tiež nebude dokončená. Reformný balík legislatívy EÚ, nie je ani zďaleka konečným cieľom. Prínosom reformy je najmä zharmonizovanie pravidiel a vytvorenie konzistentnej a efektívnej cesty k zakotveniu pevných štandardov ochrany údajov v Európe.

Možno konštatovať, že smernica je inovatívna v oblasti rozsahu a je teraz určená na pokrytie všetkých situácií spracovania osobných údajov vykonávaných v rámci policajnej a justičnej spolupráce v trestných veciach, bez ohľadu na to, či spracovanie prebieha vo vnútri alebo mimo štátnych hraníc. Trestné orgány preto už nebudú musieť používať rôzne súbory pravidiel ochrany údajov v závislosti na pôvode osobných údajov. Poskytuje smernica **o** ochrane osobných údajov dostatočný právny rámec pre ochranu osobných údajov v oblasti policajnej a justičnej spolupráce? Ako odpoveď na položenú otázku môžeme konštatovať, že smernica o ochrane údajov v sektoroch policajnej a justičnej neustanovuje všeobecný rámec ochrany údajov v rámci trestného práva z dôvodu povahy druh aktu - smernice - a smernica obsahuje len minimálne pravidlá pre harmonizáciu a ponechávajú široký priestor na voľnú úvahu členským štátom. Avšak jej prínos je citeľný.

Použitá literatúra:

1. COM(2012)11 final; legislatívne uznesenie Európskeho parlamentu z 12. marca 2014 k návrhu nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov), P7_TA(2014)0212; návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov) – Príprava všeobecného prístupu, dokument Rady 9565/15, 11.6.2015
2. Európa 2020 – Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu (COM(2010)2020)
3. Hunton & Williams: EU General Data Protection Regulation. A guide for in-house lawyers. June 2015
4. Nariadenie európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), L 119/1
5. Predbežné stanovisko Slovenskej republiky k Návrhu smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov.

6. Smernica európskeho parlamentu a rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, L 119/89
7. Spoločné vyhlásenia Európskeho parlamentu, Rady, Komisie, Spoločné vyhlásenie o praktických opatreniach pre spolurozhodovací postup (článok 251 Zmluvy o ES) (2007/C 145/02) (Ú. v. EÚ C 145, 30.6.2007).

Kontaktné údaje:
JUDr. Daniela Ježová, LL.M., PhD.
Daniela.jezova@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. 6
Bratislava
Slovenská republika

INTERNET AKO PRIESTOR PORUŠOVANIA PRAVIDIEL HOSPODÁRSKEJ SÚŤAŽE

Lucia Kasenčáková[1]

Protimonopolný úrad Slovenskej republiky, odbor kartelov

Abstract: The digital environment offers for undertakings new possibilities for marketing, searching and exchanging information and trading as well and can help business expansion. Despite the fact that the internet should, by its very nature, increase competitiveness, several cases of the competition authorities demonstrate that competition concerns may raise even in the digital environment. The article therefore deals with anti-competitive practices on the internet.

Abstrakt: Digitálny priestor otvára pre podnikateľov nové možnosti marketingu, vyhľadávania či zdieľania informácií a obchodovania a môže prispieť k rozširovaniu obchodného pôsobenia. Napriek skutočnosti, že internet by mal svojou podstatou stimulovať konkurenčné prostredie, viaceré prípady súťažných úradov demonštrujú, že aj v oblasti digitálneho priestoru sa môžu vyskytnúť súťažné obavy. Príspevok sa preto sústredí na protisúťažné praktiky na internete.

Key words: internet, breach of the competition rules, digital single market**,** e-commerce

Kľúčové slová: internet, porušenie súťažných pravidiel, jednotný digitálny trh, elektronický obchod

3 ÚVOD

Internet čoraz častejšie využívajú spotrebitelia na nákup tovarov a služieb, no cezhraničný elektronický obchod v Európskej únii rastie veľmi pomaly. V roku 2014 využívala online nakupovanie približne polovica všetkých spotrebiteľov členských štátov, no iba 15% z tejto skupiny nakúpilo tovary a služby od predajcu so sídlom v inom členskom štáte ako v štáte predajcu. Na túto skutočnosť upriamila pozornosť európska komisárka zodpovedná za politiku hospodárskej súťaže, Margrethe Vestager, na konferencii v Berlíne ešte v marci roku 2015.[2] V tejto súvislosti oznámila aj návrh Európskej komisie (ďalej len „Komisie“) zrealizovať sektorovú štúdiu, cieľom ktorej by bolo zistiť úroveň hospodárskej súťaže v oblasti elektronického obchodu, pochopiť a odstrániť prekážky pre elektronický obchod v prospech európskych občanov a podnikateľov, a to v súlade s prioritami Komisie na vytvorení jednotného digitálneho trhu.[3]

Čo je vlastne brzdou dynamickejšieho vývoja cezhraničného elektronického obchodu? Bezpochyby už teraz možno povedať, že niektoré dôvody vystupujúce ako brzda vývoja cezhraničného elektronického obchodu sú legitímne, ako napr. jazyková bariéra spotrebiteľov, či ich preferencie, rozdiely v právnych predpisoch a technických normách členských štátov. Na druhej strane prax viacerých súťažných úradov naznačuje, že existujú obavy, že niektorí podnikatelia cielene prijímajú prekážky cezhraničného elektronického obchodu s cieľom segmentovať trh podľa vnútroštátnych hraníc a zabrániť tak vstupu na trh konkurenčným podnikateľom. Využívanie internetu

[1] Komentáre a názory uvedené v tomto príspevku sú osobnými názormi autorky a nevyjadrujú oficiálny postoj Protimonopolného úradu Slovenskej republiky.

[2] European Commission – Press release: Competition: Commissioner Vestager announces proposal for e-commerce sector inquiry (26.03.2015). Dostupné na: http://europa.eu/rapid/press-release_IP-15-4701_en.htm

[3] Bližšie informácie k stratégii jednotného digitálneho trhu pozri: http://ec.europa.eu/priorities/digital-single-market/

má totiž v súčasnom digitálnom svete kľúčový význam pre podnikanie, rozširovanie obchodného pôsobenia a samotnú obchodnú stratégiu spoločností.

Hoci predbežná správa o výsledkoch tejto sektorovej štúdie je už dostupná na stránke Komisie,[4] to, či výsledky prieskumu pomôžu naplniť cieľ Komisie, sa dozvieme až v záverečnej správe, ktorá by mala byť zverejnená v prvom štvrťroku 2017. Zatiaľ si však môžeme zhrnúť to, čo o porušovaní pravidiel hospodárskej súťaže v digitálnom priestore vieme doposiaľ.

4 POZITÍVNE ASPEKTY ELEKTRONICKÉHO OBCHODU

Bezpochyby najvýraznejším pozitívnym prínosom využívania online nakupovania je skutočnosť, že pre spotrebiteľa sa otvárajú široké možnosti výberu tovaru a služieb. Vďaka internetu dokáže spotrebiteľ nakupovať tovar od rôznych predajcov, pričom internet mu umožňuje jednoducho porovnávať jednotlivé súťažné parametre, ako cenu, kvalitu tovaru a služieb, či v pohodlí domova sa oboznámiť s obchodnými podmienkami jednotlivých predajcov. Následne si spotrebiteľ takto dokáže vybrať taký produkt, ktorý najviac vyhovuje jeho preferenciám a potrebám. Jednoduché vyhľadávanie údajov na internete a dostupnosť rôznych online platforiem, ktoré dokonca umožňujú realizovať porovnanie cien za spotrebiteľa, mu výber tovarov a služieb ešte uľahčujú a dokonca vytvárajú priestor na zvýšenú transparentnosť cien. Cenová transparentnosť pritom stupňuje cenovú konkurenciu, čo je v prospech spotrebiteľov.

Rovnako aj na strane predajcov možno pozorovať viaceré pozitívne aspekty využívania internetu v rámci podnikateľskej činnosti. Predajcom sa využívaním internetu naskytli nové možnosti pre rozširovanie svojho obchodného pôsobenia. Internetový priestor im totiž umožňuje získať zákazníkov aj v oblastiach, kde sa predtým nenachádzalo pole ich pôsobenia. Využívanie informačno-komunikačných technológií všeobecne podporuje rozvoj inovácií. Okrem toho, kumulácia a vyhodnocovanie dát spotrebiteľov (rôzne údaje získané na základe registrácie, z IP adries a podobne) podnikateľom umožňuje dosiahnuť cielenejší marketing.

5 SÚŤAŽNÉ OBAVY ELEKTRONICKÉHO OBCHODU

Každá minca má dve strany, a preto je pochopiteľné, že s rozvojom elektronického obchodu sa spája aj výskyt nových praktík, ktoré poškodzujú jeho užívateľov, či už spotrebiteľov alebo predajcov.

Internetový priestor si preto vyslúžil zvýšenú pozornosť aj zo strany súťažných autorít, ktoré skúmajú tie obchodné praktiky, ktoré sú spôsobilé obmedziť hospodársku súťaž.[5] Cieľom týchto praktík je zväčša potlačiť základné výhody online nakupovania - väčší výber a nižšie ceny tovarov a služieb, ako aj brzdiť inovácie a vstup konkurentov na trh.

5.1 Obmedzenie predaja na internete

Internet v porovnaní s tradičnými metódami predaja umožňuje osloviť širšie spektrum zákazníkov a nárast online obchodovania vedie k cenovej transparentnosti, ktorá následne vyúsťuje do cenovej konkurencie - často aj v rámci vlastnej distribučnej siete. Cenová vojna je však pre mnohých podnikateľov nechceným javom, a preto niet divu, že jednými z najbežnejších obmedzení

[4] European Commission – Press release: Antitrust: Commission publishes initial findings of e-commerce sector inquiry (15.09.2016). Dostupné na: http://europa.eu/rapid/press-release_IP-16-3017_en.htm

[5] Bohatú rozhodovaciu prax, ako aj súťažnú advokáciu, možno vidieť predovšetkým v činnosti britského súťažného úradu (Competition and Markets Authority), nemeckého súťažného úradu (Bundeskartellamt) a francúzskeho súťažného úradu (Autorité de la concurrence).

hospodárskej súťaže na internete sú práve vertikálne obmedzenia, cieľom alebo následkom ktorých je obmedziť distribútorov v predaji na internete.[6]

Tak ako bežný spotrebiteľ prostredníctvom internetu dokáže nájsť najnižšiu cenu určitého produktu, internet umožňuje aj dodávateľom efektívnejšie kontrolovať svoju distribučnú sieť, postavenie svojich značiek, či dodržiavanie zmluvných obmedzení predaja zakotvených v dohodách o distribúcii s odberateľmi.

Vo všeobecnosti síce platí, že možnosť využívania internetu ako distribučného nástroja na predaj produktov by mal mať každý predajca, avšak prax súťažných úradov demonštruje, že distribútori sa stretávajú s viacerými obmedzeniami týkajúcich sa predaja produktov na internete. Medzi tie najčastejšie patria:

- cenové odporúčania, na rešpektovaní ktorých dodávateľ trvá a ich dodržiavanie vynucuje alebo cenové obmedzenia spočívajúce v stanovení minimálnych cien od dodávateľov,
- zákaz predaja na internete,
- zákaz reklamy na internete,
- územné obmedzenia alebo obmedzenia okruhu zákazníkov,
- obmedzenia využívať online platformy,
- iné zmluvné obmedzenia predaja.

5.1.1 Cenové obmedzenia

Je to iba niekoľko mesiacov, čo britský súťažný úrad udelil pokutu v celkovej výške 3 milióny libier na trhu chladiacich zariadení (2 milióny libier)[7] a na trhu kúpeľňových armatúr (780 000 libier)[8] za obmedzenie cenovej súťaže na internete. Podstatou oboch prípadov bolo **obmedziť odberateľov v určovaní si vlastných cien na internete** (*tzv. RPM – resale price maintenance*).[9]

V prípade chladiacich zariadení dodávateľ nielenže určil minimálne ceny, za akých môže byť produkt propagovaný na internete, ale dodržiavanie tohto záväzku si dodávateľ voči „neposlušným" distribútorom aj vynucoval, a to zvýšením cien odoberaného produktu, resp. zastavením dodávok produktu. Z emailovej komunikácie medzi odberateľmi a dodávateľom pritom jasne vyplývalo, že dodávateľ sa o porušení jednoducho dozvedel uskutočnením kontroly na internete. V prípade

---

6 Dojednania, ktoré existujú medzi dvoma alebo viacerými podnikateľmi, z ktorých každý podniká, na účely dohody alebo zosúladeného postupu na inej úrovni výrobného alebo distribučného reťazca a ktoré sa týkajú podmienok, za ktorých môžu strany nakupovať, predávať alebo ďalej predávať určitý tovar alebo služby (medzi dodávateľmi a odberateľmi) označujeme ako vertikálne obmedzenia. V tejto súvislosti pozri Oznámenie Komisie: Usmernenie o vertikálnych obmedzeniach (2010/C 130/01). Dostupné na: http://www.antimon.gov.sk/data/files/66_ok-uvo.pdf. Bližšie informácie k cieľovým vertikálnym dohodám pozri v dokumente vypracovanom Protimonopolným úradom SR – Cieľové vertikálne dohody, dostupnom na: http://www.antimon.gov.sk/data/files/422_cielove-vertikalne-dohody-pohlad-pmu-sr.pdf

7 História prípadu (vrátane rozhodnutia) dostupná na webovej stránke britského súťažného úradu: https://www.gov.uk/cma-cases/commercial-catering-sector-investigation-into-anti-competitive-practices

8 História prípadu (vrátane rozhodnutia) dostupná na webovej stránke britského súťažného úradu: https://www.gov.uk/cma-cases/bathroom-fittings-sector-investigation-into-anti-competitive-practices

9 RPM je definované ako obmedzenie možnosti kupujúceho stanoviť svoju predajnú cenu, bez toho, aby bola dotknutá možnosť dodávateľa uložiť maximálnu predajnú cenu alebo odporúčať predajnú cenu pod podmienkou, že nepredstavujú pevne stanovenú alebo minimálnu predajnú cenu v dôsledku tlaku ktorejkoľvek zo strán alebo v dôsledku nimi poskytnutých stimulov. RPM sa prakticky vyskytuje v dvoch základných formách – minimálne RPM (je určená minimálna cena ďalšieho predaja) a fixné RPM (je určená pevná cena ďalšieho predaja), pričom pod RPM spadajú aj „nepriame" spôsoby fixácie cien – fixácia distribučnej marže, fixovanie maximálnej úrovne zľavy, ktorú môže distribútor dať konečnému zákazníkovi, poskytnutie rabatov alebo úhrada reklamných nákladov distribútorovi.

kúpeľňových armatúr si dodávateľ rovnako vynucoval dodržiavanie pravidiel, a to zvýšením cien odoberaného produktu, ale aj zákazom využívať dodávateľove logo na internete a zastavením dodávok.

Už v minulosti pritom britský súťažný úrad viackrát pristúpil k sankcionovaniu RPM praktík na internete, a to nielen výrobcov, ale i distribučnej siete.[10] V roku 2016 však britský súťažný úrad, s cieľom rozšíriť povedomie o RPM praktikách a zvýšiť mieru dodržiavania súťažných pravidiel, siahol aj po nástroji súťažnej advokácie. V stručnom liste na troch stranách, ktorý bol určený tak dodávateľom, ako aj odberateľom, preto informoval o posledných dvoch RPM prípadoch (na trhu chladiacich zariadení a na trhu kúpeľňových armatúr), o tom, čo je to RPM, aké obchodné praktiky nemôže dodávateľ prijímať v súvislosti s cenovou politikou svojej distribučnej siete, ako aj to, kde možno nájsť užitočné informácie ohľadom RPM. Zároveň odberateľov upozornil na to, že za cenové obmedzenia môže byť pokutovaný nielen dodávateľ, ale aj jeho odberatelia.[11]

Netreba pritom zabudnúť na to, že súťažné úrady v rámci svojej rozhodovacej činnosti opakovane potvrdzujú, že vertikálne cenové obmedzenia sa považujú za jedny z najzávažnejších protisúťažných praktík *(hard-core restriction).*

5.1.2 Zákaz predaja na internete

Podnikatelia využívajúci tradičné spôsoby predaja prostredníctvom kamenného obchodu čelia z dôvodu expandujúceho elektronického obchodovania intenzívnej cenovej súťaži zo strany online predajcov. Online predaj totiž umožňuje znižovať náklady súvisiace s klasickým predajom v kamenných obchodoch (ako nájom, náklady súvisiace s činnosťou predajní a personálnym zabezpečením predajní) a zároveň umožňuje osloviť širšie spektrum potenciálnych klientov.

Najradikálnejším spôsobom, akým dodávatelia reagujú na rastúci online obchod, je úplný zákaz predaja produktov na internete. Takúto protisúťažnú praktiku demonštruje napr. britský prípad golfových loptičiek,[12] kde výrobca bránil distribútorom v predaji golfových loptičiek cez internet.

V praxi súťažných úradov sa stretávame s mnohými rozhodnutiami, kedy boli zákaz predaja na internete považovaný za cieľovú vertikálnu dohodu obmedzujúcu hospodársku súťaž,[13] pritom takýto prístup bol potvrdený aj Súdnym dvorom EÚ (ďalej len „SD EÚ“).[14] Predmetný zákaz vychádza z premisy, že ak distribútor nakúpil tovar od svojho dodávateľa, mal by na základe vlastného, od

---

[10] Napr. prípad dodávky zdravotníckych pomôcok (pojazdných skútrov) *Pride Mobility Products Limited.* Zaujímavosťou tohoto prípadu je, že cenové obmedzenia neboli súčasťou distribučných zmlúv, ale boli rozposielané distribútorom v rámci obežníkov. História prípadu (vrátane rozhodnutia) je dostupná na webovej stránke britského súťažného úradu: https://www.gov.uk/cma-cases/investigation-into-agreements-in-the-mobility-aids-sector

[11] Otvorený list je dostupný na webovej stránke britského súťažného úradu: https://www.gov.uk/government/publications/restricting-online-resale-prices-cma-letter-to-suppliers-and-retailers

[12] História prípadu (vrátane rozhodnutia) je dostupná na webovej stránke britského súťažného úradu: https://www.gov.uk/government/news/cma-alleges-breach-of-competition-law-by-ping

[13] Jeden z najznámejších prípadov je prešetrovanie francúzskeho súťažného úradu ukončené rozhodnutím č. 12-D-13 zo dňa 12. decembra 2012 vo veci *Bang & Olufsen.* Rozhodnutie, ako aj tlačová správa, je dostupné na webovej stránke francúzskeho súťažného úradu: http://www.autoritedelaconcurrence.fr/user/avisdec.php?numero=12D23

[14] Rozsudok SD EÚ zo dňa 13.10.2011 vo veci C439/09 *Pierre Fabre Dermo-Cosmétique SAS v. Komisia,* Zb. [2011], s. I-09419, ECLI:EU:C:2011:649: *„Zákaz používať pri takomto predaji internet, predstavuje obmedzenie hospodárskej súťaže na základe cieľa, ak z individuálneho a konkrétneho preskúmania obsahu a cieľa tejto zmluvnej podmienky, ako aj z hospodárskeho a právneho kontextu, do ktorého toto obmedzenie spadá, vyplýva, že vzhľadom na vlastnosti dotknutého výrobku táto podmienka nie je objektívne odôvodnená.“*

dodávateľa nezávislého, rozhodnutia rozhodovať o tom, kde a komu bude ďalej tento tovar ponúkať. Vertikálne obmedzenie spočívajúce v zákaze využívať internet ako distribučný kanál nielenže obmedzuje podnikateľov v možnosti získať nových zákazníkov, ale obmedzuje aj samotných zákazníkov na online nakupovanie.

5.1.3 Územné obmedzenia alebo obmedzenia okruhu zákazníkov

Ďalším nemenej častým vertikálnym obmedzením predaja na internete je **tzv. územné obmedzenie alebo obmedzenie okruhu zákazníkov.**

V tejto súvislosti je nutné podotknúť, že na jednej strane je legitímne, ak sa rozhodne dodávateľ vytvoriť si exkluzívnu distribučnú sieť, kde obmedzí aktívne predaje[15] do oblastí, ktoré boli exkluzívne pridelené iným distribútorom, resp. pre určitú skupinu zákazníkov pridelenú výhradne inému distribútorovi, ale to len za predpokladu, že dodávateľ a distribútor nemajú trhový podiel vyšší ako 30% *(tzv. safe harbour).*

Na druhej strane je striktne zakázané obmedzovať tzv. pasívne predaje.[16] Dodávateľ by teda nemal brániť distribútorom na určitom území v tom, aby predávali tovar zákazníkovi z iného územia, ak zákazník bol ten, ktorý iniciatívne oslovil distribútora. Rovnako by nemal obmedzovať ani všeobecnú reklamu alebo reklamu, ktorá oslovuje zákazníkov vo výhradných územiach iných distribútorov alebo skupiny zákazníkov výhradne pridelených iným distribútorom, ak takáto reklama primerane oslovuje zákazníkov aj mimo týchto území alebo mimo týchto skupín zákazníkov.

Vyššie uvedené znamená, že ak zákazník z určitej oblasti osloví distribútora z inej výhradnej oblasti za účelom dodania tovaru alebo služieb, distribútor nemôže odmietnuť dodanie produktu, alebo odovzdať objednávku automaticky inému distribútorovi iba z dôvodu, že dané územie nepatrí do jeho územnej pôsobnosti. Tento prístup je odôvodnený tým, že online nakupovanie je vnímané ako spôsob pasívneho predaja, keďže zákazník potrebuje prejaviť určitú iniciatívu vo vyhľadaní si predajcu a jeho následnom kontaktovaní.

Za najčastejšie prípady obmedzenia pasívnych predajov na internete sa preto považujú situácie, ak (výhradný) distribútor zamedzí zákazníkom nachádzajúcim sa na inom (výhradnom) území prezeranie jeho webovej stránky alebo ak distribútor automaticky presmeruje zákazníkov na webové stránky výrobcu alebo iného (výhradného) distribútora.[17] Rovnako za protisúťažné možno považovať situácie, kedy (výhradný) distribútor ukončí transakcie cez internet so zákazníkmi, akonáhle podľa údajov na kreditnej karte zistí, že príslušná adresa nepatrí do (výhradného) územia distribútora. Medzi zakázané praktiky patrí aj obmedzenie, ak distribútor obmedzí podiel celkového predaja uskutočneného cez internet; to dodávateľovi nebráni požadovať, a to bez toho, aby obmedzil online predaj distribútora, aby kupujúci predal aspoň určité absolútne množstvo (vyjadrené ako hodnota alebo objem) výrobku offline na zabezpečenie efektívneho fungovania svojho kamenného obchodu, a zároveň to dodávateľovi nebráni, aby sa ubezpečil, že online činnosť distribútora je v

---

15 „Aktívny“ predaj znamená aktívny prístup k jednotlivým zákazníkom, napr. prostredníctvom priamej poštovej reklamy vrátane posielania nevyžiadaných e-mailov alebo návštev, alebo aktívny prístup k určitej skupine zákazníkov alebo zákazníkom na určitom území prostredníctvom reklamy v médiách či na internete alebo inej reklamy konkrétne zameranej na túto skupinu zákazníkov alebo zákazníkov na tomto území. V tejto súvislosti pozri Oznámenie Komisie: Usmernenie o vertikálnych obmedzeniach (2010/C 130/01). Dostupné na: http://www.antimon.gov.sk/data/files/66_ok-uvo.pdf.

16 „Pasívny“ predaj znamená reagovanie na nevyžiadané požiadavky jednotlivých zákazníkov vrátane dodávky tovaru alebo služieb týmto zákazníkom. (Usmernenia o vertikálnych obmedzeniach EK, 2010). V tejto súvislosti pozri Oznámenie Komisie: Usmernenie o vertikálnych obmedzeniach (2010/C 130/01). Dostupné na: http://www.antimon.gov.sk/data/files/66_ok-uvo.pdf.

17 Naopak je legitímne, ak sa na webových stránkach distribútora nachádzajú odkazy na webové stránky iných distribútorov alebo na webovú stránku dodávateľa,

súlade s distribučným modelom dodávateľa.[18] V neposlednom rade rovnako, ak distribútor zaplatí vyššiu cenu za výrobky určené na ďalší predaj distribútorom online než za výrobky, ktoré sa majú ďalej predávať off-line, ide o protisúťažné správanie.[19]

5.1.4 Iné obmedzenia predaja na internete

Okrem už spomenutých bežných spôsobov obmedzenia hospodárskej súťaže sa súťažné úrady stretávajú aj s novými obchodnými praktikami s cieľom alebo následkom obmedzenia hospodárskej súťaže. Nové obchodné praktiky pritom súvisia predovšetkým s rozvojom nových inovatívnych spôsobov obchodovania a oslovovania zákazníkov.

Môžeme tu zaradiť napr. vertikálne obmedzenia spočívajúce v zákaze reklamy na internete, v zákaze využívania porovnávacích cenových nástrojov na internete, v zákaze využívať online platformy, v zákaze využívať obchodné meno, resp. značku výrobcu ako kľúčové slovo v internetových vyhľadávacích nástrojoch a iné (potenciálne) protisúťažné praktiky.

Na demonštráciu uvedených obmedzení možno poukázať na prípady nemeckého súťažného úradu, ktorý sa z dôvodu svojej prioritizačnej politiky aktívne venuje práve obmedzeniam online obchodu.

V prípade *Scout* nemecký súťažný úrad pokutoval výrobcu za prijatie zmluvného obmedzenia, na základe ktorého výrobca odmietol dodávať produkty tým predajcom, ktorí využívali online platformu eBay. Protisúťažnosť tohto správania bola potvrdená aj odvolacím súdom. V prípade *adidas* posudzoval nemecký súťažný úrad viaceré zmluvné obmedzenia, medzi ktoré patrilo, okrem obmedzenia využívať online platformy, aj obmedzenie využívať označenia týkajúce sa značky „adidas“ ako kľúčové slová vo vyhľadávacích nástrojoch za účelom propagácie svojej vlastnej predajne.[20] Rovnako prípad *Asics* je odzrkadlením toho, že výrobcovia prijímajú viaceré zmluvné obmedzenia týkajúce sa online obchodu, ako napr. zákaz využívať obchodné meno ako kľúčové slovo vo vyhľadávacích nástrojoch, ale aj zákaz využívania porovnávacích cenových nástrojov či zákaz reklamy a predaja cez online platformy.[21]

Kým v niektorých prípadoch boli prešetrovania ukončené po tom, čo výrobcovia súhlasili s odstránením sporných protisúťažných obmedzení, niektoré prípady boli ukončené deklarovaním protisúťažného správania aj po tom, čo výrobca upustil od protisúťažných zmluvných obmedzení.[22] Rovnako ani rozhodovacia činnosť národných súdov nepriniesla viac svetla do posudzovania týchto vertikálnych obmedzení, nakoľko napr. v prípade *Deuter* frankfurtský odvolací súd konštatoval, že zákaz využívania online platforiem je v súlade so súťažným právom, keďže išlo o ochranu značky,[23]

---

18 Toto absolútne množstvo požadovaných off-line predajov môže byť rovnaké pre všetkých kupujúcich alebo určené individuálne pre každého kupujúceho na základe objektívnych kritérií, ako je napríklad veľkosť kupujúceho v sieti alebo jeho geografická poloha.

19 Týmto sa nevylučuje dohoda medzi dodávateľom a kupujúcim o pevne stanovenom poplatku na podporu off-line alebo on-line predaja uskutočňovaného kupujúcim (t. j. nejde o variabilný poplatok, ktorého suma narastá v závislosti od realizovaného obratu z off-line predaja, pretože by to nepriamo viedlo k dvojitým cenám).

20 Tlačová správa je dostupná na webovej stránke nemeckého súťažného úradu: http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2014/02_07_2014_adidas.html?nn=3591568

21 Tlačová správa je dostupná na webovej stránke nemeckého súťažného úradu: http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2014/28_04_2014_Asics.html?nn=3591568

22 Napr. prípad *Asics*, kde nemecký súťažný úrad aj po súhlase s odstránením protisúťažných obmedzení vydal rozhodnutie o porušení súťažných pravidiel.

23 Na druhej strane frankfurtský odvolací súd potvrdil, že zákaz využívania cenových porovnávacích nástrojov je protisúťažným správaním.

kým francúzsky odvolací súd v prípade *Caudalie* zákaz využívania online platformy považoval za *hard-core* obmedzenie hospodárskej súťaže.[24]

O to zaujímavejšie bude sledovať vývoj nemeckého prípadu *Coty*, kde výrobca parfumov obmedzoval svojich distribútorov vo využívaní online platforiem eBay a Amazon, a to vzhľadom na to, že frankfurtský súd v rámci odvolacieho súdneho konania položil prejudiciálnu otázku SD EÚ s cieľom zistiť, či môže ísť o aspekt hospodárskej súťaže zlučiteľný s článkom 101 ods. 1 Zmluvy o fungovaní EÚ, keď sa členom selektívneho distribučného systému pôsobiacim na maloobchodnej úrovni paušálne zakazuje, aby do predaja prostredníctvom internetu zapojili tretie spoločnosti identifikovateľné navonok bez ohľadu na to, či sa v konkrétnom prípade porušujú legitímne požiadavky výrobcu na kvalitu. Okrem toho, sa nemecký súd zaujíma aj to, či zákaz zapájať do predaja prostredníctvom internetu tretie spoločnosti, ktorý sa uložil členom selektívneho distribučného systému pôsobiacim na maloobchodnej úrovni, predstavuje obmedzenie okruhu zákazníkov maloobchodníka na základe cieľa alebo či ide o obmedzenie pasívnych predajov.[25]

V prípadoch vyššie uvedených zmluvných obmedzení by preto mali súťažné úrady postupovať s náležitosťou starostlivosťou a nezabudnúť vyhodnotiť aj to, či takéto obmedzenia nemôžu predstavovať kvalitatívne kritérium výrobcu na ochranu kvality distribučnej siete, ktoré môže mať legitímny podklad.

5.2 Geo-blocking

V súčasnosti sa pozornosť Komisie, ako aj národných súťažných úradov, obracia k problematike geografického blokovania, ktorého podstata spočíva v tom, že sa na základe určitých osobných údajov bráni zákazníkom k prístupu na niektoré webové lokality *(geo-blocking).* Geografické blokovanie prístupu pritom nepochybne vedie k fragmentácii jednotného digitálneho trhu, otázkou však je, či ho možno považovať za protisúťažnú praktiku a ak áno, tak kedy.

Geo-blocking sa môže vyskytovať vo viacerých podobách, a to (a) vo forme odmietnutia predávať do iného členského štátu; (b) automatického presmerovania zákazníka na webovú stránku inej krajiny (často na webovú stránku podľa bydliska zákazníka) bez súhlasu a vedomia zákazníka a bez možnosti vylúčiť takéto presmerovanie; (c) zmenou cenových a obchodných podmienok podľa krajiny, kde má zákazník bydlisko. Všetky tieto formy geografického blokovania využívajú geografickú identifikáciu zákazníka pomocou IP adresy, informácií získaných z prehliadačov, operačných systémov, na základe nevyhnutnej registrácie zákazníka, resp. neumožnením registrácie zákazníka alebo vyplnením osobných údajov (ako bydlisko) do objednávkového formulára, prípadne zadaním mobilného čísla alebo údajov kreditnej karty. Podnikatelia pritom buď priamo blokujú prístup k svojim stránkam zo zahraničia alebo možnosť vyzdvihnúť si, dodať alebo odoslať tovar do zahraničia.

Vzhľadom na vyššie uvedené spôsoby realizácie geo-blockingu je zrejmé, že geo-blocking nápadne pripomína vertikálne obmedzenie pasívnych predajov na internete. Z prieskumu uskutočneného Komisiou[26] však vyplýva, že za geografickým obmedzením prístupu sa v určitých

---

[24] Caudalie vo svojej argumentácii tvrdil, že online platforma www.1001pharmacies.com nie je schváleným distribútorom a zároveň tvrdil, že iba schválená distribučná sieť môže využívať iba svoje vlastné webové stránky na online predaj, no nie iné internetové distribučné kanály. Rozhodnutie francúzskeho súťažného úradu č. 07-D-07 zo dňa 8. marca 2007 vo veci *Caudalie* je dostupné na webovej stránke francúzskeho súťažného úradu:
http://www.autoritedelaconcurrence.fr/user/avisdec.php?numero=07D07

[25] Návrh na začatie prejudiciálneho konania vo veci C-230/2016 (Coty Germany). Francúzsky súd v prípade *Coty* už v minulosti potvrdil, že obdobné zmluvné obmedzenia sú *hard-core* obmedzeniami hospodárskej súťaže.

[26] Mystery shopping survey on territorial restrictions and geo-blocking in the European digital single market (marec 2016). Dostupné na:
http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/geoblocking-exec-summary_en.pdf

prípadoch skrýva predovšetkým právo jednotlivých podnikateľov slobodne sa rozhodnúť, aký bude rozsah ich geografického pôsobenia, pričom podnikatelia by nemali byť nútení k tomu, aby rozšírili svoju obchodnú aktivitu aj na trhy, kde predtým nepôsobili. Okrem toho, v prieskume sa uvádzajú aj iné legitímne dôvody, ako neprimerané dodacie náklady spojené s predajom do iného členského štátu, nutnosť využívania špecifických formátov jednotlivých krajín (pre adresy, smerovacie čísla, telefónne/mobilné čísla), rozdielne pravidlá o DPH a iné odlišnosti v národných právnych úpravách.

Ak je geo-blocking výsledkom nezávislej obchodnej stratégie podnikateľa nemožno ho považovať za obmedzenie hospodárskej súťaže. Ak však bude geografické blokovanie prístupu výsledkom zmluvných obmedzení medzi dodávateľom a jeho distribučnou sieťou, prípadne výsledkom kartelovej dohody medzi konkurentmi, bude nutné takéto blokovanie preskúmať a v prípade zistenia protisúťažného správania pristúpiť k riešeniu, či už vo forme správneho konania a následného rozhodnutia o porušení súťažných pravidiel alebo v rámci súťažnej advokácie.

Sektorová štúdia Komisie totiž odhalila, že geografické blokovanie využíva 38% maloobchodníkov, pričom 12% z nich uvádza, že je výsledkom zmluvného obmedzenia určeného v distribučnej zmluve s dodávateľom.[27] V prípade digitálneho obsahu dostupného online je toto číslo ešte väčšie, keďže až 68% poskytovateľov uviedlo, že geograficky blokujú používateľov, ak sa nachádzajú v inom členskom štáte, pričom až 59% z nich uviedlo, že k takémuto blokovaniu ich zmluvne zaväzujú dodávatelia.

5.3 Online platformy

Či už ide o rôzne internetové vyhľadávače, sociálne médiá, aplikácie, internetové stránky zamerané na porovnávanie cien, online platformy[28] sa stávajú predmetom posudzovania tak zo strany regulačných orgánov, ako aj zo strany súťažných úradov, a to nie len pokiaľ ide o vertikálne obmedzenie zakazujúce ich využívanie v rámci distribučnej siete.

Napriek tomu, že cieľom online platforiem je predovšetkým prepojiť predávajúcich s kupujúcimi, aj tu dochádza k výskytu určitých súťažných obáv. Najčastejšie súťažné obavy týkajúce sa online platforiem pramenia z využívania trhovej sily prevádzkovateľom týchto platforiem, a preto je problematika online platforiem často prepojená s protisúťažnou praktikou spočívajúcou v zneužívaní dominantného postavenia, ktorá sa nemusí prejaviť iba na relevantnom trhu prevádzkovateľa, ale aj na susedných trhoch. Protisúťažné prejavy tejto praktiky sa pritom môžu vyskytovať v rôznych podobách.

Jednou z týchto podôb je napr. uzavretie dodávateľov v online platforme alebo iné potláčanie hospodárskej súťaže medzi online platformami. Tento výsledok dosiahnu prevádzkovatelia online platforiem rôznymi zmluvnými obmedzeniami obsiahnutými v zmluvách so svojimi zákazníkmi (napr. s dodávateľmi produktov predávaných cez online platformu).

---

[27] Ide o maloobchodníkov, ktorí sa zúčastnili na prieskume a ktoré sa venujú online predaju spotrebného tovaru ako oblečenie, obuv, športové potreby či spotrebná elektronika.

[28] Online platforma predstavuje dvojstranné alebo viacstranné trhy, kde sa stretávajú užívatelia a prevádzkovatelia platformy s cieľom uľahčiť vzájomnú interakciu, ako napr. výmenu informácií alebo obchodnú transakciu. Medzi užívateľov pritom môžu patriť rôzne skupiny od odberateľov, predajcov, inzerentov, vývojárov softvéru a podobne. Medzi online platformy možno zariadiť napr. Amazon Marketplace, Bing Search, Facebook, Google Play, Google Search, Uber a ďalšie. Pre viac informácií pozri Commission Staff Working Document on Online Platforms, accompanying the document "Communication on Online Platforms and the Digital Single Market" (COM(2016) 288). Dostupné na: https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-online-platforms

Pre ilustráciu možno spomenúť nemecký prípad *Amazon*.[29] Protisúťažná praktika Amazonu spočívala v obmedzovaní svojich zákazníkov – online vydavateľov vo využívaní inej platformy ako Amazon. Toto obmedzenie dosiahla spoločnosť Amazon cenovými dojednaniami, na základe ktorých boli vydavatelia povinní poskytnúť rovnakú alebo lepšiu cenu na Amazone ako na svojej vlastnej platforme, resp. na inej platforme. Cenové obmedzenie bolo nakoniec odstránené nielen v Nemecku, ale aj v iných európskych krajinách.

Ešte viac však v očiach verejnosti rezonoval prípad hotel *Hotel Online Booking,* ktorý bol predmetom prešetrovania vo viacerých európskych krajinách. Išlo o prípad online platformy medzi hotelmi a online cestovnými agentúrami. Protisúťažné správanie opäť spočívalo v zmluvnom obmedzení, cieľom ktorého bolo zaistiť, aby ceny, za ktoré bude hotel ponúkať svoje služby na svojej vlastnej online platforme alebo cez iný predajný kanál, neboli nižšie ako tie ceny, ktoré bude uplatňovať na online platforme prevádzkovateľa, s ktorým uzatvoril zmluvu. Takéto zmluvné ustanovenia pritom eliminovali cenovú súťaž na rôznych distribučných kanáloch. Kým vo Veľkej Británii, Francúzsku, Taliansku a Švédsku bolo prešetrovaniu ukončené tým, že prevádzkovateľ online platformy prijal záväzky, v rámci ktorých sa zaviazal odstrániť tieto zmluvné obmedzenia, v Nemecku bolo prešetrovanie ukončené prijatím meritórneho rozhodnutia.

Ako končia prešetrovania týkajúce sa online platforiem? Väčšinou sa často končia prijatím behaviorálnych záväzkov, ktorých výhoda spočíva v predovšetkým v rýchlom a efektívnom odstránení súťažných obáv, čo je nevyhnutné predovšetkým pre tak rýchlo sa rozvíjajúci a meniaci sa digitálny priestor.

5.4 Kartelové dohody

Ani kartelové dohody[30] nie sú výnimkou, pokiaľ ide o implementovanie protisúťažného správania v priestore elektronického obchodovania.

Britský súťažný úrad nedávno pokutoval dvoch konkurenčných online predajcov plagátov a rámov, ktorí sa dohodli, že nebudú podliezať svoje ceny na online platforme Amazon.[31] Predmetný prípad bol zaujímavý tým, že konkurenti dosiahli úspešné implementovanie dohody používaním automatického softvéru na preceňovanie produktov.

Okrem toho, však v praxi nie je vylúčené stretnúť sa aj s prípadmi, kedy iniciatíva pre zavedenie vertikálneho cenového obmedzenia (RPM) na internete prichádza práve z dolného trhu, teda od odberateľov dotknutého výrobku – konkurentov, a to s cieľom eliminovať cenový boj medzi konkurentmi. V takomto prípade RPM slúži práve ako nástroj pre uľahčenie horizontálnej koordinácie medzi distribútormi jednej značky.

5.5 Osobné údaje verzus súťažné právo

V súčasnosti sa stále viac súťažné právo ocitá v situácii, kedy sa stáva prostriedkom na riešenie viacerých problémov, a to predovšetkým v prierezových právnych odvetviach. Súťažné úrady sa tak vyjadrujú nielen ku klasickým súťažným otázkam, ale aj k takým okruhom, ktoré na prvý pohľad spadajú do inej právnej oblasti, ako napr. otázky týkajúce sa nastavenia tendrov, ochrany spotrebiteľa, či ochrany osobných údajov.

Kým otázky súvisiace s nastavením tendra možno odôvodniť povinnosťou uplatňovania súťažného princípu v priebehu celého procesu verejného obstarávania a rovnako je v niektorých

---

29 Detaily k prípadu pozri na webovej stránke nemeckého súťažného úradu: http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Kartellverbot/2013/B6-46-12.pdf?__blob=publicationFile&v=2

30 Kartel je dohoda medzi podnikateľmi, ktorí sú vzájomnými konkurentmi, pričom jej cieľom alebo následkom je obmedzenie hospodárskej súťaže. Viac informácií na: http://www.antimon.gov.sk/co-je-kartel/

31 História prípadu (vrátane rozhodnutia) je dostupná na webovej stránke britského súťažného úradu: https://www.gov.uk/cma-cases/online-sales-of-discretionary-consumer-products

situáciách odôvodnené podávať vyjadrenia súvisiace s ochranou spotrebiteľa,[32] postavenie osobných údajov zo súťažno-právneho hľadiska je komplexnejšou problematikou.

SD EÚ sa už vo svojom rozsudku vo veci *Asnef-Equifax*[33] vyjadril k vzťahu medzi osobnými údajmi a aplikovaním súťažných pravidiel, keď uviedol, že *„prípadné otázky týkajúce sa citlivého aspektu osobných údajov nevyplývajú ako také z práva hospodárskej súťaže, môžu byť vyriešené na základe relevantných ustanovení v oblasti ochrany týchto údajov."* Z predmetného rozsudku vychádzajú viaceré súťažné úrady pri posudzovaní prípadov dotýkajúcich sa osobných údajov.

Z praxe súťažných úradov však vyplýva, že osobné údaje predstavujú aj určitý faktor hospodárskej súťaže, keďže umožňujú zlepšovať produkty, a ako bolo už vyššie uvedené, uľahčujú zacielenie reklamy. Kumulovanie a analyzovanie množstvá informácií týkajúcich sa minulých a súčasných zvykov, preferencií a záujmov totiž prispieva k vytváraniu profilov. Aplikuje sa tu pritom jednoduché pravidlo - čím je osobných údajov viac, tým rastie záujem na využívaní kumulovaných údajov.

Súťažné trendy preto ukazujú, že problematika osobných údajov ako súťažného aspektu zohráva výraznú úlohu najmä u dominantných hráčov na trhu. SD EÚ v rozsudku vo veci Michelin[34] konštatoval, že *„dominantný podnikateľ má osobitnú zodpovednosť za to, aby jeho správanie nebolo na ujmu účinnej a nerušenej hospodárskej súťaže*."

Určitú interakciu medzi postavením podnikateľa s dominantným postavením a ochranou osobných údajov ilustruje napr. prípad francúzskeho súťažného úradu vo veci *GDF Suez*,[35] kde bola táto spoločnosť prešetrovaná pre zneužitie dominantného postavenia práve z dôvodu, že osobné údaje, ktoré kumulovala z titulu svojho postavenia štátneho monopolu na trhu poskytovania plynu a elektriny, využívala na inom neregulovanom trhu. Rovnako v prípade *Belgickej národnej lotériovej spoločnosti*[36] dospel belgický súťažný úrad k záveru, že správanie tohto štátneho monopolu spočívajúce vo využívaní získaných osobných údajov pre marketing a komerčné stávkovacie služby súkromnej spoločnosti Scoore spadá pod zneužívanie dominantného postavenia. Asi najväčšiu pozornosť si však v blízkej budúcnosti bude zasluhovať prešetrovanie voči spoločnosti Facebook[37] oznámené tento rok nemeckým súťažným úradom.

Vzhľadom na špecifickosť problematiky osobných údajov však možno dospieť k záveru, že prístup k osobným údajom sa nedá riešiť inak ako individuálnym posúdením, kde je nutné zvážiť všetky aspekty konkrétneho prípadu *(case-by-case analysis).*

6 ZÁVER

Cieľom predmetného príspevku bolo zvýšiť povedomie o rôznorodosti protisúťažných praktík v digitálnom priestore. Hoci sa totiž často internet spája so širokým spektrom nelegálnych konaní od

---

[32] Účelom súťažných úradov je ochrana hospodárskej súťaže pred jej obmedzovaním, ako aj vytváranie podmienok na jej ďalší rozvoj práve v prospech spotrebiteľov.

[33] Rozsudok Súdneho dvora zo dňa 23.11.2006 vo veci C-238/05 *Asnef-Equifax v. Komisia,* Zb. [2006], s. I-11125, ECLI:EU:C:2006:734

[34] Rozsudok Súdneho dvora zo dňa 09.11.1983 vo veci 322/81 Michelin v. Komisia, Zb. [1983], s. 03461, ECLI:EU:C:1983:313

[35] Bližšie informácie pozri v rozhodnutí francúzskeho súťažného úradu č. 14-MC-02 zo dňa 9. septembra 2014 vo veci *GDF Suez.*
http://www.autoritedelaconcurrence.fr/user/avisdec.php?numero=14MC02

[36] Viac informácií pozri v tlačovej správe na webovej stránke belgického súťažného úradu: https://www.belgiancompetition.be/sites/default/files/content/download/files/20150923_press_release_15_abc.pdf

[37] Viac informácií pozri v tlačovej správe na webovej stránke nemeckého súťažného úradu: http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568

zásahu do práv spotrebiteľov, či do práv vyplývajúcich z duševného vlastníctva až po trestné činy, obmedzeniu hospodárskej súťaže v digitálnom priestore sa venuje menšia pozornosť.

V súvislosti s obmedzovaním hospodárskej súťaže v elektronickom obchode je pritom podstatné nielen zabezpečiť, aby súťažné úrady dokázali dostatočne promptne reagovať na rýchlo sa vyvíjajúci rozvoj digitálneho priestoru, ale zároveň je nevyhnutné, aby sa vytvorila kultúra dodržiavania súťažných pravidiel *(a culture of compliance*), aby každý podnikateľ rozumel tomu, aké obchodné praktiky môže prijímať, aby jeho správanie neporušovalo pravidlá hospodárskej súťaže.

Kontaktné údaje:
Mgr. Lucia Kasenčáková
lucia.kasencakova@antimon.gov.sk
Protimonopolný úrad Slovenskej republiky
Drieňová 24
826 03 Bratislava
Slovenská republika

PORUŠOVANIE PRÁV DUŠEVNÉHO VLASTNÍCTVA A DOMÉNOVÉ SPORY

Tomáš Klinka

Úrad priemyselného vlastníctva SR

Abstrakt: Domain Name Disputes occur often hand in hand with Intellectual Property Rights (IPRs) Infringement, Trade Mark Rights the most frequently. Beside an ordinary court procedure for many top-level domains (TLDs) since the 90s there has been established another system and that is Alternative Dispute Resolution (ADR). As from January 2017 domain name disputes in TLD .sk will be resolvable within ADR as well.

Abstrakt: Doménové spory sú často sprevádzané potenciálnym porušovaním práv duševného vlastníctva, najčastejšie práv z ochranných známok. Popri klasickom súdnom konaní boli vo viacerých vrcholových doménach (TLD) zavedené alternatívne riešenia sporov (ADR). Od januára 2017 aj spory vo vrcholovej doméne .sk bude možné riešiť v rámci ADR.

Kľúčové slová: Domain Name Disputes, Alternative Dispute Resolution (ADR), Intellectual Property Rights (IPRs), Domain Registration or Use in Bad Faith, Legitimate Interest.

Kľúčové slová: Doménové spory, Alternatívne riešenie sporov (ADR), Práva duševného vlastníctva, Registrácia alebo používanie domény v zlej viere, Legitímny záujem.

1 ÚVOD

Rozvoj internetu nastolil nové štandardy a zásadne posunul horizonty aj v oblasti duševného vlastníctva. Masové využívanie práv duševného vlastníctva, či už ide o autorské práva, práva z ochranných známok alebo práva z registrovaných dizajnov, a najmä ich efektívna ochrana si v prostredí internetu vyžadujú osobitný prístup zohľadňujúci povahu predmetov duševného vlastníctva na jednej strane a technologické výzvy on-line sveta na strane druhej. To platí tak pre digitálny obsah chránený prostriedkami duševného vlastníctva, ako aj pre registráciu a používanie domén. Doménové spory sú typickým sprievodným javom rozvoja internetu a ich efektívne riešenie si vyžaduje dôslednú hmotnoprávnu analýzu a adekvátne procesné pravidlá.

2 DOMÉNOVÉ SPORY

Z hľadiska bežného užívateľa je internet vybudovaný na systéme názvov domén (*Domain Name System* - DNS)[1]. Užívateľ si tak nemusí pamätať a orientovať sa v abstraktných IP adresách, ktoré predstavujú jedinečnú číselnú identifikáciu každého počítača s priamym pripojením na internet. Doménové mená sú tak vlastne praktickým sprievodcom po internete. A svojmu držiteľovi môžu prinášať aj zaujímavú komerčnú hodnotu, ak sa vďaka nim ponuka jeho produktov alebo služieb dostane k širšiemu okruhu potenciálnych zákazníkov.

Vrcholové domény resp. domény najvyššej úrovne (*Top-level domains* - TLDs) sa delia na generické vrcholové domény (*generic Top-level domains* - gTLDs), ako napríklad .com alebo .org, a na národné vrcholové domény (*country-code Top-level domains* - ccTLDs), ako napr. .us, .de, .cz alebo .sk. Domény druhej úrovne podradené jednotlivým vrcholovým doménam prideľujú prostredníctvom komerčných registrátorov jednotlivé doménové autority, ktorou je pre vrcholovú doménu .sk spoločnosť SK-NIC, a.s.[2] A práve konflikty medzi doménami druhej úrovne[3] a inými

[1] Pozri aj https://www.icann.org/ a https://www.iana.org/ (7.11.2016).
[2] Pozri aj https://www.sk-nic.sk (7.11.2016).
[3] Pre zjednodušenie sa ďalej v príspevku pojmy „doména“ a „doménové meno“ používa v zmysle „doména druhej úrovne“.

právami - najčastejšie právami duševného vlastníctva - máme na mysli, keď hovoríme o doménových sporoch.

2.1 Podstata doménových sporov

Prečo vlastne vznikajú doménové spory? Predovšetkým je to z dôvodu, že v procese registrácie domén sa neskúmajú prípadné konflikty s právami tretích osôb a dotknuté osoby nedokážu registrácii domény zabrániť. Inými slovami, nie je úlohou - a ani v technických možnostiach - registrátora a ani doménovej autority pri registrácii domény iniciatívne vyhľadávať kolízne ochranné známky alebo iné práva. Ako vyplýva aj zo znenia *Pravidiel poskytovania menného priestoru v internetovej doméne .sk*[4], ostáva výlučne na zodpovednosti samotného žiadateľa, že ním zvolené meno nezasahuje do práv tretích osôb. Druhým dôvodom je zaručená jedinečnosť domény podradenej pod konkrétnu doménu najvyššej úrovne. Nie je teda možné registrovať viac ako jednu doménu lawconference.sk, i keď postačuje aj drobné vzájomné rozlíšenie akýmkoľvek alfanumerickým znakom (napr. lawconference1.sk). V spojení so snahou získať konkurenčnú výhodu alebo sa obohatiť sa tak registrujú aj také domény, ktoré sú zhodné alebo podobné s konkrétnymi ochrannými známkami.

V praxi možno rozlíšiť niekoľko typických foriem zneužitia domén, medzi najznámejšie a najrozšírenejšie patrí *cybersquatting* (alebo aj *domain grabbing*) a jeho variant *typosquatting* (alebo aj *URL hijacking*). Všeobecnejší pojem *cybersquatting* zahŕňa rôzne prípady špekulatívneho obsadenia domény, teda takú registráciu a/alebo používanie domény, kde držiteľ domény s ohľadom na okolnosti daného prípadu nekonal v dobrej viere a zasahuje tým do práv tretích osôb, najmä majiteľov ochranných známok. Pri *typosquattingu* žiadateľ registruje domény podobné s ochrannými známkami s použitím častých preklepov, ktoré sa stávajú pri písaní na počítačovej klávesnici (napr. yuube.com, namiesto youtube.com alebo arifrance.com namiesto airfrance.com).

2.2 Slovenské doménové spory

V roku 2012 vydalo občianske združenie *European Information Society Institute* (EISi)[5] publikáciu „*Doménová čítanka. Výber zo slovenských doménových rozhodnutí*“, ktorá je dostupná on-line na webe EISi[6] pod licenciou Creative Commons. Možno v nej nájsť viac ako 20 súdnych rozhodnutí týkajúcich sa doménových sporov. Pre ilustratívne účely tohto príspevku určite postačujú tri veci: illy.sk, viagra.sk a valvoline.sk

Vo veci „illy.sk“ rozhodol Okresný súd Banská Bystrica 27. októbra 2009 rozsudkom sp. zn. 10CbPv/4/2009 tak, že žalobe o zdržanie sa používania označenia „illy“ a o prevod domény „illy.sk“ vyhovel s nasledovným odôvodnením: „*Odporca je držiteľom internetovej domény illy.sk, ktorú používa tak, že po vpísaní adresy http://www.illy.sk a odkliknutí automaticky dochádza k presmerovaniu na stránku www.caffemauro.sk propagujúcu produkty a značku konkurenčnej spoločnosti a súťažiteľa M. D. S.P.A., ktoré sú rovnaké a podobné tovarom, pre ktoré má navrhovateľ platne zaregistrované ochranné známky obsahujúce slovný prvok illy. Tým odporca bráni navrhovateľovi propagovať svoje produkty pod označením zodpovedajúcim jeho ochranným známkam na sieti internet a dopúšťa sa voči nemu nekalosúťažného konania vo forme vyvolávania*

---

[4] Pravidlo 10.4 znie: „*Držiteľ Domény vyhlasuje, že bude dbať o to, aby ním užívaná Doména neporušovala priamo alebo nepriamo práva tretích subjektov, najmä práva k ochranným známkam, užívaniu obchodného mena alebo iných práv týkajúcich sa duševného vlastníctva, a v prípade ich porušenia sám zodpovedá za spôsobenú škodu tretím osobám. Držiteľ Domény berie na vedomie, že za neprípustné označenie Domény sa v každom prípade považuje použitie slova, ktoré je dominantným prvkom a) ochrannej známky zapísanej Úradom Priemyselného Vlastníctva SR, b) medzinárodnej ochrannej známky chránenej pre územie SR, resp. c) všeobecne známej ochrannej známky bez ohľadu na štát jej pôvodu, ktorých držiteľom alebo používateľom je osoba odlišná od budúceho Držiteľa. Držiteľ Domény podaním žiadosti o registráciu Domény potvrdzuje, že s vedomím možného porušenia práv uvedených v tomto bode Pravidiel a právnych predpisov vyvinul všetko úsilie, ktoré je možné po ňom spravodlivo požadovať, aby zaistil, že registrovaná Doména nebude tieto práva a právne predpisy porušovať.*“.

[5] Pozri aj www.eisionline.org (7.11.2016).

[6] HUSOVEC, M. (ed.) *Doménová čítanka. Výber zo slovenských doménových rozhodnutí*. EISi, 2012 http://www.eisionline.org/images/PAPERS/domenova%20citanka.pdf (7.11.2016).

nebezpečenstva zámeny a parazitovania na povesti, i porušovania jeho známkových práv. Odporca takto poškodzuje a zavádza i spotrebiteľov, ktorí sa pri použití domény illy.sk (prakticky zhodnej s rozlišovacou časťou obchodného mena navrhovateľa a označením jeho výrobkov) logicky domnievajú, že ide o produkty navrhovateľa.".

Vo veci „viagra.sk" rozhodol Okresný súd Banská Bystrica 24. marca 2010 rozsudkom sp. zn. 16CbPv/13/2008 tak, že vyhovel žalobe a nariadil prevod domény viagra.sk na žalobcu. Z odôvodnenia rozsudku: „*Z vykonaného dokazovania mal súd za preukázané, že žalovaný 1) tým, že sa stal držiteľom doménového mena viagra.sk, ktoré je totožné so všeobecne známou ochrannou známkou žalobcu VIAGRA, zasiahol a zasahuje do práv k jeho ochrannej známke. Aj keď žalovaný 1) neoznačuje totožným označením viagra žiadne tovary a služby, ustanovenie § 25 ods. 1 vymedzujúce práva majiteľa ochrannej známky negatívnym spôsobom treba interpretovať vo vzťahu k pozitívnemu vymedzeniu práv majiteľa ochrannej známky v § 24 ods. 1 a § 26 ods. 1 a 2. Jednou z funkcií ochrannej známky je totiž aj funkcia propagačná (náborová), ktorej podstatu možno vyvodiť z § 24 ods. 1 v tom, že majiteľ ochrannej známky má právo používať ochrannú známku v spojení so zapísanými tovarmi alebo službami. Žalobca nemôže v prostredí internetu využívať propagačnú stránku svojej ochrannej známky tým spôsobom, že by na internetovej stránke pod doménovým menom viagra.sk predstavoval svoj liek Viagra napriek tomu, že jeho ochranná známka má časovú prioritu predchádzajúcu registrácii domény. Treba zdôrazniť, že žalovaný 1) nemá (a ani nikdy nemal) nijaké právo používať s ochrannou známkou totožné označenie viagra, pretože iba zo samotnej technickej registrácie doménového mena, v tomto prípade uskutočnenej ešte neskoršie než je priorita ochrannej známky, nevznikajú majiteľovi doménového mena žiadne právnym poriadkom uznané práva na označenia. Takýto protiprávny stav, ktorý žalovanému 1) umožňuje žalovaný 2) [pozn.: ide o SK-NIC, a.s.], je ešte zvýraznený tým, že žalobcova ochranná známka je všeobecne známou, kedy zákon nevyžaduje väzbu na rovnaké alebo podobné tovary a služby ako známkou chránené.*". Súd ďalej konštatoval, že popri porušení známkových práv, došlo aj k nekalosúťažnému konaniu a to nielen na strane držiteľa domény viagra.sk, ale dokonca aj na strane SK-NIC, a.s. Špekulatívnosť u držiteľa videl súd v tom, že internetovú stránku s doménou viagra.sk držiteľ neprevádzkuje a jej prevod ponúkol žalobcovi za odplatu mnohonásobne prevyšujúcu náklady na registráciu domény (50 000 eur).

Vo veci „valvoline.sk" sa zaoberali návrhom na vydania predbežného opatrenia súdy troch stupňov: Dovolací Najvyšší súd SR v uznesení z 13. októbra 2010, sp. zn. 3M Obdo 1/2009 uviedol: „*Navrhovateľ mal naliehavý právny a ekonomický záujem na tom, aby nedochádzalo k porušovaniu práv k jeho ochranným známkam a ku konaniu nekalej súťaže narušujúcej pokojný stav zo strany odporcu. Tento naliehavý právny a ekonomický záujem na vydanie predbežného opatrenia navrhovateľ zdôvodnil vo svojom podaní tým, že zatiaľ čo odporca neoprávnene využíva pre svoje podnikanie výhody svetovo presláveného označenia Valvoline (tzn. všeobecne známej ochrannej známky) a farebného „V", navrhovateľ musel čeliť odmietaniu uzavretia distribučných zmlúv s novým predajcom. Takéto konanie považoval navrhovateľ za konanie, ktorým mu hrozilo nebezpečenstvo vzniku ťažko napraviteľnej majetkovej (strata tržieb, strata trhu, strata bezprostredných distribútorov a odberateľov) i nemajetkovej (strata goodwilu, erodovanie známkovej ochrany) ujmy.*".

Z uvedených troch príkladov doménových sporov, ktoré prejednávali slovenské súdy, možno identifikovať niekoľko všeobecných charakteristík. Z hmotnoprávneho hľadiska sú uplatňované nároky spravidla založené tak na známkovej ochrane, ako aj na ochrane proti nekalej súťaži. Súdy pri rozhodovaní o týchto nárokoch považujú za významné najmä a) špekulatívne konanie držiteľa domény (resp. jeho konanie v zlej viere), b) chýbajúce oprávnenie držiteľa domény k danému označeniu, c) časovú prioritu ochrannej známky, d) známosť a dobré meno ochrannej známky a f) aj iné funkcie ochrannej známky (napr. propagačná funkcia). Konštrukcia pasívnej legitimácie je pomerne ťažkopádna, keď - pravdepodobne v záujme právnej istoty žalobcu - býva popri samotnom držiteľovi domény žalovaná aj národná doménová autorita SK-NIC, a.s. Je zaujímavé, že v doménových sporoch žalobcovia zväčša neuplatňujú žiadne nároky na finančné plnenia, či už reparačné alebo satisfakčné, prednosť má odstránenie protiprávneho stavu a jeho následkov. A napriek obvyklej praxi slovenských súdov, nie je ani zďaleka jasný právny základ „nároku" na prevod domény[7].

[7] HUSOVEC, M.: Je možné žalovať o prevod domény? In Revue pro právo a technologie č. 1/2011; článok je dostupný on-line na http://www.lexforum.cz/268 (7.11.2016). HUSOVEC, M.: Je ešte stále

3 CHARAKTERISTIKA ALTERNATÍVNEHO RIEŠENIA DOMÉNOVÝCH SPOROV (ADR)

Alternatívne riešenie sporov (*Alternative Dispute Resolution* - ADR) je používané ako štandardné riešenie sporov pre generické domény, ako napr. „TLDcom“ či „TLDorg“, ale aj pre národné domény vo Francúzsku, Holandsku, Švajčiarsku, Poľsku alebo Srbsku; naposledy bolo ADR zavedené od 1. marca 2015 v Českej republike[8] a to po predchádzajúcom dlhoročnom rozhodovaní doménových sporov v rozhodcovskom konaní (*Rozhodčí soud při Hospodářské komoře ČR a Agrární komoře ČR*), ktoré ukončilo až rozhodnutie Nejvyššího soudu ČR vo veci vo veci „suzuki.cz“ zo 17. decembra 2013 , sp. zn. 23 Cdo 3895/2011[9].

V rámci ADR sa riešia doménové spory medzi držiteľmi domén a tretími osobami, ktorí ako sťažovatelia toto konanie iniciujú v záujme ochrany svojich práv (často práv duševného vlastníctva a typicky známkových práv). Riešenie sporov prebieha na diaľku, zväčša elektronicky s následným vydaním expertného rozhodnutia. Z hľadiska všeobecných zásad alternatívneho riešenia sporov (nielen tých doménových) nie je výsledkom ADR rozhodnutie v úzkom slova zmysle[10], ale skôr stanovisko experta (*expert's opinion*). Je potrebné zdôrazniť, že doménové ADR nepredstavuje rozhodcovské konanie v zmysle príslušnej legislatívy[11]. Tiež je potrebné dôsledne odlišovať doménové ADR od tzv. alternatívneho riešenia spotrebiteľských sporov[12].

ADR nepredstavuje výkon štátnej moci. Rozhodnutia experta je samovykonateľné bez potreby nútenej exekúcie a jeho „výkon“ zabezpečí doménová autorita vyznačením príslušnej zmeny v registri domén. Táto samovykonateľnosť je možná (a efektívna) najmä preto, lebo v ADR možno uplatniť len nárok na zrušenie domény alebo nárok na prevod domény. Nemožno uplatniť napr. nárok na náhradu škody ani iné nároky, ktoré majiteľom ochranných známok priznáva právny poriadok. ADR je príkladom osobitného typu samoregulácie, resp. komunitnej spoluregulácie, oddelenej od výkonu štátnej moci. Výnimočne môže byť ADR zakotvené aj priamo v zákone. Príkladom je samotná Európska únia, ktorá prostredníctvom svojich nariadení v roku 2002 vytvorila ADR v doméne .eu[13] alebo aj USA s *Anticybersquatting Consumer Protection Act (ACPA) z roku 1999*. V drvivej väčšine krajín však ADR funguje ako forma samoregulácie, kde správca generickej alebo národnej domény zakotvuje možnosť riešenia sporov do svojich pravidiel a následne ním poveruje určité zoskupenie expertov[14].

Prípadné obavy, že v dôsledku ADR by niekomu mohlo byť odňaté právo obrátiť sa na súd, sú neopodstatnené. Neúspešný sťažovateľ alebo neúspešný držiteľ domény sa môže - v stanovenej lehote - obrátiť na príslušný súd, ktorý rozhodnutím experta nie je formálne viazaný. Na druhej strane ADR rozhodnutia bývajú súdmi rešpektované kvôli vysokej úrovni právnej expertízy a argumentácie.

3.1 Cesta k ADR v doméne .sk

Na podnet Úradu priemyselného vlastníctva SR (ÚPV SR) na zasadnutí 19. januára 2015 *Medzirezortná komisia na koordináciu spolupráce v oblasti boja proti falšovaniu a autorskému pirátstvu* (MRK) schválila aktualizáciu *Národnej stratégie boja proti falšovaniu a autorskému pirátstvu* a prijala *Akčný plán na rok 2015*, ktorý zahŕňa aj iniciovanie zavedenia ADR konania v doménových sporoch s národnou doménou .sk[15]. Zástupcovia ÚPV SR na základe toho oslovili SK-NIC, a.s. a aj *Komisiu pre správu národnej domény .sk* a na jej zasadnutí 9. decembra 2015 spolu so zástupcami EISi predstavili návrh na zavedenie ADR[16]. Prvé pokusy o zavedenie ADR v doméne .sk pritom

možné žalovať o prevod domény? In Revue pro právo a technologie č. 6/2012; článok je dostupný on-line na https://journals.muni.cz/revue/article/download/4129/pdf (7.11.2016).

8 http://www.nic.cz/page/314/pravidla-a-postupy/ (7.11.2016).

9 http://kraken.slv.cz/23Cdo3895/2011 (7.11.2016).

10 Z týchto dôvodov sa v súvislosti s ADR nepoužívajú pojmy ako „právomoc“, „rozsudok“, „právoplatnosť“ alebo „účastník konania“.

11 Zákon č. 242/2002 Z. z. o rozhodcovskom konaní alebo zákon č. 335/2014 Z. z. o spotrebiteľskom rozhodcovskom konaní.

12 Zákon č. 391/2015 Z. z. o alternatívnom riešení spotrebiteľských sporov.

13 Nariadenie Európskeho parlamentu a Rady (ES) č. 733/2002 z 22. apríla 2002 o zavedení domény najvyššej úrovne „.eu“.

14 Napr. WIPO Arbitration Center; pozri http://www.wipo.int/amc/en/ (7.11.2016).

15 http://www.upv.sk/swift_data/source/pdf/Narodna_strategia_aktualizacia_2015.pdf (7.11.2016).

16 http://informatizacia.sk/ext_dok-zapis_stret_komsk_13_09122015/22593c (7.11.2016).

prebehli už v roku 2012[17]. *Komisia pre správu národnej domény .sk* dňa 4. apríla 2016 schválila *Pravidlá alternatívneho riešenia sporov* (Pravidlá ADR) a vybrala konkrétne centrum ADR, ktorým sa stalo EISi. Vzhľadom na navrhnutú účinnosť Pravidiel ADR (9. január 2017) sa následne k Pravidlám ADR otvorili verejné konzultácie[18], ktoré organizovali spoločne EISi a SK-NIC, a.s. Výsledky verejných konzultácii sa premietli aj do revidovaného znenia Pravidiel ADR, ktoré boli schválené v novembri 2016[19].

3.2 Pravidlá ADR

Pravidlá ADR tvoria prílohu a nedielnu súčasť *Pravidiel poskytovania domén v doméne najvyššej úrovne .sk* a súčasť Zmluvy o Doméne [Pravidlo 1.1]. Cieľom riešenia sporov podľa Pravidiel ADR je, s vedomím ich technickej, obchodnej a ekonomickej funkcie, umožniť rýchle riešenie sporov o domény .sk, avšak s dôrazom na kvalitu, nestrannosť, transparentnosť a spravodlivosť [Pravidlo 1.2].

Centrom ADR je European Information Society Institute, o.z. (EISi). Centrum ADR vedie zoznam expertov, administruje priebeh sporu podľa Pravidiel ADR a vydáva *Poriadok pre riešenie sporov o Domény .sk* [Pravidlo 2.2]. **Expertom** je osoba, ktorá rieši spor podľa Pravidiel ADR a je zapísaná v zozname expertov vedenom Centrom ADR; ak nie je uvedené inak, Expertom sa rozumie aj Panel expertov [Pravidlo 2.3]. **Panel expertov** je skupina troch expertov riešiacich spor podľa Pravidiel ADR, ak je postupom podľa Poriadku zvolené riešenie sporu Panelom expertov [Pravidlo 2.4]. **Sťažovateľom** je osoba, ktorá podá Centru ADR v súlade s Pravidlami ADR návrh na riešenie sporu s Držiteľom vo veci Domény [Pravidlo 2.5]. **Chráneným označením** sa rozumie právom chránené označenie, najmä zapísaná ochranná známka, označenie pôvodu výrobku, zemepisné označenie výrobku, názov chránenej odrody rastlín, nezapísané označenie, obchodné meno, názov právnickej osoby, vrátane názvu orgánov verejnej správy vrátane verejnoprávnych inštitúcií, štátov či medzinárodných organizácií, označenie podniku či prevádzkarne, meno alebo chránený pseudonym alebo všeobecne známa prezývka fyzickej osoby alebo názov chráneného literárneho či umeleckého diela alebo označenie literárnych postáv [Pravidlo 2.6].

Hmotnoprávne jadro riešenia doménového sporu možno nájsť v Pravidle 3.1, ktoré znie nasledovne:

Držiteľ sa zaväzuje podriadiť sa riešeniu sporov podľa Pravidiel ADR a Poriadku v prípade, že Sťažovateľ podá Centru ADR návrh, v ktorom tvrdí, že

- **Reťazec znakov tvoriaci Doménu Držiteľa je zhodný alebo podobný s Chráneným označením, ku ktorému má alebo vykonáva Sťažovateľ práva, medzi Doménou Držiteľa a Chráneným označením existuje pravdepodobnosť zámeny, pričom toto sa neuplatňuje, ak z bodu 3.8 [pozn.: ak Chránené označenie má v relevantnej časti verejnosti dobré meno alebo dobrú povesť] nevyplýva inak, a zároveň**
- **Doména**
  - **a) bola zaregistrovaná alebo získaná bez toho, aby mal súčasný Držiteľ k Doméne alebo Chránenému označeniu právo alebo legitímny záujem a zároveň [!!!]**
  - **b) nebola zaregistrovaná, získaná alebo používaná v dobrej viere.**

Okruh prípadov, na ktoré by sa Pravidlá ADR mohli uplatňovať, je v súlade s *Uniform Domain-Name Dispute-Resolution Policy* (UDRP)[20] a na rozdiel od ADR v doméne .eu sa vyžaduje **kumulácia oboch základných podmienok**: a) nedostatku subjektívneho práva resp. legitímneho záujmu a b) konania v zlej viere. Pravidlá ADR umožňujú expertovi, ktorý doménový spor rieši, považovať v určitých situáciách každú z týchto podmienok za splnenú [Pravidlá 3.2 až 3.4] Kategórie zhodnosti a podobnosti sú známe zo známkového práva a ich posudzovanie by nemalo spôsobovať problémy. Pokiaľ ide o koncept pravdepodobnosti zámeny, je potrebné upozorniť, že na rozdiel od

17 http://informatizacia.sk/ext_dok-zapis_stretnutia_komsk_11_24092012/14950c (7.11.2016).
18 http://www.eisionline.org/index.php/sk/2-uncategorised/140-otvorenie-verejnej-diskusie-k-pravidlam-alternativneho-riesenia-sporov-adr (7.11.2016).
19 Pravidlá ADR budú čoskoro zverejnené na webovom sídle https://www.sk-nic.sk.
20 https://www.icann.org/resources/pages/help/dndr/udrp-en (7.11.2016).

známkovoprávnej konštrukcie[21] sa nemusí brať do úvahy aj zhodnosť alebo podobnosť tovarov alebo služieb, čo zohľadňuje špecifiká doménových sporov.

Pravidlá ADR priznávajú aktívnu legitimáciu popri nositeľovi práv k Chránenému označeniu (napr. majiteľovi ochrannej známky) aj držiteľovi výhradnej licencie a so súhlasom nositeľa práv aj iným osobám [Pravidlo 3.9]. V rámci riešenia sporu podľa Pravidiel ADR nie je možné priznať náhradu vzniknutej ujmy či náhradu nákladov vynaložených na riešenie sporu, ani náhradu poplatkov zaplatených Centru ADR [Pravidlo 4.2]. Rozhodnutie Experta je konečné a nie je možné ho preskúmať. Tým nie je dotknuté právo ktorejkoľvek strany začať súdne konanie alebo rozhodcovské konanie [Pravidlo 4.3 v spojení s Pravidlami 7.1 a 7.2].

Centrum ADR zabezpečí, aby bolo rozhodnutie Experta zverejnené v súlade s Poriadkom, a to v elektronickej forme a najneskôr do 30 dní od jeho doručenia obom stranám [Pravidlo 4.4]. To by malo prispieť k transparentnosti a budovaniu odbornej autority Centra ADR v oblasti riešenia doménových sporov.

Doménová autorita SK-NIC, a.s. nie je účastníkom riešenia sporu podľa Pravidiel ADR [Pravidlo 6.1] a jej postavenie sa obmedzuje výlučne na vykonávateľa rozhodnutia Experta [Pravidlo 6.2] s výnimkou ak držiteľ domény do 10 dní od doručenia rozhodnutia Experta podľa bodu 6.2 doručí SK-NICu dokument preukazujúci začatie konania v súvisiacej veci pred súdom alebo rozhodcovským súdom, SK-NIC nevykoná zmenu uvedenú vo výroku rozhodnutia Experta.

4 ZÁVER

Doménové spory sú špecifickým prípadom porušovania práv na internete. V záujme ich rýchleho a efektívneho riešenia sa spoločným úsilím vládneho aj mimovládneho sektora podarilo aj na Slovensku zaviesť ADR v doméne .sk. Centrom ADR sa stal *European Information Society Institute* (EISi). Až náležitá aplikácia Pravidiel ADR v praxi ukáže všetky výhody (a prípadné riziká) ADR. Dôležité však je, aby sa pritom vždy uplatňovala odbornosť, transparentnosť a spravodlivosť. Štartovacie nastavenie ADR v doméne .sk k tomu má všetky predpoklady.

Použitá literatúra:

HUSOVEC, M. (ed.) *Doménová čítanka. Výber zo slovenských doménových rozhodnutí*. EISi, 2012 http://www.eisionline.org/images/PAPERS/domenova%20citanka.pdf (7.11.2016).
HUSOVEC, M.: Je možné žalovať o prevod domény? In Revue pro právo a technologie č. 1/2011; článok je dostupný on-line na http://www.lexforum.cz/268 (7.11.2016).
HUSOVEC, M.: Je ešte stále možné žalovať o prevod domény? In Revue pro právo a technologie č. 6/2012; článok je dostupný on-line na https://journals.muni.cz/revue/article/download/4129/pdf (7.11.2016).

Kontaktné údaje:

JUDr. Tomáš Klinka
tomas.klinka@indprop.gov.sk
Úrad priemyselného vlastníctva SR
Švermova 43
974 04 Banská Bystrica
Slovenská republika

.

[21] Pozri § 8 ods. 2 zákona č. 506/2009 Z. z. o ochranných známkach.

LEX MERCARTORIA A LEX INFORMATICA

Andrea Kluknavská

Právnická fakulta Univerzity Komenského

Abstract: Modern information communication technologies have become integral parts of our society, in which the cyberspace specifically represents a parallel of the virtual world with the real world. Legal systems of the existence of cyberspace, which includes the Internet, failed to react and did not address regulation of this phenomenon. The question of whether cyberspace should be regulated stands in the spotlight of various concepts of modifications for regulation of cyberspace and the Internet.

Abstrakt: Moderné informačné a komunikačné technológie sa stali neoddeliteľnou súčasťou našej spoločnosti, v ktorej práve kyberpriestor predstavuje paralelu virtuálneho sveta k svetu reálnemu. Právne systémy na existenciu kyberpriestoru, ktorého súčasťou je internet, nedokázali reagovať a neriešili reguláciu tohto fenoménu. Otázka, či by mal byť kyberpriestor regulovaný, stojí v centre pozornosti rôznych konceptov úpravy regulácie kyberpriestoru a internetu.
Kľúčové slová: Cyberspace, internet, Self – regulation, jurisdiction of state, lex mercatoria, lex informatica
Kľúčové slová: Kyberpriestor, internet, samoregulácia, jurisdikcia štátu, lex mercartoria, lex informatica.

1 ÚVOD

Kyberpriestor sa stal v posledných desaťročiach súčasťou nášho každodenného života. Kyberpriestor nie je už len miestom a priestorom pre vedcov a cyber-freakov, ale rozvinul sa do globálneho trhu a umožňuje nielen veľkým spoločnostiam, ale i jednotlivcom stať sa hráčom v tomto nekonečnom priestore. Jedným klikom myškou sa uskutočňujú geograficky hranice presahujúce obchody, ktoré sa stali obchodmi masovými a sú charakteristické svojou rýchlosťou. Jedným klikom myškou sa stávame súčasťou tohto virtuálneho sveta.

Právne systémy však na rýchly vývoj a zmeny v rámci kyberpriestoru reagujú iba veľmi ťažko, čo súvisí s náročnosťou a zdĺhavosťou legislatívneho procesu, ako i faktom, že fenomém kyberpriestor nie je právnym subjektom a nie je geograficky vymedzený. A tu vyvstáva otázka ako by malo byť toto nové prostredie regulované. Práve z uvedeného dôvodu sa počas celej existencie fenoménu kyberpriestor formovali a formujú rôzne koncepcie možnej úpravy regulácie.

2 KYBERPRIESTOR

Vznik pojmu kyberpriestor sa spája so zakladateľom cyberpunku, americko-kanadským autorom Williamom F. Gibsonom, ktorý tento pojem použil v poviedke „Ako vypáliť Chrome“ a neskôr vo svojej knihe Neuromancer, kde popísal kyberpriestor ako konsezuálnu dátovú halucináciu, vizualizovanú v podobe imaginárneho priestoru, ktorý tvoria počítačovo spracované dáta a tento priestor je prístupný len vedomím užívateľov.[1] Jeho metaforická vízia, „kyberpriestor je metafora“, sa stala v osemdesiatych a deväťdesiatych rokoch minulého storočia vzorom pre tvorcou počítačových systémov a samotný pojem sa stal pevnou časťou subkultúr spojených s rozvíjajúcimi sa digitálnymi médiami.

Následne pojem kyberpriestor preberá jazyk teoretickej reflexie kyberkultúry a digitálnych médií. Ako jeden z prvých začal pojem kyberpriestor vo vzťahu k existujúcim počítačovým sieťam používať John Perry Barlow.[2] Podľa Barlowa je kyberpriestor možné chápať ako deteritorializovaný symbolický

[1] POLČÁK,R. – ŠKOP,M. – MACEK, J.: Normatívne systémy v kyberpriestore (úvod do štúdia). Brno: Masarykova univerzita,2005, s. 7. Pozri ďalej GIBSON,W.: Jak vypálit Chrome. Brno: Návrat, 2004, GIBSON, W. Neuromancer. Plzeň: Laser,1992, str. 46.

[2] Pozri ďalej Barlow, J.P. Unabhängichkeitserklärung des Cyberspace. [cit.16.10.2016]. Dostupné na http://www.heise.de/tp/artikel/1/1028/1.html

priestor mediovanej komunikácie a záleží len na zložitosti technológie, nakoľko komplexný kyberpiestor bude. Barlowský kyberpriestor teda variuje od jednoduchých telefónnych rozhovorov cez priestor súčasného internetu až po celkom pohlcujúce priestory virtuálnych realít, ktoré sú čiastočne celkom fiktívne.

V deväťdesiatych rokoch minulého storočia sa stretávame s tzv. sociálno-antropologickým konceptom kyberpriestoru, čo súvisí so zvýšeným záujmom sociálnych teoretikov o témy digitálnych médií. Podľa Davida Hakkena je kyberpriestor ako sociálna aréna, do ktorej vstupujú všetci sociálni aktéri, ktorí používajú k vzájomnej sociálnej interakcii pokročilé informačné teórie.[3]

Kyberpriestor prestal byť už dávno fikciou, je mladou, meniacou sa a silnejúcou vrstvou reality – je technologicky mediovaný priestor sociálnej interakcie. Je to teda určite priestor v mnohých ohľadoch metamorfický, ale zároveň i priestor kultúrne a mocensky kolonizovaný.

Kybernetický priestor je teda virtuálny priestor bez hraníc, považovaný za globálnu interaktívnu doménu v rámci informačného prostredia, ktorá je charakteristická používaním elektronického a elektromagnetického spektra pre vytváranie, ukladanie, modifikovanie a výmenu dát a využívanie služieb a zároveň kybernetický priestor znamená aj kombinovaný fenomén globálneho prepojenia, decentralizovaných a stále sa rozširujúcich elektronických informačných, komunikačných a riadiacich systémov, ako aj prepojenia spoločenských a hospodárskych procesov objavujúcich sa vo forme dát a informácií prostredníctvom týchto systémov, vrátane dát v nich uložených, resp. spracovávaných.

3 INTERNET AKO SÚČASŤ KYBERPRIESTORU

Súčasťou kyberpriestoru ako priestoru tak viruálneho a reálneho, priestoru bez hraníc je internet. Internet vznikol ako siet štyroch počítačov na Kalifornskej univerzite[4] v druhej polovici minulého storočia a jeho rozšírenie do celého sveta vyvolalo veľký obdiv. Predstavy vizionárov o „globálne propojenej počítačovej siete, cez ktorú by mohol každý rýchle a jednoducho pristupovať k dátam, aplikaciám a programom z ktoréhokoľvek miesta na svete“ pripadali ako neskutočné a ťažko realizovateľné, avšak čím viac sa tieto myšlienky realizovali a stávali skutočnosťou, začalo byť zrejmé, že ide o jeden z najdôležitejších vynálezov na svete. [5]

Internet teda predstavuje priestor, priestor samostatný, ktorý je úplne odlišný od reálneho sveta, a práve to ho robilo výnimočným, a preto bolo veľmi ťažké, ba dokonca sa zdalo až nemožné ho v danom odbobí právne regulovať.[6] Nepotrebnosť regulácie bola charakteristická práve pre obdobie počiatkov internetu. Otázka regulácie však vyvstala až neskôr, kedy sa začalo otvorene diskutovať a v podstate táto diskusia trvá až do dnes. V popredí stojí otázka, či a ako má byť tento priestor regulovaný.

4 MODELY ÚPRAVY INTERNETU[7]

Samoregulácia a štátna regulácia

Výsledkom v rámci debát prebiehajúcich v deväťdeiatych rokoch minulého storočia ohľadne regulácie internetu (a teda i kyberpriestoru) bolo vytvorenie dvoch oblastí názorov, a to názory, ktoré uprednostňovali samoreguláciu a názory, kde v popredí stála štátna regulácia. Liberáli, predovšetkým v USA, sa zasadzovali za to, aby internetový priestor nebol regulovaný a tvrdili, že je žiaduce, aby

---

[3] POLČÁK,R. – ŠKOP,M. – MACEK, J.: Normatívne systémy v kyberpriestore (úvod do štúdia). Brno: Masarykova univerzita,2005, s. 8.

[4] Brief history of the internet, Internet society. [cit.16.10.2016]. Dostupné na: http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet#LGR66.

[5] LICKLIDR, J. C. R., CLARK, W. On-Line Man Computer Communication. AFIPS Conference Proceedings, 1962, č. 21, s. 113 - 128. ROBERTS, L. – W., S.: A Brief history of Internet [cit.16.10.2016]. Dostupné na: http://www.isoc.org/internet/history/brief.shtml.

[6] SEGURA-SERRENO,A.: Internet regulation and the role of International law. [cit.16.10.2016]. Dostupné na http://www.mpil.de/files/pdf3/06_antoniov1.pdf

[7] Úprava internetu je vývoj a aplikácia vládami, súkromným sektorom a občianskou spoločnosťou, v ich jednotlivých úlohách, zo spoločných princípov, noriem, pravidiel, rozhodnutí a vytvárania procedúr a programov, ktoré tvarujú evolúciu a využívanie internetu. Pracovná definícia vytvorená na Svetovom summite informačnej spoločnosti v roku 2005. Pozri ďalej KRUGER, L.G.: Governance and the Domain Name system: Issues for Congress, April 23, 2013. [cit.16.10.2016]. Dostupné na http://www.fas.org/sg/crs/misc/R42351.pdf

štát do internetového priestoru nezasahoval, a teda internet mal byť bez štátnej regulácie.[8] Liberáli sa snažia o vytvorenie miesta pre „netcitizens“, teda pre obyvateľov internetu. Vo svojej argumentácii vychádzajú z charakteristík kyberpiestoru, ktorý je bez hraníc, a preto považujú snahy teritoriálnych autorít za nerealistické v snahe o regulovanie tohto nikde nekončiaceho priestoru. Podľa zástancov tohto názoru bolo najrozumnejšie namiesto štátnej regulácie poskytnúť samoreguláciu, založenú na myšlienke delegácie tzv. neformálne pravidlá „netiquette internet etiquette“ sformulované v rámci využívania daného priestoru jeho užívateľmi ako i ďalšími subjektami, ktoré dáta na internete sprostredkúvajú. Netcitizens sú skutoční a legitímni tvorcovia tohto nového sociálneho priestoru.[9] V rámci presadzovania samoregulácie zostáva nezodpovedaná otázka, či každá existujúca oblasť bude podliehať samoregulácii, alebo či budú existovať oblasti, v ktorých bude potrebný a v niektorých prípadoch priam žiadúci zásah štátu.
Druhým názorom vychádzajúcim z danej debaty bola skupina, ktorá nepripúšťala myšlienku, aby internet zostal bez zásahu vnútroštátnej právnej regulácie. Samotné špecifiká internetu (vrátane kyberpriestoru) ako voľného, nezávislého a geograficky neohraničeného priestoru poukazujú na to, že tento priestor pravdepodobne celkom podliehať jurisdikcii štátu nemôže, a preto sa objavujú názory na právnu reguláciu na základe kombinácie princípu samoregulácie a štátnej regulácie, táto možnosť by potom mala zabezpečiť určitú legitímnosť, flexibilitu a vymáhateľnosť požiadaviek na internetovú reguláciu tak, aby sa stala fungujúcim právnym systémom.[10]

Kolízne normy a obmedzenie práva silnejšieho

Vrámci rôznych debát ohľadne regulácie kyberpriestoru a internetu sa stretneme i s názorom, ktorý stavia do popredia presvedčenie, že i napriek globalizácii internetu nesmie dôsť k strate rešpektu voči suverenite jednotlivých štátov.[11] Ak stratia štáty svoju suverenitu bude to prvý krok k akémusi svetovému právnemu poriadku, ktorý bude stáť na princípe práva silnejšieho. Do určitého stupňa tento proces nebude asi možné celkom zastaviť, avšak je potrebné zabrániť, aby začiatkom tohto procesu bol práve internet. Rosenthal zároveň veľmi striktne poukazuje na to, že nemôžeme ignorovať fakt, že ak niekto chce využívať výhody globalizácie, musí znášať i nevýhody.[12] Ak teda chce podnikateľ robiť obchody so subjektami cudzej krajiny, tak musí znášať a rešpektovať i pravidlá tej krajiny. Práve z vyššie uvedených dôvodov sú názory na vytvorenie jednotných medzinárodných štandardov nereálne, avšak veľký potenciál vidí Rosenthal v kolíznom práve, ktoré by malo byť založené na obdobnej úprave ako námorné právo, tak aby nedošlo k spochybneniu jurisdikcie jednotlivých štátov a právo silnejšieho bolo obmedzené.[13]

[8]BECKOVÁ, D.: Regulácia internetu na medzinárodnej úrovni – spôsoby, minulosť a budúcnosť, obsah právnej úpravy, regulované vzťahy. In Informačná spoločnosť a medzinárodné právo. s.28 a nasl. [cit.16.10.2016]. Dostupné na http://www.upjs.sk/pracoviska/univerzitna-kniznica/e-publikacia/#prf

[9]DE VES MESTDAGH,C.N.J.–RIJGERSBERG, R. W.: Internet governance and global self regulation: teoretica and empirical buildings blocks for a general theory of self regulation. [cit.14.10.2016]. Dostupné na http://www.tandfonline.com/doi/abs/ 10.1080/17521467. 2010.1142 4719

[10]BECKOVÁ, D.: Regulácia internetu na medzinárodnej úrovni – spôsoby, minulosť a budúcnosť, obsah právnej úpravy, regulované vzťahy. In Informačná spoločnosť a medzinárodné právo. s.28 a nasl. [cit.16.10.2016]. Dostupné na http://www.upjs.sk/pracoviska/univerzitna-kniznica/e-publikacia/#prf

[11]ROSENTHAL,D.: Herausforderungen durch die Globalität des Internets:Problemstellung und Lösungsansätze der Praxis. [cit.16.10.2016]. Dostupné na http://www.homburger.ch/fileadmin/ publications /HEFOGLOI.pdf

[12]ROSENTHAL,D.: Herausforderungen durch die Globalität des Internets:Problemstellung und Lösungsansätze der Praxis. [cit.16.10.2016]. Dostupné na http://www.homburger.ch/fileadmin/ publications /HEFOGLOI.pdf

[13]ROSENTHAL,D.: Herausforderungen durch die Globalität des Internets:Problemstellung und Lösungsansätze der Praxis. [cit.16.10.2016]. Dostupné na http://www.homburger.ch/fileadmin/ publications /HEFOGLOI.pdf

Solumov model úpravy internetu

Lawrence B. Solum z Ilinoiskej univerzity vo svojej štúdii uvádza medzi základné modely úpravy internetu v súčasnosti tieto modely: model of cyberspace alebo spontaneous ordering, model of transnational institutions a international organization, model of code and internet architecture, model of national governments and law a model of market and economics.

Cyberspace and spontaneous Ordering vychádza z teórie liberálov 90-tych rokov presadzujúcich samoreguláciu internetu (aj kybernetického priestoru), ktorej sme sa venovali v texte vyššie. Solum tu poukazuje na to, že v danom období, teda v deväťdesiatych rokoch minulého storočia, sa táto cesta javila ako tá správna. Vtedy sa nepočítalo s tým, že vlády a štáty si začali uvedomovať dôležitosť a využiteľnosť internetu a v súčasnosti už nazývať tento priestor „nezávislou krajinou" v zmysle prepojenosti vlád a medzinárodných spoločností je už veľmi ťažké. Zároveň je potrebné uviesť, že úvahy o kreovaní samostatných inštitúcií v rámci predmetného priestoru sú efektívnym názorom proti pokladniu internetu za krajinu bez zákona. Napriek tomu v sebe táto teória nesie dôležité presvedčenie, a tým je, že samotná architektúra internetu je v rozpore s národnou vládou nad internetom, pretože internet je globálna sieť, ktorá môže preniesť akúkoľvek informáciu, ktorá môže byť digitalizovaná, z čoho vyplýva, že žiaden štát nemá prostriedky, a to ani technické a ani finančné, na kontrolu týchto informácii s cieľom monitorovať obsah v podmienkach štátnych hraníc.[14] Informácie sa internetom lámu na menšie časti, ktoré sa môžu dopraviť do cieľa rôznymi cestami.[15]

Model transnationálnych inštitúcií a nadnárodných organizácií stojí na myšlienke zabezpečiť kontrolu virtuálneho priestoru prostredníctvom nadnárodných organizácií, ktoré by boli nezávislé od jurisdikcie štátu. Tento nápad sa zároveň triešti v chápaní nezávislosti týchto nadnárodných organizácií od vplyvu národných vlád. V súčasnosti existuje spoločnosť ICANN[16] ako medzinárodná organizácia, ktorá nie je založená na základe zmlúv, narozdiel od WIPO a ITU[17], ktoré sú agentúrami OSN. Autorita ICANN prišla s alternatívnym riešením sporov vo forme pravidiel rozhodcovského konania, ktoré zahrňujú vedľa procesnej úpravy tiež autonómnu hmotnoprávnu úpravu.[18] Z uvedeného teda vyplýva, že v prípade ak si subjekt registruje doménové meno zároveň sa zaväzuje touto registráciou okrem iného i k tomu, že strpí odobratie tohto doménového mena v prípade, ak rozhodca skonštatuje naplnenie podmienok autonómneho doménového práva.

Model národných vlád a práva je charakteristický tým, že stojí na téze, že ak internet zasahuje ako subjekt do spoločenských vzťahov, mal by byť regulovaný štátom, pričom tento model nesie v sebe dve možné cesty, a to reguláciu internetu vládami alebo regulácia obsahu pri otvorenom internete.[19] Ovládanie internetu prvou cestou si vybrala Čína, ktorá reguluje sieť a má monopol kontrolovať a nakladať so všetkými spojeniami smerujúcimi von z krajiny alebo dnu do krajiny. Reguláciu má v kompetencii Ministerstvo priemyslu a informatiky, ktoré funguje ako strážca k globálnemu internetu, povoľuje prístup iba k zopár prevádzkovým kanálom a akéhoľvek porušenie je sankcionované štátom. Druhou cestou je regulácia cez blokovanie IP adries, serverov a stránok s neprípustným obsahom. Tu však vystupuje problém a rozdiel s ďalším modelom, a to ten, že internet nie je navrhnutý, aby zodpovedal kontrole vlády, pretože napríklad číselný systém IP nie je hierarchicky upravený tak, aby vedel poskytnúť informáciu o každej IP adrese. To znamená, že prvý problém je technický,

[14]CINA,J.: Internet liberum: Medzinárodné územné režimy ako vzor úpravy internetu. In Informačná spoločnosť a medzinárodné právo. [cit.16.10.2016]. Dostupné na http://www.upjs.sk/pracoviska/ univerzitna-kniznica/e-publikacia/#prf

[15]Internet nefunguje ako telefónna sieť, tu je možné v akomkoľvek bode do siete zasiahnuť, pri internete je možné blokovať počítače alebo server, ale to nie je záruka, že dáta budú presmerované cez proxy server. Pozri ďalej SOLUM, L.B.: Models of internet governance. Dostupné na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825

[16]Internet Corporation for Assigned Names and Numbers. Pozri ďalej https://www.icann.org/

[17]World Intellectual Property Organization a International Telecommunication Union. Pozri ďalej www.wiro.int a www.itu.int

[18]POLČÁK, R.: Internet a proměny práva. Auditorium: Praha, 2012, s. 131

[19]SOLUM, L. B.: Models of internet governance. [cit.16.10.2016]. Dostupné na https://papers.ssrn.com /sol3/ papers.cfm?abstract_id=1136825

a vymožiteľnosť naráža na technickú stránku veci a druhým problémom je právna povaha, kedy charakter internetu ako globálnej siete prináša otázku personálnej jurisdikcie.[20]
Z uvedeného vyplýva, že geografická delokácia kyberpriestoru je špecifická vzhľadom na to, že technologicky možným prekonaním vzdialenosti dochádza k stretu rôznych účastníkov, kultúr a záujmov, vzniku cezhraničných transakcií, šíreniu myšlienok a konfrontácií názorov, čo spôsobuje, že konania iných účastníkov môžu mať dopad na dianie v krajinách, kde nevznikli a kde tieto konania nie sú povolené, majú iný status právnej ochrany alebo nie sú regulované vôbec, prípadne sa vyznačujú iným faktickým dopadom.[21] A v situácii, ak sa štát snaží regulovať samotnú štruktúru predmetného priestoru alebo prichádza do konfliktu s obsahom, ktorého pôvod je mimo hraníc, naráža na ďalšie problémy, ktoré v súčasnosti vyriešené ešte nie sú.

Model regulácie trhu a ekonomiky poukazuje na to, že i trh si vytvoril vlastný pohľad cez neviditeľnú ruku trhu. Príklad prístup ICANN k doménovému prístupu ilustruje ako sa trh pozerá na internet a na otázku, ktorá sa má klásť pri úprave, a to otázku najväčšieho prínosu pre spoločnosť, najväčšej využiteľnosti, najväčšieho možného prístupu k užívateľom s cieľom poskytnúť čo najviac služieb.[22]

Posledným modelom je model kódu a internetovej architektúry, ktorý vychádza z tézy, že kód je primárny regulátor virtuálneho priestoru a v tejto logike prirovnáva internetovú architektúru k architektúre budov, kde sa síce ľudia môžu pohybovať na základe vlastného uváženia, no primárne sa pohybujú tak, ako im to samotná architektúra budovy dovolí.[23] Čo znamená, že v kyberpriestore sa ľudia môžu správať tak, ako im to štruktúra a kód povoľuje, čím dochádza prirodzene k obmedzeniu prípadných neprípustných činností.

Lex informatica a lex mercartoria
Ako vyplýva z vyššie uvedeného pri realizácii práva na internete sa štát nemôže spoliehať na svoj tradičný monopol násilného donútenia ani na to, čo veda medzinárodného práva verejného označuje ako územnú výsosť. Zrejmou prekážkou efektívnej realizácie práva v realite informačnej spoločnosti je i malá flexibilita právotvorných a právo aplikujúcich štátnych inštitúcií a z nej prameniaca neschopnosť štátu adekvátne reagovať na technologický a spoločenský vývoj. Aktuálna teleologická interpretácia platného práva vzhľadom k praktickej efektivite (tj. interpretácia za využitia argumentu effet utile) v tejto situácií nestačí a namiesto štátu teda potenciál sporných vzťahov na internete stále viac pokrývajú fragmenty paraprávneho - neprávneho poriadku označovaného ako lex informatica.
S konceptom úpravy kyberpriestoru a internetu, ktoré vychádzajú zo stredovekého obchodného práva – lex mercartoria, sa stretávame už v deväťdesiatych rokoch minulého storočia.[24] Hardyho

[20] Vyššie uvedené dva problémy – technický a otázka právnej jurisdikcie sa prejavili v prípade spoločnosti Yahoo!, ktorú zažalovali francúzske organizácie - Liga proti rasizmu a antisemitizmu a Únia francúzskych židovských študentov, za propagáciu nacizmu. Na stránkach Yahoo! totiž prebiehali aukcie s tovarom s nacistickou tématikou, čo je vo Francúzsku protizákonné. Spoločnosť sa bránila, že nedokáže úspešne filtrovať užívateľov IP adries (len 70%). Napriek tomu dali francúzske súdy za pravdu francúzskym organizáciám. Yahoo! následne podala sťažnosť na kalifornský súd, keďže spoločnosť tam mala sídlo, a vtedy sa ukázal druhý problém, pretože kalifornské súdy uznali spoločnosti neoprávnené zásahy do práv francúzskymi súdmi, v spojení s vynucovaním práva mimo francúzskych hraníc.
[21] LIPTÁK, F.: Soft Law a iné mimoprávne refulácie a ich význam pre internet. In Informačná spoločnosť a medzinárodné právo, s. 49. [cit.16.10.2016]. Dostupné na http://www.upjs.sk/pracoviska/univerzitna-kniznica/e-publikacia/#prf
[22] CINA,J.: Internet liberum: Medzinárodné územné režimy ako vzor úpravy internetu. In Informačná spoločnosť a medzinárodné právo, s. 36. [cit.16.10.2016]. Dostupné na http://www.upjs.sk/pracoviska/univerzitna-kniznica/e-publikacia/#prf
[23] SOLUM, L. B.: Models of internet governance. Dostupné na https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825. [cit.14.10.2016]. Pozri ďalej LESSIG, L.: Code, and Other Laws of Cyberspace. New York: Basic Books, 1999.
[24] POLANSKI, P.P.: Towards a supranational Internet law. In Journal of Internal Commercial Law and Technology, Vol 1. Issue 1/2016. [cit. 3.10.2016]. Dostupné na http://heinonline.org/HOL/LandingPage? handle=hein.journals/jcolate1&div=3&id=&page=

Trottera môžeme považovať s najväčšou pravdepodobnosťou za toho, ktorý poukázal na podobnosti stredovekého obchodu a online commerce[25]. Lex mercartoria obsahuje realitu rozvíjajúceho sa obsahu právnych noriem, pravidiel a inštitúcií mimo štátu ako aj inštitútov, a priam romantickú ideu o spontánnej tvorbe práva oddelenej od štátu.

V stredoveku vstupovalo do obchodných vzťahov obdobne ako i dnes množstvo subjektov. Charakteristické pre tieto subjekty však je to, že nejde o tie isté subjekty, ale vždy o iné, a preto pevné zmluvné vzťahy neboli vždy praktické. Stredoveké právo kupcov vychádzalo z autonómnej tvorby práva a riešenie sporov bolo založené na súdoch, kde si strany sporu dobrovoľne vyberali sudcov, ktorí mali dôveru oboch strán a rozhodovali podľa obyčajového práva obchodníckej komunity, rozhodovali podľa zásad dobrého a spravodlivého.[26] Základným prameňom teda boli obchodné zvyklosti.

Ako sme už viackrát uviedli vyššie v texte právne poriadky štátov nedokázali ani pri vzniku kyberpriestoru ani dnes reagovať na nové situácie a rýchlo sa meniace situácie, čo spôsobilo, že v rámci priestoru si subjekty, ktoré vstupovali do rôznych vzťahov, vlastnými pravidlami upravili sporné záležitosti, ktoré bolo potrebné aktuálne riešiť. Pravidlá vznikali prirodzene a spontánne, keďže subjekty spoločenských vzťahov túto úpravu požadujú pre svoje fungovanie a vymedzenie pravidiel, ktoré by transparentne určili ich povinnosti a práva, a tak vymedzili spôsob a princípy svojho fungovania, čím by eliminovali riziká plynúce z právnej neistoty, ktorá je charakteristická pre stav bez úprav, a preto si ich súkromné subjekty vytvárajú autonómne, vlastné súbory pravidiel podľa potrieb vzhľadom na vzniknuté situácie.[27]

Spoločnosť ICANN, ktorá registruje domény a je fundamentálnou súčasťou internetovej štruktúry, má svoje vlastné súbory pravidiel. Jedná sa o súkromnú entitu, ktorá sa vyznačuje samoreguláciou. Ide o non-profit spoločnosť. Obdobne funguje aj spoločnosť IETF, ktorá vyvíja a podporuje internetové štandardy. Venuje sa najmä TCP/IP. Ide o otvorenú spoločnosť, ktorá vydáva štandardy a nevyžaduje žiadne formálne členstvo alebo iné požiadavky. V deväťdesiatych rokoch minulého storočia sa IETF vymanila z područia vlády USA a stala sa nezávislou medzinárodnou organizáciou pridruženou k Internet Society. Obdobne i súkromná spoločnosť Paypal, ktorej pravidlá vypracovala súkromná spoločnosť, vrátane návrhu riešenia sporov.[28]

ICANN ako spoločnosť registrujúca domény má vytvorený vlastný súbor pravidiel jednak hmotnoprávnych, teda pravidlá upravujúce práva a povinnosti, ale i procesné ustanovenia. Hovoríme o online dispute resolution methods – alternatívne riešenia sporov (riešenie doménových sporov, oline arbitráže, online mediácie atď). ICANN prišla s návrhom riešiť doménové spory pravidlami rozhodcovského konania. Výhodou takéhoto riešenia sporu je, že o spore obdobne ako v stredovekom lex mercatoria rozhodujú ľudia, ktorých môžeme považovať za odborníkov a znalcov rozporovanej problematiky. Otázkou, ktorá v tomto momente vyvstáva je, vynuteľnosť dodržiavania predmetných pravidiel, resp. rozhodnutí v rámci alternatívne riešených sporov, teda bez účasti štátneho donútenia. I tu si kyberpriestor našiel svoju cestu a zakladá si na vysokej spoločenskej akceptácii, na hodnotení kvality a spokojnosti. V zásade nie je nutné používať formálne právne postupy a aplikovať legislatívu danej jurisdikcie, pretože spoločná platforma umožňuje prostredníctvom svojich pravidiel odmeňovať poctivé subjekty na základe hodnotení a poškodenie reputácie má ďalekosiahlejší dopad ako napríklad zárobok na nespokojnom zákazníkovi.[29] Aj tu vidíme ďalšiu paralelu so stredovekým lex mercartoria, samoregulácia v rámci uplatňovania pravidiel

[25]POLANSKI, P.P.: Towards a supranational Internet law. In Journal of Internal Commercial Law and Technology, Vol 1. Issue 1/2016. [cit. 3.10.2016]. Dostupné na http://heinonline.org/ HOL/LandingPage? handle=hein.journals/jcolate1&div=3&id=&page=

[26]LIPTÁK, F.: Soft law a iné mimoprávne regulácie a ich význam pre internet. In Informačná spoločnosť a medzinárodné právo. s. 50. [cit. 16.10.2016]. Dostupné na http://www.upjs.sk/ pracoviska/ univerzitna -kniznica/e-publikacia/#prf

[27]Tamže, s. 51

[28]Podmienky riešenia sporu s Paypal. Pozri ďalej http://topobuv.sk/ako-nakupovat-paypal.

[29]LIPTÁK, F.:Soft law a iné mimoprávne regulácie a ich význam pre internet. In Informačná spoločnosť a medzinárodné právo. s. 52. [cit. 16.10.2016]. Dostupné na http://www.upjs.sk/ pracoviska/univerzitna -kniznica/e-publikacia/#prf

hmotnoprávnych, ale i rešpektovanie rozhodnutí kupcovských súdov a sankcií, pretože v prípade ich nedodržania bol tento pochybil spomedzi sudcov vylúčený.
Ako vyplýva z vyššie uvedeného textu paralely medzi stredovekým lex mercartoria a reguláciou kyberpriestoru sú zrejmé, čím vyvstáva otázka, či práve modern cyberlaw lex mercartoria by nebolo tým správnym riešením pre reguláciu kyberpriestoru, predovšetkým na základe zistení, že mnohé zo zásad a princípov stredovekého obchodného práva sa aplikujú dnes v lex informatica, i keď v inom, modernejšom šate. Nespornou výhodou tejto regulácie je to, že v prípadoch, keď štáty nechcú spolupracovať, resp. nemajú záujem vstupovať do všetkých oblastí kyberpriestoru alebo spolupráca nie je reálna, môže práve takýto prístup uľahčiť situáciu a riešiť aktuálne situácie.
S poukazom na uvedené môžeme analógiu medzi lex mercartoria a lex informatica nájsť predovšetkým v nasledujúcich atribútoch: 1. spontánnosť (emergentnosť), dobrovoľnosť a autonómnosť tvorby práva 2. subjekty si volia súbor noriem, ktoré budú aplikovať sami, 3. alternatívne riešenie sporov a arbitrážne súdnictvo, 4. vysoká spoločenská akceptácia a 5. mimo sféry vplyvu štátu.
Na príklade lex mercartoria je možné vzhliadnuť v kyberpriestore prirodzené právo, kde si subjekty bez zásahu štátu sami upravujú vzájomné vzťahy a vytvárajú si súbor pravidiel ako hmotnoprávnych tak i procesnoprávnych, vzhľadom na aktuálne vzniknuté situácie. Táto spontánna tvorba pravidiel sa podobá hayekovskému modelu spontánneho poriadku, kde pravidlá vznikajú spontánne, prirodzene a na báze samoregulácie vznikajú pravidlá v spoločnosti a upravujú jej fungovanie.

5 ZÁVER

V súčasnosti neexistuje centrálna a jediná autorita, ktorá by stanovila, ktoré pravidlá platia alebo majú platiť pre celý kyberpriestor vo všetkých existujúcich spoločenských vzťahoch a zároveň je existencia takejto autority viac menej nereálna, a práve preto je v centre kyberpriestoru evidentná a rozšírená autonómna a súkromná tvorba práva. Výsledkom debát o regulácii kyberpriestoru sú dve oblasti názorov, a to názory, ktoré uprednostňujú samoreguláciu a štátnu reguláciu. Avšak i tieto okruhy v sebe nesú množstvo ďalších otázok, ako napríklad, či sa má samoregulácia týkať celého internetového priestoru alebo budú možné i zásahy jurisdikcie štátu. Objavujú sa však i názory o prepojení samoregulácie internetu s jurisdikciou štátu alebo prepojenie samoregulácie a medzinárodného práva s poukazom na geografický rozmer internetu.
Uvedený stav zároveň poukazuje na fakt, že samoregulácia ani štátny dohľad ako samotné riešenia nestačia. V tom istom čase kedy prebiehajú tieto teoretické a spoločenské debaty o budúcnosti kyberpriestoru, ide kyberpriestor svojou cestou a reaguje na všetky aktuálne otázky tak, že samotné subjekty si volia dobrovoľne súbory pravidiel, ktoré budú aplikovať, pričom tieto pravidlá vznikajú spontánne z potreby úpravy a sú oddelené od jurisdikcie štátu. Zároveň prevládajú pravidlá neštátnej povahy, ktoré i napriek nižšej záväznosti nesmú byť podceňované a zastávajú významné miesto v rámci súčasnej úpravy fungovania kyberpriestoru.

Zoznam použitej literatúry:

Barlow, J.P. Unabhängichkeitserklärung des Cyberspace. Dostupné na http://www.heise.de/tp/artikel/1/1028/1.html

BECKOVÁ, D.: Regulácia internetu na medzinárodnej úrovni – spôsoby, minulosť a budúcnosť, obsah právnej úpravy, regulované vzťahy. In Informačná spoločnosť a medzinárodné právo. s.28 a nasl. Dostupné na http://www.upjs.sk/pracoviska/univerzitna -kniznica/e-publikacia/#prf

Brief history of the internet, Internet society. Dostupné na: <http://www.internetsociety.org/internet/ internet-51/ history-internet/brief-history-internet#LGR66>.
CINA,J.: Internet liberum: Medzinárodné územné režimy ako vzor úpravy internetu. In Informačná spoločnosť a medzinárodné právo. Dostupné na http://www.upjs.sk/pracoviska/univerzitna -kniznica/e-publikacia/#prf

DE VES MESTDAGH,C.N.J. –RIJGERSBERG, R.W.: Internet governance and global self regulation: teoretica and empirical buildings blocks for a general theory of self regulation. Dostupné na http://www.tandfonline.com/doi/abs/10.1080/17521467.2010.11424719

GIBSON,W.: Jak vypálit Chrome. Brno: Návrat, 2004.

GIBSON, W. Neuromancer. Plzeň: Laser,1992.

KRUGER, L.G.: Governance and the Domain Name system: Issues for Congress, April 23,2013. Dostupné na http://www.fas.org/sg/crs/misc/R42351.pdf

Licklider, J. C. R., Clark, W. On-Line Man Computer Communication. AFIPS Conference Proceedings, 1962, č. 21, s. 113 - 128.

LIPTÁK, F.: Soft Law a iné mimoprávne regulácie a ich význam pre internet. In Informačná spoločnosť a medzinárodné právo, s. 49. Dostupné na http://www.upjs.sk/pracoviska/univerzitna -kniznica/e-publikacia/#prf

POLANSKI, P.P.: Towards a supranational Internet law. In Journal of Internal Commercial Law and Technology, Vol 1. Issue 1/2016. Dostupné na http://heinonline.org/HOL/ LandingPage? handle=hein.journals/jcolate1&div=3&id=&page=

POLČÁK,R. – ŠKOP,M. – MACEK, J.: Normatívne systémy v kyberpriestore (úvod do štúdia). Brno: Masarykova univerzita, 2005.

POLČÁK, R.: Internet a proměny práva. Auditorium: Praha, 2012.

ROBERTS, L.-W., S. A Brief history of Internet Dostupné na: http://www.isoc.org/ internet/history/brief.shtml.

ROSENTHAL,D.: Herausforderungen durch die Globalität des Internets: Problemstellung und Lösungsansätze der Praxis. Dostupné na http://www.homburger.ch/fileadmin/ publications /HEFOGLOI.pdf

SEGURA-SERRENO,A.: Internet regulation and the role of International law. Dostupné na http://www.mpil.de/files/pdf3/06_antoniov1.pdf

SOLUM, L. B.: Models of internet governance. Dostupné na https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=1136825

Kontaktné údaje:
Mgr. Andrea Kluknavská, PhD., LL.M.
andrea.kluknavska@flaw.uniba.sk
Právnická fakulta Univerzity Komenského
Šafárikovo námestie č. 6
P. O. BOX 313
810 00 Bratislava

PRÁVOMOC PRI SÚDNYCH SPOROCH OHĽADOM PORUŠENIA PRÁV DUŠEVNÉHO VLASTNÍCTVA NA INTERNETE

Pavel Lacko

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: Due to the main characteristic of the internet which is its „omnipresence“, transnational breaches and violations of intellectual property rights occur relatively often when the breaching party comes or the damage or other harm happen in a country (or countries) different from the domicile of the rightsholder. This article deals with the question of determining in which country such claim should be made in front of a court providing that under the respective circumstances a recovery of claims through court litigation seems effective.

Abstrakt: Vzhľadom na základnú charakteristiku internetu, ktorou je jeho „všadeprítomnosť“, dochádza pomerne často k cezhraničnému porušovaniu a zásahom do práv duševného vlastníctva, kedy porušovateľ pochádza alebo škoda alebo iná ujma nastanú v štáte/štátoch odlišných od sídla (domicilu) nositeľa práv duševného vlastníctva. Príspevok autora sa venuje otázke posúdenia, v ktorom štáte má byť takýto nárok uplatnený na súde za predpokladu, že za daných okolností sa súdne vymáhanie nárokov javí ako efektívne.

Keywords: jurisdiction, intellectual property rights, internet, trade mark, copyright

Kľúčové slová: právomoc, práva duševného vlastníctva, internet, ochranná známka, autorské právo

1 ÚVOD

Vzhľadom na „všadeprítomný“ charakter internetu dochádza jeho prostredníctvom pomerne jednoducho k porušovaniu práv duševného vlastníctva, ktoré má cezhraničný charakter, predovšetkým z dôvodu, že porušenie práv alebo jeho následky nastanú v štáte odlišnom od domicilu porušovateľa.

Pri zvažovaní možnosti vedenia súdneho sporu v súvislosti s porušením práv duševného vlastníctva je samozrejme potrebné posúdiť, či s ohľadom na čas trvania súdneho sporu, majetkové pomery porušovateľa a výšku spôsobenej ujmy má z ekonomického hľadiska význam viesť súdny spor.[1]

Tento príspevok sa venuje prípadom, keď sa na základe posúdenia tejto ekonomickej stránky javí vedenie súdneho sporu ako relevantná možnosť uplatnenia práv ich nositeľa. Za daných okolností je pred posúdením hmotnoprávnej stránky danej veci najprv potrebné stanoviť, súdy ktorého štátu majú právomoc danú vec rozhodovať.

Na úvod je ešte potrebné poznamenať, že tento príspevok sa s ohľadom na jeho obmedzený rozsah zameriava len na niektoré práva duševného vlastníctva, konkrétne ochranné známky a autorské práva, pri ktorých sú zásahy prostredníctvom internetu najobvyklejšie.

2 OCHRANNÉ ZNÁMKY

Prvým aspektom, ktorý je potrebné skúmať v prípade vedenia súdneho sporu s cudzím prvkom je právomoc, teda súdy ktorého štátu majú oprávnenie rozhodovať o danom porušení práv duševného vlastníctva na internete.

[1] Súdnemu sporu obvykle predchádza komunikácia medzi porušovateľom a nositeľom práv ohľadom mimosúdneho riešenia konkrétnej veci, najčastejšie na základe oznámenia o porušení práv duševného vlastníctva a žiadosti o ukončenie ďalšieho porušovania (tzv. *cease and desist letter*) resp. dohody o urovnaní.

Vo vzťahu k ochranným známkach je ohľadom právomoci potrebné rozlišovať medzi ochrannými známkami Európskej únie (ďalej len „ochranná známka EÚ“) a tzv. národnými ochrannými známkami.

2.1 Národné ochranné známky

V prípade národných ochranných známok (ktoré sú zaregistrované pre konkrétny štát) je potrebné vychádzať z ustanovení všeobecných predpisov regulujúcich právomoc. V prípade Slovenskej republiky je týmto predpisom nariadenie Európskeho parlamentu a Rady (EÚ) 1215/2012 z 12. decembra 2012 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach (prepracované znenie) (ďalej len „Nariadenie Brusel I“) a zákon č. 97/1963 Zb. o medzinárodnom práve súkromnom a procesnom v platnom znení (ďalej len „ZoMPS“).

Pokiaľ má porušovateľ domicil[2] v členskom štáte EÚ, aplikuje sa čl. 4 nariadenia Brusel I, v zmysle ktorého je možné (generálnu) právomoc založiť na základe domicilu žalovanej strany. Okrem toho je možné na založenie právomoci aplikovať aj čl. 7(2) nariadenia Brusel I, v zmysle ktorého *„vo veciach nárokov z mimozmluvnej zodpovednosti majú právomoc súdy podľa miesta, kde došlo alebo by mohlo dôjsť ku skutočnosti, ktorá zakladá takýto nárok*“.

V prípade porušenia práv vyplývajúcich z ochrannej známky prostredníctvom internetu podal Súdny dvor Európskej únie (ďalej len „SDEÚ“ alebo „Súdny dvor EÚ“) upresňujúci výklad ohľadom toho, čo je potrebné považovať za miesto, kde došlo alebo by mohlo dôjsť ku skutočnosti, ktorá zakladá nárok z mimozmluvnej zodpovednosti. V prípade *Wintersteiger*[3] si nemecká spoločnosť Products 4U rezervovala kľúčové slovo (AdWord) *Wintersteiger* v rámci internetového reklamného systému, ktorý vyvinula spoločnosť Google. Predmetné kľúčové slovo bolo obmedzené na stránku Google fungujúcu na nemeckej národnej doméne prvej úrovne *google.de*. Pri zadaní výrazu *Wintersteiger* sa v pravej časti obrazovky v rubrike *Anzeige* (reklamy) zobrazila aj reklama spoločnosti Products 4U. Majiteľom ochrannej známky *Wintersteiger* však bola rakúska spoločnosť Wintersteiger. Predmetnú ochrannú známku mala zaregistrovanú len ako národnú ochrannú známku v Rakúsku. Spoločnosť Wintersteiger podala žalobu na zdržanie sa konania na rakúske súdy, pričom tvrdila, že spoločnosť Products 4U uvedením reklamy na stránke *google.de* porušila jej práva k rakúskej ochrannej známke. Pokiaľ ide o právomoc rakúskych súdov rozhodnúť o danej žalobe, spoločnosť Wintersteiger sa odvolala na článok 5 bod 3 nariadenia č. 44/2001.[4] Uviedla totiž, že stránka google.de je dostupná aj z Rakúska a výsledky vyhľadávania sú v nemeckom jazyku. Uvedený prípad sa dostal až pred rakúsky najvyšší súd, ktorý si v súvislosti s touto vecou položil otázku, za akých okolností môže reklama prostredníctvom používania rakúskej ochrannej známky *Wintersteiger* na internetovej stránke, ktorá pôsobí na národnej doméne prvej úrovne *.de* založiť podľa predmetného ustanovenia Nariadenia Brusel I právomoc rakúskych súdov rozhodnúť o žalobe na zdržanie sa používania rakúskej ochrannej známky.

SDEÚ sa priklonil k záveru, že pokiaľ ide o miesto vzniku mimozmluvnej zodpovednosti, *„ochrana vyplývajúca zo zápisu národnej ochrannej známky sa v zásade obmedzuje na územie členského štátu zápisu, takže jej majiteľ sa spravidla nemôže dovolávať ochrany mimo územia daného štátu“*.[5] *„Keď ide o právomoc rozhodnúť o tvrdeniach, že došlo k porušeniu práv k národnej ochrannej známke, treba zobrať do úvahy, že sledovaný cieľ predvídateľnosti pravidiel, ako aj riadna správa vecí verejných svedčia vzhľadom na kritérium miesta vzniku škody [presnejšie, mimozmluvnej zodpovednosti, pozn. autora] v prospech priznania právomoci súdom členského štátu, v ktorom je dotknuté právo chránené... Tieto súdy sú oprávnené rozhodovať o náhrade celej škody údajne spôsobenej majiteľovi chráneného práva z dôvodu jeho porušenia, ako aj o žalobe na zdržanie sa akéhokoľvek zásahu do uvedeného práva.“*[6]

---

2 Pojem domicil je definovaný v čl. 62 a 63 Nariadenia Brusel I. Pre bližšie objasnenie pozri napr. LACKO, P. Nariadenie Brusel I (prepracované znenie): Komentár, str. 252 a nasl.

3 C-523/10 Wintersteiger AG proti Products 4U Sondermaschinenbau GmbH ECLI:EU:C:2012:220.

4 V súčasnosti čl. 7(2) Nariadenia Brusel I.

5 C-523/10 Wintersteiger AG proti Products 4U Sondermaschinenbau GmbH ECLI:EU:C:2012:220, bod 25.

6 Tamže, bod 27 a 28. Pre úplnosť je potrebné dodať, že Súdny dvor EÚ sa zaoberal aj otázkou, kde sa nachádza „miesto, kde nastala skutočnosť, ktorá mala za následok vznik škody“, pričom došiel k záveru, že ide o členský štát, v ktorom je usadený inzerent (používajúci príslušné kľúčové slovo).

V prípade zásahu do práv z národnej ochrannej známky je teda možné porušovateľa žalovať buď v štáte jeho domicilu alebo na súdoch štátu, kde je predmetná ochranná známka registrovaná. V tejto súvislosti je však potrebné upozorniť na skutočnosť, že právomoc súdu v mieste registrácie ochrannej známky ešte neznamená, že súd v danom prípade (na základe hmotnoprávneho posúdenia veci) dôjde k záveru, že skutočne došlo k zásahu do práv vyplývajúcich z ochrannej známky. Ako vyplýva z teritoriálneho charakteru ochranných známok, ochrana je obmedzená len na územie štátu registrácie a nositeľ teda musí preukázať, že k zásahu došlo na tomto území.

Pre úplnosť je potrebné poznamenať, že pokiaľ porušiteľ nemá domicil v členskom štáte EÚ, je na určenie právomoci slovenských súdov potrebné použiť príslušné ustanovenie ZoMPS, konkrétne § 37b písm. a), v zmysle ktorého *„vo veciach nárokov na náhradu škody z iného ako zmluvného vzťahu, ak ku skutočnosti, ktorá zakladá nárok na náhradu škody, došlo alebo by mohlo dôjsť na území Slovenskej republiky“*. Napriek tomu, že uvedené ustanovenie je obmedzené na vznik škody (a nezahŕňa akúkoľvek inú formu mimozmluvnej zodpovednosti), záver by mal byť rovnaký, ako v prípade *Wintersteiger* a právomoc by mali mať slovenské súdy, pokiaľ je ochranná známka na Slovensku registrovaná.

2.1.1 Výlučná právomoc

Pre úplnosť je potrebné spomenúť aj výlučnú právomoc v zmysle čl. 24(4) Nariadenia Brusel I. V zmysle tohto ustanovenia platí, že *„v konaniach týkajúcich sa registrácie alebo platnosti patentov, ochranných známok, priemyselných vzorov alebo iných obdobných práv, ktoré sa musia registrovať alebo pri ktorých sa musí žiadať o ochranu, a to bez ohľadu na to, či je táto otázka predmetom žaloby alebo obrany proti žalobe, súd členského štátu, v ktorom sa žiadosť o registráciu alebo ochranu podala, v ktorom sa registrácia alebo ochrana poskytli, alebo v ktorom sa podľa právneho nástroja Únie alebo medzinárodného dohovoru za poskytnuté považujú.“*

Pokiaľ je teda predmetom konania registrácia alebo platnosť ochranných známok (alebo iných práv duševného vlastníctva, ktoré podliehajú registrácii), výlučnú právomoc rozhodovať o tejto spornej otázke majú výlučne súdy členského štátu miesta registrácie. Dôležité je upozorniť, že čl. 24(4) sa vzťahuje výlučne na spory týkajúce sa registrácie a platnosti a nepoužije sa v prípade sporov ohľadom porušenia týchto práv.

2.2 Ochranné známky Európskej únie

V prípade ochranných známok EÚ je právomoc (vo veciach porušenia práv vyplývajúcich z týchto ochranných známok) upravená v osobitnom predpise, a to nariadení Rady (ES) č. 207/2009 z 26. februára 2009 o ochrannej známke Európskej únie (kodifikované znenie) (ďalej len „Nariadenie 207/2009“). V zmysle čl. 97 tohto nariadenia sa uplatňuje tzv. kaskádový systém určenia právomoci, v zmysle ktorého je právomoc súdov stanovená nasledovne: *„Konania vo veci príslušných žalôb a návrhov uvedených v článku 96 prebiehať na súdoch toho členského štátu, v ktorom má odporca trvalý pobyt,*[7] *alebo pokiaľ nemá trvalý pobyt v žiadnom členskom štáte, potom v tom, v ktorom má podnik. Ak odporca nemá ani trvalý pobyt, ani podnik v žiadnom členskom štáte, budú takéto konania prebiehať na súdoch členského štátu, v ktorom má trvalý pobyt žalobca, alebo ak nemá trvalý pobyt v žiadnom členskom štáte, potom v tom, v ktorom má podnik. Ak nemá takýto trvalý pobyt ani takýto podnik odporca ani žalobca, budú takéto konania prebiehať na súdoch toho členského štátu, v ktorom má svoje sídlo úrad.“*

Nariadenie 207/2009 teda stanovuje postupne päť kritérií v konkrétnom poradí, na základe ktorých je možné určiť právomoc, pričom každé nasledujúce kritérium sa uplatní, pokiaľ nie je možné použiť predchádzajúce kritérium.

Je zároveň potrebné upozorniť na osobitné kritérium pre založenie právomoci v zmysle čl. 97(5), podľa ktorého konania o príslušných žalobách a návrhoch, okrem žalôb na určenie, že nedochádza k porušovaniu ochrannej známky EÚ *„sa môžu uskutočniť aj pred súdmi toho členského štátu, na ktorého území došlo k porušeniu alebo hrozí, že k nemu dôjde“*.

Právomoc členského štátu, kde je usadený inzerent (jeho domicil) vyplýva už z čl. 4 Nariadenia Brusel I. Predmetný výklad teda neposkytuje nositeľovi práv možnosť žalovať porušiteľa v inom členskom štáte, ktorý by nevyplýval už z ustanovenia čl. 4.

[7] V tomto prípade by namiesto pojmu „trvalý pobyt“ bolo vhodnejšie použiť pojem „domicil“, a to aj vzhľadom na iné jazykové verzie nariadenia 207/2009.

V tejto súvislosti je potrebné dodať, že nariadenie 207/2009 uplatňuje ohľadom rozsahu právomoci obdobný (tzv. mozaikový) systém, ku ktorému sa dopracoval Súdny dvor EÚ v prípade *Shevill*.[8] Predmetný mozaikový systém je založený na princípe, že pokiaľ je právomoc založená na prvých piatich „kaskádových" kritériách (v zmysle čl. 97(1-4)) má stanovený súd právomoc rozhodovať o porušení, ku ktorému došlo alebo hrozí, že k nemu dôjde na území ktoréhokoľvek členského štátu. Ak je však právomoc založená na čl. 97(5), určený súd má právomoc iba vzhľadom na skutky spáchané alebo skutky, ktoré hrozia na území toho členského štátu, v ktorom sa daný súd nachádza.

Súdny dvor EÚ sa zatiaľ priamo nevyjadril k otázke, ktorý súd by mal mať právomoc v zmysle čl. 97(5) nariadenia č. 207/2009. V tejto súvislosti nie je možné použiť pravidlo stanovené v prípade *Wintersteiger*, v zmysle ktorého majú právomoc súdy štátu, v ktorom je ochranná známka zapísaná. Ochranná známka EÚ je totiž „zapísaná" pre všetky členské štáty a pripustiť možnosť právomoci súdov všetkých členských štátov by bolo jednak príliš rozsiahle a zároveň by to vo veľkej miere oslabovalo právnu istotu dotknutých strán, ktoré by nevedeli predpovedať, v ktorom členskom štáte môže byť podaná príslušná žaloba. Ohľadom otázky právomoci v prípade porušenia ochrannej známky EÚ prostredníctvom internetu by však bolo možné aplikovať princípy, o ktorých bolo rozhodnuté v súvislosti s porušením práv z ochranných známok v „offline" svete, teda mimo internetu. SDEÚ v tejto súvislosti v prípade *Coty*[9] rozhodol, že pojem územie členského štátu, v ktorom bol akt porušenia spáchaný alebo hrozí[10] je potrebné vykladať autonómne vo vzťahu k pojmu „miesto, kde došlo alebo by mohlo dôjsť ku skutočnosti, ktorá zakladá… nárok na náhradu škody"[11]. Inými slovami povedané, napriek tomu, že aj nariadenie 207/2009 (ktoré reguluje právomoc vo vzťahu k ochranným známkam EÚ) aj nariadenie Brusel I (ktoré reguluje právomoc vo všeobecnosti vo všetkých občianskych aj obchodných veciach) umožňujú založiť právomoc súdu na základe kritéria, ktoré súvisí zo vznikom škody, nie je možné obsah týchto ustanovení navzájom zamieňať. Súd vo svojom ďalšom výklade zároveň uviedol, že *„väzba sa viaže na aktívne konanie osoby, ktorá je pôvodcom tohto porušenia. Preto väzba uvedená v tomto ustanovení zahŕňa územie členského štátu, v ktorom udalosť, ktorá je základom údajného porušenia, bola spáchaná alebo hrozí, a nie územie členského štátu, v ktorom nastali účinky tohto porušenia."*[12] Výklad ustanovenia o založení právomoci v zmysle čl. 97(5) nariadenia 207/2009 je teda užší a právomoc sa viaže výlučne na udalosť, ktorej následkom bol vznik škody (resp. iného druhu mimozmluvnej zodpovednosti) a nie na škodu ako takú. Rozhodujúce je teda miesto konania a nie miesto, v ktorom nastal následok takéhoto konania.

Pokiaľ závery rozhodnutia vo veci *Coty* extrapolujeme do „online sveta", mala by byť právomoc na základe tohto ustanovenia založená len na základe tej skutočnosti, v ktorom členskom štáte porušiteľ konal bez ohľadu na to, kde nastal následok takéhoto konania. Je zrejmé, že takýto výklad neprispieva k účinnému bráneniu voči porušovaniu práva, keďže v praxi nie je jednoduché zistiť a dokázať „odkiaľ" porušiteľ konal. Navyše, takéto miesto je častokrát jedným z miest v zmysle čl. 97(1-2), kedy je právomoc možné založiť na niektorom z týchto ustanovení a čl. 97(5) teda nijakým spôsobom nerozširuje možnosti nositeľa práv, ohľadom členských štátov, v ktorých je možné podať na porušovateľa žalobu.

Na záver je možné dodať, že *de lege ferenda* by bolo možné uvažovať o právomoci založenej na mieste porušenia práv vyplývajúcich z ochranných známok EÚ, ktoré by sa viazalo na miesto, kde bola aktivita porušovateľa smerovaná, obdobne ako je to v prípade právomoci pri spotrebiteľských zmluvách v zmysle čl. 17(1)(c) nariadenia Brusel I. V takom prípade by stačilo skúmať, na ktorý členský štát (alebo členské štáty) sa porušiteľ pri svojej aktivite zameriava (a to napr. na základe použitého jazyka, meny, miesta doručenia tovaru a pod.). Avšak dokým nebude podaný iný výklad SDEÚ, ktorým by sa odklonil od interpretácie v rozhodnutí *Coty*, je potrebné pridržiavať sa záverov uvedených vyššie a skúmať miesto konania porušiteľa, prípadne využiť kaskádový systém pre založenie právomoci v zmysle čl. 97(1-4) nariadenia 207/2009.[13]

---

8 Vec C-68/93 *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd proti Presse Alliance SA* [1995] ECR I-415.

9 Vec C-360/12 Coty Germany GmbH proti First Note Perfumes NV, ECLI:EU:C:2015:485.

10 Ide o ustanovenie, ktorému v súčasnosti zodpovedá čl. 97(5) nariadenia 207/2009.

11 Predmetnému ustanoveniu v súčasnosti zodpovedá čl. 7(2) Nariadenia Brusel I.

12 Vec C-360/12 Coty Germany GmbH proti First Note Perfumes NV, ECLI:EU:C:2015:485, bod 34.

13 Rovnaký záver bol vyjadrený aj v článku ROSATI, E. International Jusridiction in Online EU Trade Mark Infrigement Cases: Where is the Place of Infringement Located? s. 488 a nasl.

3 AUTORSKÉ PRÁVO

Vo vzťahu k porušeniu autorských práv je potrebné poznamenať, že rovnako ide o mimozmluvnú zodpovednosť, na ktorú sa aplikuje čl. 7(2) Nariadenia Brusel I, v zmysle ktorého majú právomoc súdy toho štátu, v ktorom buď došlo k udalosti, ktorá má za následok vznik mimozmluvnej zodpovednosti alebo došlo k samotnému následku (najčastejšie škode) ako dôsledku tejto mimozmluvnej zodpovednosti. Nositeľ práv má samozrejme možnosť žalovať porušovateľa aj v mieste jeho domicilu podľa čl. 4 Nariadenia Brusel I. Vo vzťahu k zásahu do autorských práv prostredníctvom internetu zostáva otvorená otázka, kde sa nachádza príslušné miesto v zmysle čl. 7(2).

Touto otázkou sa zaoberal SDEÚ v prípade *Pinckney*.[14] V danej veci pán Pinckney, ktorý mal domicil vo Francúzsku, tvrdil, že je autorom, skladateľom a interpretom dvanástich piesní nahraných skupinou Aubrey Small na gramofónovú platňu. Pán Pinckney zistil, že tieto piesne boli bez jeho súhlasu nahrané na CD vylisované spoločnosťou Mediatech v Rakúsku a následne predávané britskými spoločnosťami na rôznych internetových stránkach prístupných z miesta jeho domicilu (Francúzsko). Následne podal pán Pinckney na spoločnosť Mediatech vo Francúzsku žalobu, ktorou sa domáhal náhrady škody vzniknutej zásahom do jeho autorských práv. Mediatech namietala právomoc francúzskych súdov. Prípad sa dostal až pred kasačný súd, ktorý predložil prejudiciálnu otázku Súdnemu dvoru EÚ týkajúcu sa právomoci v takomto prípade. Otázkou bolo, či sa súd prikloní k princípu aplikovanému pri zásahu do osobnostných práv, v zmysle ktorého môže obeť podať žalobu na súd podľa miesta, kde sa nachádza centrum jej záujmov, pričom daný súd môže rozhodovať o celkovej škode (teda aj o tej, ktorá nastala mimo štátu, kde sa vedie konanie). *„Miestom, kde má osoba centrum svojich záujmov, je vo všeobecnosti miesto jej obvyklého pobytu. Osoba však môže mať centrum svojich záujmov aj v členskom štáte, v ktorom nemá obvyklý pobyt, pokiaľ môžu iné indície, ako napríklad výkon povolania, preukázať zvlášť úzku väzbu k tomuto štátu.“*[15] Druhou alternatívou bolo, že sa uplatní princíp použitý pri zásahu do práv vyplývajúcich z národných ochranných známok, podľa ktorého majú právomoc súdy členského štátu, v ktorom je dané právo duševného vlastníctva chránené, ktoré môžu najlepšie posúdiť, či naozaj došlo k zásahu do predmetného práva.

Súd sa nakoniec priklonil k druhej spomenutej interpretácii, ktorá akcentuje na teritoriálny charakter ochrany autorského práva. Na základe toho majú súdy právomoc rozhodovať len o škode (alebo inej ujme založenej na mimozmluvnej zodpovednosti) spôsobenej na území členského štátu, v ktorom sa tento súd nachádza.[16]

V prípade zásahu do autorských práv prostredníctvom internetu sa teda uplatní tzv. mozaikový princíp, v zmysle ktorého majú súdy v súlade s čl. 7(2) Nariadenia Brusel I právomoc rozhodovať vždy len o škode spôsobenej na území členského štátu, kde sa tento súd nachádza. Pokiaľ má nositeľ práva záujem, aby v jednom konaní bolo rozhodnuté o celom rozsahu ujmy (bez ohľadu na to, kde táto ujma vznikla), je potrebné porušovateľa žalovať v štáte jeho domicilu. Samotná ujma je pritom založená najčastejšie na skutočnosti, že tretie osoby si zaobstarajú prostredníctvom internetovej stránky prístupnej v obvode súdu, ktorý začal konanie, rozmnoženinu diela, ku ktorému sa viažu práva, ktorých sa domáha žalobca.

Pre poriadok je ešte potrebné dodať, že v prípade, ak žalovaný nemá domicil v členskom štáte, uplatní sa § 37b písm. a) ZoMPS, a to za rovnakých podmienok, ako je opísané v bode 2.1 vyššie. Je potrebné zdôrazniť, že aj v tomto prípade bude právomoc slovenského súdu obmedzená na škodu, pričom ostatné následky mimozmluvnej zodpovednosti nie sú spomenutým ustanovením pokryté.

4 ZÁVER

K porušovaniu práv duševného vlastníctva (najmä ochranných známok a autorských práv) na internete dochádza veľmi často. Pokiaľ je v konkrétnom prípade ekonomické viesť súdny spor, môže sa žalobca rozhodnúť, v ktorom štáte podá žalobu, a to predovšetkým s ohľadom na pravidlá popísané vyššie súvisiace s domicilom žalovaného a miesta, kde je dané právo duševného vlastníctva chránené.

---

[14] Vec C-170/12 Peter Pinckney proti KDG Mediatech AG ECLI:EU:C:2013:635.

[15] C-509/09 eDate Advertising GmbH proti X a C-161/10 Olivier Martinez a Robert Martinez proti MGN Limited [2011] ECR I-10269, bod 52.

[16] DICKINSON, A.; LEIN, E.: The Brussels I Regulation Recast. s. 170-171.

Záleží na okolnosti konkrétneho prípadu, ktoré z možných alternatív právomoci si žalobca zvolí. S ohľadom na aktuálnu interpretáciu relevantných predpisov sa ako najschodnejší javí postup (minimálne v prípade porušenia autorského práva a ochranných známok EÚ), v zmysle ktorého je porušovateľ žalovaný v mieste jeho domicilu, a to z dôvodu, že v danom mieste je možné požadovať náhradu komplexnej ujmy bez ohľadu na to, kde vznikla.

Použitá literatúra:

DICKINSON, A.; LEIN, E.: The Brussels I Regulation Recast. Oxford: Oxford University Press, 2015. 572 s. ISBN 978-0198714286.
LACKO, P.*:* Nariadenie Brusel I (prepracované znenie): Komentár. Bratislava: Wolters Kluwer, 2016. 340 s. ISBN 978-80-8168-438-8.
ROSATI, E. International Jusridiction in Online EU Trade Mark Infrigement Cases: Where is the Place of Infringement Located? In: European Intellectual Property Review, 2016, č. 38(8) s. 482-491.

Kontaktné údaje:

JUDr. Pavel Lacko, LL.M.
pavel.lacko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

REKLAMA NA INTERNETE V KONTEXTE DAŇOVO UZNATEĽNÝCH VÝDAVKOV

Peter Lukáčka, Matej Smalik

Univerzita Komenského v Bratislave, Právnická fakulta

Abstrakt: Reklama na internete v súčasnosti zažíva značný progres, ktorý nie je porovnateľný s iným obdobím v histórii reklamy. Tento fakt je ovplyvnený skutočnosťou, že práve v podmienkach internetu je reklama mnohonásobne účinnejšia a efektívnejšia ako iné tzv. „*klasické*“ formy reklamy. Tento spôsob reklamy však otvára pomerne široký priestor pre porušovanie právnych predpisov v sfére daňového práva. Z tohto dôvodu sa autori zameriavajú v príspevku na posudzovanie rizík pri preukazovaní daňovo uznateľných výdavkov reklamy na internete ako aj v oblasti tzv. rozloženia dôkazného bremena v daňovom konaní.

Kľúčové slová: reklama, internet, dane, výdavok na reklamu

Abstract: Advertising on the Internet is currently experiencing significant progress, which is not comparable with other periods in the history of advertising. This is influenced by the fact that advertising on Internet is many times more efficient and effective than other so-called "Classical" forms of advertising. On the other hand this method of advertising opens a wide space for violation of legislation in the sphere of tax law. For this reason, the authors focus in the article on the risk assessment of tax-deductible expenses of advertising on the Internet as well as on the so-called allocation of the burden of proof in tax proceedings.

Keywords: advertising, internet, taxes, expenditure on advertising

1 ÚVOD

V súčasnosti je reklama pomerne rýchlo rozvíjajúcou sa oblasťou, ktorá má svoje výrazné osobitosti v porovnaní s inými formami realizácie resp. činnosti podnikateľa a zároveň je dôležitým faktorom, ktorý do značnej miery determinuje uplatnenie sa podnikateľa z hľadiska dosiahnutia jeho podnikateľského zámeru. Zároveň reklama významne ovplyvňuje jeden z primárnych cieľov podnikateľa, ktorým je dosahovanie zisku. Špecifickou sférou reklamy je práve jej realizácia v prostredí internetu. Vzhľadom na skutočnosť, že internet je možné vnímať nie len ako verejne dostupný celosvetový systém vzájomne prepojených počítačových sietí bez právnej subjektivyti, ale taktiež aj ako nový kultúrny priestor, kde sa čoraz viac odohráva politický, rodinný ako aj profesijný život jednotlivca[1] je nevyhnutné, aby aj v týchto nových podmienkach pomerne výraznej anonymity boli dodržiavané pravidlá, ktoré sa pre tento druh reklamy vyžadujú príslušnými právnymi predpismi[2] a rovnako je potrebné zamerať pozornosť na oblasť daňových predpisov[3], ktorých aplikácia v prípade reklamy na internete skrýva viaceré úskalia, ktoré bližšie analyzujeme v tomto príspevku.

[1] Bližšie pozri: HUSOVEC, M.: Zodpovednosť na internete podľa českého a slovenského práva. Praha: CZ.NIC, z. s. p., o., 2014, s. 31

[2] napr.: Zákon č. 147/2001 Z. z. o reklame a o zmene a doplnení niektorých zákonov; zákon č. 351/2011 Z. z. o elektronických komunikáciách; zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. a pod.

[3] napr.: Zákon č. 595/2003 Z. z. o dani z príjmov; zákon č. 222/2004 Z. z. o dani z pridanej hodnoty; zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov a pod.

2 REKLAMA NA INTERNETE

Tak ako sme už naznačili, je reklama v priestore internetu najrýchlejšie sa rozvíjajúcou formou reklamy, ktorej pravidlá sa vyvíjajú spolu s rozvojom technológií, ktorých je významnou súčasťou, ba niekedy je práve reklama dôvodom ich vzniku (hry, aplikácie a pod.). Význam reklamy je ovplyvnený skutočnosťou, že práve v podmienkach internetu je reklama účinnejšia a efektívnejšia ako iné tzv. „*klasické*" formy reklamy v rozhlasových, printových prípadne iných médiách. Táto skutočnosť vyplýva z možností prostredia v ktorom sa tento druh reklamy realizuje a zároveň zo špecifického spôsobu jej realizácie.
V tejto súvislosti je možné jednoznačne vnímať jej komparatívne výhody oproti klasickej forme reklamy, ako:

- **adresnosť** – možnosť zamerať reklamu na okruh subjektov identifikovaných na základe ich individuálnych znakov resp. preferencií,
- **interaktivita reklamy a umožnenie priamej realizácie obchodu s cieľovou skupinou** – prepojenie s internetovým obchodom podnikateľa,
- **flexibilita** – zmeny resp. úpravy reklamnej kampane počas jej realizácie,
- **permanentnosť** – je dostupná s možnosťou realizácie 24/7,
- **umožňuje realizáciu aj pri nižšej finančnej náročnosti** – najmä vo vzťahu k začínajúcim podnikateľom to môže byť významnou výhodou.

Z uvedených skutočností je možné vyvodiť záver, že práve tento druh reklamy je pre podnikateľov zaujímavý a je pravdepodobné, že tento záujem ako aj objem prostriedkov investovaných do internetovej reklamy bude v budúcnosti narastať.

Pre správne pochopenie realizácie reklamy na internete je nevyhnutné jednoznačne identifikovať jej najčastejšie formy a rovnako aj činnosti prostredníctvom ktorých dochádza k jej efektívnej realizácii.
V tejto súvislosti je možné hovoriť o tzv.:

Copy Writing - vytvorenie textu a jeho editácia:
Je tvorba reklamných textov a popisu k výrobkom alebo službe. Tento text slúži na to, aby zaujal jeho adresáta, ktorému je určený a taktiež slúži na to, aby si daný výrobok vedel podnikateľ zaradiť v rámci internetového obchodu. Na základe týchto textov ich adresáti získajú základné informácie o:
- výrobku/produkte, či službe,
- funkcii výrobku,
- technických parametroch a iné.

Takýto popis vytvára všeobecne povedomie o výrobku, službe, spoločnosti a ich adresáti sa o ňom dozvedajú a v podvedomí sa im vytvára záujem o danú ponuku. V tomto kontexte ide o významnú súčasť realizácie reklamy na internete.

Spracovanie grafiky:
Predstavuje vyhotovenie fotografií výrobku, prípadne vhodného obrázku pre propagovanie služby. Všetky výrobky, ktoré chce podnikateľ reklamovať musí mať najskôr náležite graficky spracované. Pre potreby spracovania vhodnej grafiky výrobku je nevyhnutné vyhotovovať fotografie v rôznych pohľadoch, tak aby bolo čo najlepšie vidieť a zobraziť daný produkt tak, aby adresát získal o propagovanom produkte, čo možno najpodrobnejšie informácie.

Po uskutočnení vyššie uvedených základných činností (ktoré bývajú často-krát dopĺňané o ďalšie sofistikované práce) môže podnikateľ pristúpiť k jej realizácii a to rôznymi spôsobmi. Najbežnejšími z nich sú

Direct mailing :
Je priamy marketing, ktorého podstatou je zaslanie e-mailu konkrétnej osobe. Táto funkcia umožňuje poslať reklamnú ponuku, obrázok, text, katalóg. Každý jeden adresát, ktorý využíva e-mailovú schránku, tak určite takéto e-maily dostáva pravidelne. Sú rôzne, informujú o tom, že na trhu je nový produkt alebo ponúkajú danú službu, prípadne sa snažia o smerovanie jeho adresáta priamo do

inernetového/kamnného obchodu podnikateľa. Táto služba môže byť z objektívnych dôvodov (najmä v prípadoch ak sa jedná o databázy klientov v desiatkach tisíc e-mailových adries) realizovaná výlučne prostredníctvom spoločnosti, ktorá sa na tieto služby špecializuje a to najmä vzhľadom na pomerne značnú technickú náročnosť.

Platba za kliknutie (PPC/CPC)

Podstatou tohto spôsobu internetovej reklamy je, že podnikateľ platí prevádzkovateľovi tejto služby, nie za zobrazenie reklamy na určitej stránke, ale až za to, že adresát reklamy „*klikne*" na zobrazovanú reklamu. Tento systém funguje na princípe aukcie - kto je ochotný zaplatiť za kliknutie (návštevu propagovanej stránky) najviac, toho inzerát bude zobrazený na prvej pozícii.

Platba za zobrazenie (CPM)

Podstatou tohto spôsobu realizácie reklamy na internete je v tom, že podnikateľ (t.j. ten kto prezentuje svoj výrobok/službu na internete) platí prevádzkovateľovi tejto služby za 1000 zobrazení určitého inzerátu a to bez ohľadu na to, či na inzerát aj niekto „klikne" (vzbudí u neho záujem) alebo nie.

Vyššie uvedené spôsoby reklamy sú realizované spravidla na sociálnych sieťach resp. prostredníctvom spoločností, ktoré prevádzkujú internetové prehliadače a pod. a proces nastavenia tejto reklamy tak, aby bola, čo možno najefektívnejšia, je v podstate veľmi náročnou disciplínou, ktorej sa venujú osobitné podnikateľské subjekty, ktoré poskytujú v tejto oblasti poradenstvo a podporu.

3 ROZLOŽENIE DÔKAZNÉHO BREMENA V DAŇOVOM KONANÍ

Vzhľadom na špecifické podmienky a požiadavky realizácie reklamy na internete, je možné činnosť smerujúcu k dosiahnutiu, čo najvyššej miery efektívnosti z hľadiska vynaložených finančných prostriedkov označiť ako vysoko-sofistikovanú činnosť, pri ktorej nie je možné hovoriť o jej realizácii obvyklým spôsobom tak, ako je tomu pri iných druhoch reklamy. Z tohto dôvodu pomerne často dochádza k objednaniu si týchto reklamných činností dodávateľským spôsobom - prostredníctvom iného subjektu (napr.: prostredníctvom zmluvy o dielo, prípadne formou nepomenovanej zmluvy podľa zákona č. 513/1991 Zb.), ktorý má profesionálne zázemie na uskutočnenie vyššie uvedených činností. Zabezpečenie týchto služieb dodávateľským spôsobom spolu s priamymi výdavkami, ktoré je potrebné vynaložiť na reklamu, môžu predstavovať pomerne značné objemy finančných prostriedkov, ktoré významne ovplyvňujú aj daňové základy podnikateľov. Na tejto situácii (daňový výdavok a následné zníženie daňového základu) by nemalo byť nič zaujímavé resp. podozrivé, avšak problém môže nastať pre objednávateľa reklamy v prípade, ak ho daňový úrad (spravidla pri kontrole) požiada nie len o zdokladovanie skutočnosti, že za reklamné služby zaplatil (faktúry, prevodné príkazy a pod.), ale bude požadovať aj preukázanie toho, že reklama za ktorú bolo platené, bola aj jednoznačne realizovaná s odôvodnením, že je na daňovníkovi, aby preukázal, že ním deklarované/vynaložené finančné prostriedky (ako daňové výdavky) boli použité v súlade s:

- § 2 písm. i) zákona o dani z príjmov, t.j. daňovým výdavkom je výdavok (náklad) na dosiahnutie, zabezpečenie a udržanie zdaniteľných príjmov preukázateľne vynaložený daňovníkom, zaúčtovaný v účtovníctve daňovníka alebo zaevidovaný v evidencii daňovníka podľa *§ 6 ods. 11*, pričom pri využívaní majetku, ktorý môže mať charakter osobnej potreby a s ním súvisiacich výdavkov (nákladov), je daňový výdavok uznaný len v pomernej časti podľa *§ 19 ods. 2 písm. t)*, v akej sa používa na dosiahnutie, zabezpečenie a udržanie zdaniteľných príjmov, ak tento zákon neustanovuje inak,

a

- § 19 ods.2 písm. k) zákona o dani z prímov t. j. výdavky boli vynaložené na účel prezentácie podnikateľskej činnosti daňovníka, tovaru, služieb, nehnuteľností, obchodného mena, ochrannej známky, obchodného označenia výrobkov a iných práv a záväzkov súvisiacich s činnosťou daňovníka so zámerom dosiahnutia, zabezpečenia, udržania alebo zvýšenia príjmov daňovníka,

a

- zároveň v zmysle § 21 ods.1 písm. e) zákon o dani z príjmov sa vyžaduje, aby takto vynaložené náklady neboli v rozpore so zákonom o reklame.

Tzn. aj výdavok na reklamu na internete musí byť

- vynaložený na účel prezentácie podnikateľskej činnosti daňovníka, tovaru, služieb, nehnuteľností, obchodného mena, ochrannej známky, obchodného označenia výrobkov a iných práv a záväzkov súvisiacich s činnosťou daňovníka.
- vynaložený so zámerom dosiahnutia, zabezpečenia, udržania alebo zvýšenia príjmov daňovníka.
- realizovaný v súlade so základnými požiadavkami na reklamu podľa zákona o reklame.

Ak sú výdavky na reklamu vynaložené v súlade s uvedenými podmienkami, potom tieto výdavky by mali byť daňovo uznané v plnej výške bez ohľadu na formu uskutočnenia reklamy, t.j. aj v rámci jej realizácie na internete.

Uvedené sa zdá byť jasné a zrozumiteľné a dovolíme si uviesť, že aj spravodlivé. Domnievame sa však, že uvedené môžu komplikovať ďalšie ustanovenia zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov, ktorým sa riadi správa daní a rovnako sa aplikujú pri výkone daňovej kontroly:

§ 3

(3) **Správca dane hodnotí dôkazy podľa svojej úvahy**, a to každý dôkaz jednotlivo a všetky dôkazy v ich vzájomnej súvislosti, pritom prihliada na všetko, čo pri správe daní vyšlo najavo.

(6) Pri uplatňovaní osobitných predpisov pri správe daní sa berie do úvahy skutočný obsah právneho úkonu alebo inej skutočnosti rozhodujúcej pre zistenie, vyrubenie alebo vybratie dane. **Na právny úkon alebo inú skutočnosť rozhodujúcu pre zistenie, vyrubenie alebo vybratie dane, ktoré nemajú ekonomické opodstatnenie a ktorých výsledkom je účelové obchádzanie daňovej povinnosti alebo získanie takého daňového zvýhodnenia, na ktoré by inak nebol daňový subjekt oprávnený, alebo ktorých výsledkom je účelové zníženie daňovej povinnosti, sa pri správe daní neprihliada.**

. . .

§ 24

Dokazovanie
1. Daňový subjekt preukazuje
a) skutočnosti, ktoré majú vplyv na správne určenie dane a skutočnosti, ktoré je povinný uvádzať v daňovom priznaní alebo iných podaniach, ktoré je povinný podávať podľa osobitných predpisov,
b) **skutočnosti, na ktorých preukázanie bol vyzvaný správcom dane v priebehu daňovej kontroly alebo daňového konania,**
c) vierohodnosť, správnosť a úplnosť evidencií a záznamov, ktoré je povinný viesť.

V čom môže teda nastať problém ?
Z pohľadu prípadnej daňovej kontroly je v zmysle ustálenej judikatúry pomerne zásadné, aby daňovník preukázal oprávnenosť daňového výdavku nie len po **formálnej** stránke predložením písomných dokladov (zmlúv, faktúr a pod.), ale aj preukázaním **materiálneho** podkladu z ktorého by bolo zrejmé, že sa uskutočnil deklarovaný obchod - v našom prípade reklama na internete. A práve na tomto mieste reálne môže nastať zásadná komplikácia pre podnikateľa (objednávateľa reklamy) a to vzhľadom na skutočnosť, že reklama na internete sa realizuje inak ako v klasických printových médiách, pri ktorých je možné spätne bez pochybností overiť alebo doložiť realizáciu konkrétnej reklamy v takomto médiu. Reklama na internete prebieha v konkrétnom čase a v podstate vo vzťahu ku konkrétnym osobám, ktoré si zobrazujú určité webové stránky. V tejto súvislosti považujeme za potrebné podotknúť, že sa spravidla tomuto istému subjektu ani nezobrazí tá istá reklama (toho istého

podnikateľa - daňovníka) dva krát, tzn. že v prípade, že subjekt klikne na určitú stránku v čase „x" a následne v čase „x + y" je pravdepodobné, že reklama na tej istej stránke už bude iná. V tomto kontexte sa javia ako problematické požiadavky daňových úradov pri výkone daňovej kontroly, v zmysle ktorých žiadajú od daňovníka, aby preukázal resp. zdokladoval okrem iného aj „*aktuálne dátumy vysielania reklamy"*, čo vzhľadom na osobitosti spôsobu realizácie reklamy na internete je značne problematické a v prípadoch reklamy prostredníctvom PPC alebo CMP skoro nemožné. Osobitne je otázka unesenia dôkazného bremena aktuálna v prípade, ak preukázanie tejto skutočnosti požaduje daňový úrad od subjektu - podnikateľa, ktorý si vo forme dodávky objednal zabezpečenie takýchto reklamných služieb ďalším subjektom, ktorý mal priamy vzťah zo spoločnosťou resp. spoločnosťami, ktoré tieto reklamné služby realizovali, t.j. daňový kontrolór požaduje preukázanie realizácie reklamy od pôvodného objednávateľa, ktorý ani nemusel prísť do styku s podnikateľom, ktorý reklamu uskutočňoval, resp. na stránkach ktorého sa táto reklama zobrazovala.

V tomto kontexte je možné do istej miery konfrontovať odlišné prístupy Najvyššieho súdu Slovenskej republiky (ďalej aj „NS SR"), ktoré sa týkajú problematiky tzv. rozloženia dôkazného bremena v daňovom konaní.
V prvom z týchto rozhodnutí (ktoré sa síce týka odpočtu na DPH, ale je z hľadiska dokazovania použiteľný aj pre daňovo uznateľné výdavky), NS SR uvádza: „*V danom prípade nepostačuje,* pokiaľ si platiteľ uplatňuje nárok na odpočítanie dane z dodávateľskej faktúry, *iba predloženie účtovných dokladov a zmlúv, pretože uskutočnenie zdaniteľného plnenia je potrebné preukázať nie len po formálnej ale aj po obsahovej stránke. K tejto námietke dáva žalobcovi súd do pozornosti, že v zmysle vyššie citovaného ustanovenia zákona o správe daní § 29 ods. 8 (pozn. aut.: podľa aktuálnej právnej úpravy sa jedná o § 24 zákona o správe daní) je dôkazné bremeno na strane daňového subjektu. V daňovom konaní je povinnosťou daňového subjektu preukázať všetky tvrdené skutočnosti, pričom správca dane tieto dôkazy posudzuje. Správca dane, ktorý získa oprávnené pochybnosti o tom, či bola predmetná služba dodaná nie je povinný dokazovať jej nedodanie, ale daňový subjekt musí vedieť preukázať uskutočnenie zdaniteľného plnenia osobou uvedenou v predkladaných faktúrach,* pokiaľ si uplatňuje nárok na odpočítanie dane z dodávateľskej faktúry. *Ak daňovník neunesie v tomto zmysle dôkazné bremeno nemôže byť úspešný* v uplatnení nároku na odpočet DPH.*"*[4]

Vo vzťahu k tomuto rozhodnutiu by teda platilo, že pokiaľ si daňový subjekt objednáva reklamnú činnosť na internete musí byť schopný jednoznačne preukázať okrem formálnych požiadaviek (faktúr, zmlúv a pod.) zároveň aj jej realizáciu, čo môže byť v konkrétnom prípade problematické a to najmä pokiaľ hovoríme o situácii kedy je táto reklama realizovaná dodávateľským spôsobom. V tomto prípade spravidla objednávateľ nedisponuje materiálmi z ktorých by jednoznačne vyplývalo, kedy a kde sa jeho reklama zobrazila. Domnievame sa, že požadovať takéto materiály od objednávateľa reklamy nie je na mieste a príslušný daňový úrad by mal tieto dokumenty požadovať od osôb u ktorých je objektívny predpoklad, že by nimi mohli resp. mali disponovať. V tomto kontexte sa preto prikláňame k záverom a právnej argumentácii uvedenej v inom rozhodnutí NS SR, podľa ktorého: „*...nie je možné od daňového subjektu požadovať preukázanie skutočností, na ktorých sa sám nepodieľal s následnou satisfakciou v podobe stanovenia výsledku zo strany správcu dane, že „daňový subjekt neuniesol dôkazné bremeno*. *Podporiac svoj názor vyššie uvedeným rozhodnutím má najvyšší súd za to, že dôkazné bremeno, ktoré znáša daňový subjekt je jasne limitované ustanovením § 29 ods. 8 zákona č. 511/1992 Zb. (pozn. aut.: aktuálne sa jedná o § 24 ods. 1 zákona č. 563/2009 Z.z, o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov), ktoré však v záujme zachovania ústavne konformného výkladu tohto ustanovenia nie je možné vykladať extenzívne na ťarchu daňového subjektu a zaťažiť ho preukázaním skutočností, ktoré svojou účasťou nezabezpečoval."*[5] Domnievame sa, že v duchu tohto rozhodnutia by mali byť brané na zreteľ aj objektívne možnosti daňového subjektu tak, aby si svoju dôkaznú povinnosť mohol splniť a aby sa len účelovo nevytváral priestor pre určenie dane podľa pomôcok ako aj pre pokutovanie daňových subjektov v prípadoch kde si daňový subjekt túto povinnosť nemôže splniť.

[4] Rozsudok Najvyššieho súdu Slovenskej republiky z 31. mája 2011, sp. zn. 4 Sžf 20/2011
[5] Rozsudok Najvyššieho súdu Slovenskej republiky z 28. novembra 2012, sp. zn. 6Sžf/10/2012

5 ZÁVER

Reklama na internete je v súčasnosti fenomén v rámci ktorého dochádza k realizácii obchodov v značnej výške a u ktorého je predpoklad, že sa bude neustále vyvíjať a zdokonaľovať. V súvislosti s daňovým aspektmi je zrejmé, že vzhľadom na osobitosti v tejto oblasti je potrebné vykladať pravidlá správy daní pri zohľadnení týchto osobitostí tak, aby bola na jednej strane zabezpečená riadna kontrola daňových subjektov, no na druhej strane, aby nedochádzalo k ukladaniu takých povinností daňovým subjektom, ktoré objektívne nemôžu splniť. V tomto zmysle by bolo vhodné v rovine úvah *de lege ferenda* uvažovať o zmenách právnej úpravy v oblasti dokazovania v daňovom konaní tak, aby bol priestor na takýto postup resp. svojvôľu daňového úradu znemožnený

Použité zdroje:

HUSOVEC, M.: Zodpovednosť na internete podľa českého a slovenského práva. Praha: CZ.NIC, z. s. p., o., 2014, ISBN 978-80-904248-8-3, s. 230
Rozsudok Najvyššieho súdu Slovenskej republiky z 31. mája 2011, sp. zn. 4 Sžf 20/2011
Rozsudok Najvyššieho súdu Slovenskej republiky z 28. novembra 2012, sp. zn. 6Sžf/10/2012
Zákon č. 147/2001 Z. z. o reklame a o zmene a doplnení niektorých zákonov
Zákon č. 351/2011 Z. z. o elektronických komunikáciách;
Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.
Zákon č. 595/2003 Z. z. o dani z príjmov
Zákon č. 222/2004 Z. z. o dani z pridanej hodnoty
Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov

Kontaktné údaje:

JUDr. Peter Lukáčka, PhD.
peter.lukacka@flaw.uniba.sk
Katedra obchodného a hospodárskeho práva
Právnická fakulta Univerzity Komenského v Bratislave
Šafárikovo nám. 6
P.O.BOX 313
810 00 Bratislava 1
Slovenská republika

JUDr. Matej Smalik, PhD.
matej.smalik@flaw.uniba.sk
Katedra obchodného a hospodárskeho práva
Právnická fakulta Univerzity Komenského v Bratislave
Šafárikovo nám. 6
P.O.BOX 313
810 00 Bratislava 1
Slovenská republika

INTERNET Z PERSPEKTIVY OBECNÉHO NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ – VYBRANÉ ASPEKTY

INTERNET FROM THE PERSPECTIVE OF THE GENERAL REGULATION ON THE PROTECTION OF PERSONAL DATA - SELECTED ASPECTS

Jakub Morávek[1]

Právnická fakulta Univerzity Karlovy v Praze

Anotace
Autor se v příspěvku zaměřuje na základní pojednání o novém právním rámci Evropské unie pro ochranu osobních údajů a na souvislosti, které z nového právního rámce pro ochranu osobních údajů vyplývají ve vztahu ke zpracování osobních údajů v rámci internetu.

Anotace
The paper is primarily concerned on issue of new legal framework for personal data protection and on the issue personal data processing in internet.

Klíčová slova: ochrana osobních údajů, nový právní rámec, internet

Key words: personal data protection, new legal framework, internet

ÚVOD

Právní rámec pro ochranu osobních údajů, jak je v současné době konstituován v evropském právním prostoru, staví z principiálního hlediska na zásadách vyjádřených v dokumentech Rady Evropy a Organizace pro hospodářskou spolupráci a rozvoj, které vznikly v 70. a 80. letech minulého století. Tyto byly vyústěním přibližně třicetiletého vývoje následujícího po druhé světové válce. Členové mezinárodního společenství, kteří principy a zásady v rámci jmenovaných mezinárodních organizací formulovaly, jednak reagovaly na události druhé světové války a doby před ní, kdy zejména nacistický režim zásadním způsobem zneužíval osobní údaje a další informace, a jednak reagovaly na aktuální potřeby z hlediska zajištění volného pohybu zboží, služeb, kapitálu, pracovních sil a osob vůbec.

Konkrétněji řečeno, prvními významnými akty, jejichž účelem bylo ustanovit určité standardy v oblasti ochrany dat, byla usnesení Resolution (73) 22 a Resolution (74) 29[2] Rady Evropy, jejichž účelem bylo působit restriktivně ve vztahu ke zpracování osobních údajů, a to jak v rámci sféry soukromé, tak veřejné. Usnesení se týkala zejména principů ochrany soukromí osob při vytváření elektronických databank. Nepřímým cílem Rady Evropy bylo takto zprostředkovaně iniciovat vznik národních úprav v této oblasti.

Hozené rukavice se chopilo hned několik států. Není překvapením, že se jednalo o státy západní Evropy, které se nacházely ve stádiu hospodářského růstu. Rovněž není s podivem, že se

---

[1] Jakub Morávek je odborným asistentem, vědeckým pracovníkem a tajemníkem katedry pracovního práva a práva sociálního zabezpečení Právnické fakulty Univerzity Karlovy v Praze a advokátem v Praze. Působí jako místopředseda České společnosti pro pracovní právo a sociální zabezpečení. Tento příspěvek vznikl díky podpoře poskytované v rámci výzkumného projektu „Soukromé právo XXI. století“, id. č. PRVOUK P05, a zohledňuje právní stav ke dni 31. října 2016. Příspěvek v některých částech vychází z jiného textu autora, konkrétně z *Morávek, J.* Nový právní rámec pro ochranu osobních údajů a pracovněprávní vztahy in Sborník z konference Trnavské právnické dny 2016, Plzeň: Aleš Čeněk, 2016 – v tisku.

[2] Resolution (73) 22E 26. September 1973 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, Resolution (74) 29E 20. September 1974 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector

jednalo vesměs o státy, které byly členy Evropských společenství. Konkrétně přijaly vnitrostátní úpravu na ochranu dat v roce 1973 Švédsko, v roce 1977 Spolková republika Německo, v roce 1978 Rakousko a následně pak Dánsko, Francie, Norsko a Lucembursko.

Brzy se ukázalo, že iniciativa vycházející ze zmíněných rezolucí není dostatečná, a že pro efektivní fungování mezinárodní spolupráce v této oblasti není žádoucí spontánní vnitrostátní normotvorba. Řešením vzniklé situace bylo nastolit jednoznačné (závazné) minimální mezinárodní standardy ochrany dat – druhým krokem, který však vyžadoval relativně vyšší míru integrace zainteresovaných států, bylo zakotvení zásady, že je možné na vnitrostátní úrovni poskytnout i vyšší míru ochrany, nikoli však způsobem, který by omezoval pohyb dat mezi státy, jejichž principiální východiska a standardy v této oblasti dosahují nutného minimálního mezinárodním aktem určeného standardu.

Na potřebu přijetí mezinárodních standardů ochrany dat reagovala Organizace pro hospodářskou spolupráci a rozvoj, která se jako vůbec první pokusila o komplexní vydefinování a konkretizaci pravidel za účelem sjednocení národních úprav ochrany osobních údajů a odstranění překážek jejich předávání ze zemí původu. Výstupem snah OECD bylo vydání „*Doporučení pro ochranu soukromí a toky osobních údajů přes hranice*“ ze dne 1. října 1980. [3]

I když se z mezinárodněprávního hlediska jedná pouze o *soft law*, je dokument podstatný právě s ohledem na soubor v něm vymezených principů. Ty se později objevují i v dokumentech majících povahu *hard law*, jako je úmluva Rady Evropy ze dne 28. ledna 1981, která byla vyhlášena ve Sbírce mezinárodních smluv České republiky pod č. 115/2001 Sb.m.s. - Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (jinak také známá pod zkratkou Úmluva č. 108). Nalezneme je i v evropských směrnicích – konkrétně ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Prostřednictvím Úmluvy č. 108 a zejména směrnice 95/46/ES došlo (z hlediska právního řádu České republiky) k přenesení principů z doporučení OECD[4] nejprve rámcově do zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, a posléze konkrétněji i do předpisu, který jej nahradil, a kterým byla provedena transpozice směrnice 95/46/ES, tj. do zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.[5]

Doplňme, že z hlediska primárního práva EU je základ pro regulaci ochrany osobních údajů položen čl. 16 Smlouvy o fungování Evropské unie a dále čl. 8 Listiny základních práv EU. S ohledem na účel právní úpravy na ochranu osobních údajů (viz níže) lze mít za to, že předpoklady pro právní regulaci ze strany orgánů Evropské unie, tedy subsidiarita a proporcionalita, jsou v tomto případě nezpochybnitelně naplněny – otázkou však zůstává, zda pro regulaci formou směrnice či nařízení.

1. O OBECNÉM NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Evropská právní úprava ve směrnici 95/46/ES, jako primárním pramenu právní regulace ochrany osobních údajů, byla formulována relativně značně obecně. Postupem času, zejména v důsledku působení (expertní) pracovní skupiny zřízené na základě čl. 29 směrnice 95/46/ES (WP 29) a Soudního dvora EU, však získala poměrně jasné obrysy a osvědčilo se (viz například

[3] OECD doporučuje členským státům, aby zejména: (i) do svého vnitrostátního práva zahrnuly principy vztahující se k ochraně soukromí a svobody jednotlivce tak, jak jsou obsaženy v tomto materiálu a (ii) odstranily překážky, které v zájmu ochrany osobnosti brání jejich předávání mimo zemi jejich původu. K doporučení srov. např. http://www.oecd.org/dataoecd/16/6/15589535.pdf

[4] Zmíněnými principy jsou: (a) *princip omezení sběru osobních údajů* (správnost a legálnost); (b) *princip kvality osobních údajů* (adekvátnost účelu, přesnost, úplnost a aktuálnost); (c) *princip specifikace účelu sběru osobních údajů* (stanovení účelu musí předcházet začátku sběru dat); (d) *princip omezení užití osobních údajů* (mohou být zpřístupněna nebo užita jinak pouze se souhlasem subjektu dat nebo na základě zákona); (e) *princip záruk bezpečnosti osobních údajů* (musí být chráněna před ztrátou či neoprávněným přístupem, zničením, užitím, změnou nebo zveřejněním); (f) *princip otevřenosti* (veřejnost informací o povaze a účelu zpracovávaných osobních dat a o jejich správci); (g) *princip účasti subjektu osobních údajů* (právo na informaci o datech o něm sbíraných, právo na zpřístupnění jeho dat, právo na výmaz, opravu a doplnění); (h) *princip odpovědnosti správce osobních údajů* (odpovídá za dodržování všech výše uvedených principů).

[5] Dále jen „***OchOúZ***“

rozhodnutím Soudního dvora EU ve věci González vs. Google Spain SL, C-131/12), že může být aplikována i na moderní technologie.

Je však obvyklou součástí legislativního života, že ve vztahu ke každé právní úpravě existuje záměr ji zlepšit, změnit či zpřesnit. Ten se nevyhnul ani právní úpravě na ochranu osobních údajů, když se na přelomu tisíciletí objevilo první důslednější volání po její změně. V této souvislosti byl vznášen relativně legitimní argument, že od doby, kdy byla připravována směrnice, sice neuplynula příliš dlouhá doba, avšak z hlediska rozvoje moderních technologií (rozšíření mobilních telefonů, první chytré telefony, rozšíření internetu, internet věcí atp.) ušla společnost cestu, která není měřitelná časem. Nelze tudíž aplikovat obecné teoretické východisko vážící se na princi právní jistoty, dle nějž by od nabytí účinnosti právní úpravy do její zásadnější novelizace mělo uplynout alespoň 10 let, tedy doba, kdy se v rámci judikatury a aplikační praxe osvědčí, zda a případě jak právní úprava slouží původně sledovanému účelu (zda jí odpovídajícím způsobem vyložila judikatura, zda odpovídá společenským a technologickým změnám atp.).

1.1. LEGISLATIVNÍ PRÁCE

V rámci úvodních úvah o změně stávajícího právního rámce pro ochranu osobních údajů byly v základu zvažovány tři varianty řešení: (a) novelizace stávající legislativy (primárně směrnice 95/46/ES), (b) zrušení stávající legislativy a přijetí nových směrnic, (c) zrušení stávající legislativy a přijetí právní regulace formou nařízení.

Jelikož byla hlavním iniciátorem nového právního rámce evropská byrokracie, není v kontextu základních tendencí byrokracie s podivem, že prosazována byla forma nařízení. Tento tlak byl dále podpořen i zájmy nadnárodních korporací.

Z hlediska ať již skupiny společností nebo jedné společnosti působící ve více členských státech EU bylo a je totiž jen těžko pochopitelné, že právní úprava na ochranu osobních údajů v EU je sice primárně formulována směrnicí 95/46/ES, byla však transponována do národních právních úprav v částečně odlišné podobě, a co je hlavní, i když je třeba v národních právních řádech vyjádřena obdobně, jsou zde zásadní aplikační rozdíly na straně národních úřadu pro ochranu osobních údajů – jedním z takových případů je oznamovací povinnost ve smyslu ust. § 16 OchOúZ, resp. předběžné posouzení rizikového zpracování osobních údajů ve smyslu čl. 20 směrnice 95/46/ES atp. Tyto rozdíly z povahy věci zvyšují náklady nadnárodních korporací a ztěžují jejich činnost. Jsou pro ně překážkou volného pohybu osobních údajů a tudíž i zboží, služeb, kapitálu, pracovních sil a osob vůbec.

Otázka formy právní regulace byla v rámci legislativního procesu s členskými státy konzultována. Členské státy se poměrně jednoznačně vyjádřili tak, že iniciativu EU oceňují, avšak pro právní úpravu prostřednictvím nařízení dle jejich mínění podmínky splněny nejsou.

Evropský zákonodárce se však nenechal zmást, a již na přelomu let 2011 a 2012 formuloval relativně komplexní návrh nařízení o ochraně osobních údajů. Ten byl ještě podroben podrobné a poměrně dlouhé a důkladné diskusi, navrhovány byly řádově tisícovky pozměňovacích návrhů, včetně komplexních pozměňovacích návrhů. V roce 2016 byl nakonec legislativní proces ukončen a bylo přijato 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), spolu s dalšími souvisejícími předpisy. Účinnosti by mělo nařízení (nový právní rámec pro ochranu osobních údajů) nabýt dne 25. května 2018.

Do nabytí účinnosti obecného nařízení se předpokládá přijetí prováděcích právních předpisů ze strany orgánů EU, kterých se předpokládá větší počet.

Z povahy věci bude v národních právních řadech třeba zakotvit (nově) úřady pro ochranu osobních údajů, jejich kompetence. Bude také nezbytné provázat nový právní rámec s vnitrostátní právní úpravou v dotčených oblastech (včetně například procesních otázek).

Obecné nařízení rovněž nabízí určité možnosti pro národní právní řády, pro odchylky od nařízení. Ze strany orgánů EU jsou nicméně poměrně zjevné signály v tom smyslu, že zavádění větších odchylek ze strany národních parlamentů není žádoucí.

1.2. ÚČEL OBECNÉHO NAŘÍZENÍ A JEHO NĚKTERÉ VÝZNAMNÉ ASPEKTY

Základní účel právní úpravy zůstává *de facto* zachován, když se taktéž jedná (jako ve směrnici 95/46/ES) na jedné straně o ochranu osobnostní sféry subjektů údajů před nepřiměřenými zásahy činěnými zpracováním osobních údajů (ochrana osobních údajů) a z druhé strany o zajištění volného

pohybu osobních údajů v rámci bezpečného prostoru (primárně EU, resp. EHP) s cílem nebránit volnému pohybu zboží, služeb, kapitálu, pracovních sil a osob vůbec. V této souvislosti je snad jen trochu nejasné, zda dikcí čl. 1 odst. 2 obecného nařízení, dle kterého „*Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů.*“, sledují evropské orgány nějaké konkrétní (prozatím neznámé) další cíle.

Cílem nařízení je dále (a) reagovat na moderní technologie, (b) zajistit jednotou interpretaci a aplikaci právní úpravy napříč EU a (c) nastavit jednotný systém trestání napříč EU – zde je ve srovnání se stávající právní úpravou v rámci OchOúZ zásadní rozdíl, když nařízení (čl. 83 obecného nařízení) stanoví jako maximální výši sankce částku 10.000.000 EUR, resp. 20.000.000 EUR, příp. 2 %, resp. 4 % z celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

Vedle toho jsou v nařízení formulovány určité figury, které buďto v dílčí podobě již známe z judikatury nebo doporučení WP 29 (např. právo být zapomenut, závazná podniková pravidla - BCR), nebo se objevují na obecné úrovni zcela nově (viz níže).

Jde-li o nové figury a obraty, které nařízení přináší, poukázat lze zejména na to, co je významné mj. i z hlediska předávání osobních údajů do jiných zemí. Nařízení již oproti směrnici do jisté míry reflektuje realitu stávajícího globalizovaného světa, která se mj. vyznačuje složitými majetkovými vztahy mezi obchodními korporacemi – nařízení v čl. 4 odst. 19 pro své účely definuje pojem skupina podniků (k tomuto dále rovněž recitál č. 48). Jinak řečeno, obecné nařízení o ochraně osobních údajů již umí z hlediska předávání a sdílení údajů do jisté míry pracovat se skupinou společností působících ve více zemích světa – z hlediska obecného nařízení by tudíž již mělo být například relativně řešitelné (mimo souhlas zaměstnance), pokud mateřská společnost má zájem sbírat a zpracovávat údaje o zaměstnancích svých dceřiných společností, aby tak mohla optimalizovat personální zdroje v rámci skupiny.

Vrátíme-li se zpět k obecnému pohledu na nařízení, zůstává otázkou, zda sama podrobnější úprava (oproti směrnici je nařízení nejméně jednou tak rozsáhlé; o OchOúZ nemluvě), kterou nařízení v podstatě ve všech směrech oproti směrnici přináší, bude s to sledovaných cílů dosáhnout. Rozhodná totiž, stejně jako v současné době, bude primárně rozhodovací praxe národních správních soudů – před SDEU se dostane jen nepatrný počet případů. Na tom pravděpodobně nic nezmění ani Evropský sbor pro ochranu osobních údajů (viz níže).

Jinak řečeno, lze mít jistou pochybnost, jestli shodné zákonodárství napříč prostorem Evropské unie může vést a povede k tomu, že bude dosaženo jednotné aplikace právní úpravy, tedy že ze zákonodárství rekonstruované obecné a následně v rozhodovací praxi správních soudů a správních orgánů individuální normy budou totožné. Takový stav je dle všeho v reálném časovém horizontu nedosažitelným ideálem. Vždyť zajistit i jen jednotnou aplikaci zdejšího právního řádu (právního řádu České republiky) ze strany kupříkladu obecných soudů je téměř neřešitelný úkol, který se daří jen částečně zvládnout prostřednictvím působením vysokých soudů (Nejvyššího soudu a Nejvyššího správního soudu). Takový (evropský) soud však bude pro oblast ochrany osobních údajů *de facto* scházet – s ohledem na způsob fungování a možnosti přenesení věci před SDEU nemůže takovou funkci odpovídajícím způsobem plnit SDEU.

Ještě více skeptický pohled nežli na otázku jednotné interpretace a aplikace předmětné legislativy (obsahů jednotlivých pojmů a obsahu jednotlivých povinností) lze mít ve vztahu k naplnění principu/účelu jednotného trestání napříč evropským prostorem – ať již z hlediska vzájemné informovanosti jednotlivých národních úřadů pro ochranu osobních údajů, nebo z hlediska ingerence národních správních soudů, či z hlediska odlišné ekonomické síly trestaných subjektů, dosavadní historie v této oblasti a „národních tradic“.

Dále, v novém právním rámci o ochraně osobních údajů pojal zákonodárce poměrně značně ambiciózní záměr, jímž je snaha relativně konkrétněji regulovat jevy, na které se bude vztahovat, včetně moderních technologií. Tato skutečnost, která může být vnímána pozitivně, je však výhodou jen zdánlivou.

Stávající právní úprava se vyznačuje značnou obecností Ta je v prvopočátcích účinnosti právní úpravy z hlediska právní jistoty částečně problematická, avšak po dostatečně dlouhé době, v níž se právní úprava uplatňuje, je-li zde dostatečné množství rozhodnutí, které dávají lépe tušit, jak jí uchopit, se následně ukazuje jako vhodnější nežli úprava popisná – obecné skutkové podstaty dávají v návaznosti na účel a smysl právní úpravy možnost vztáhnout právní úpravu na všechny jevy, které se objeví v budoucnu, a které nebyly dříve známy (např. moderní technologie), a na které by se však

právní úprava s ohledem na svůj smysl a účel aplikovat měla. Tyto možnosti jsou u kazuistické právní úpravy poměrně omezeny.

Jinak řečeno, směrnice 95/46/ES je ve své obecnosti schopna obstát i dnes, a byla by v základu schopna obstát zcela jistě i v budoucnu; uvedené nic nemění na tom, že kupříkladu z hlediska reality velkých nadnárodních korporací trpí nedostatky, které by bylo třeba odstranit. Naproti tomu, bude-li právní úprava relativně konkrétní, jak je tomu (částečně) v obecném nařízení, takový závěr již platit nemusí. Je třeba vnímat, jaký nastal posun v oblasti společenských struktur a technologií za posledních 20 let a zejména, jak jsme si před 20 lety představovali, že by se společenské struktury a technologie mohly změnit.

Tento bod lze uzavřít pozitivně s tím, že řada závěrů obsažená ve stanoviscích WP 29, stejně tak jako v dosavadní judikatuře SDEU, by měla obstát i v novém právním rámci ochrany osobních údajů. K tomu, které to budou, by se měl vyjádřit Evropský sbor pro ochranu osobních údajů, který se zřizuje na základě čl. 68 obecného nařízení o ochraně osobních údajů (Evropský sbor pro ochranu osobních údajů by měl být *de facto* nástupcem WP 29).

2. OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ A INTERNET – VYBRANÉ ASPEKTY

Jak již bylo uvedeno shora, obecné nařízení o ochraně osobních údajů v základu sleduje se směrnicí 95/46/ES shodné výchozí účely. Spolu s tím je shodný i základní principiální rámec, který *de facto* váže na jmenované dokumenty Rady Evropy a OECD.

Komplexní pojednání o jednotlivých aspektech, ustanoveních a institutech obecného nařízení je materií pro samostatnou rozsáhlou monografii. Na tomto místě se tudíž zaměříme jen na označený některých výrazných a zajímavých momentů, které mají mj. vazbu na zpracování osobních údajů v prostředí internetu a za pomoci moderních technologií.

2.1. PŮSOBNOST

Bylo již naznačeno, že evropský zákonodárce si v rámci obecného nařízení neklade malé cíle, když se pokouší reagovat na moderní technologie a stávající globalizovanou podobu světa. O rizicích přílišné kazuistiky a výhodách obecných skutkových podstat v této souvislosti bylo hovořeno shora.

Lze mít za to, že s tendencí označenou v předešlém odstavci souvisí například i vymezení místní a osobní působnosti[6] nařízení v rámci čl. 3 ve spojení s recitálem č. 23. Poukázat lze zejména na čl. 3 odst. 2 nařízení, dle kterého se nařízení „*vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí: (a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo (b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie.*“ K tomu pak recitál č. 23 nařízen uvádí „*Aby bylo zajištěno, že fyzickým osobám nebude odepřena ochrana, na niž mají podle tohoto nařízení nárok, mělo by se na zpracování osobních údajů subjektů údajů nacházejících se v Unii uskutečněné správcem nebo zpracovatelem, jenž není v Unii usazen, vztahovat toto nařízení, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů bez ohledu na to, zda je spojena s platbou. Aby se určilo, zda takový správce nebo zpracovatel nabízí zboží nebo služby subjektům údajů nacházejícím se v Unii, je třeba zjistit, zda je zjevné, že má správce nebo zpracovatel v úmyslu nabízet služby subjektům údajů v jednom nebo více členských státech v Unii. Zatímco pouhá dostupnost internetových stránek správce, zpracovatele nebo zprostředkovatele v Unii, e-mailové adresy nebo jiných kontaktních údajů anebo používání jazyka obecně používaného ve třetí zemi, v níž je správce usazen, nepostačuje ke zjištění tohoto úmyslu, mohly by faktory, jako je používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat zboží a služby v tomto jiném jazyce nebo zmínky o zákaznících či uživatelích nacházejících se v Unii, být zjevným dokladem toho, že správce má v úmyslu nabízet zboží nebo služby subjektům údajů v Unii.*“

Budeme-li brát Velkou Británii stále jako součást Evropské unie, pak se rozlišující kritérium v podobě jazykové mutace webových stránek ukazuje jako nedostatečné, neboť většina velkých internetových obchodů atp., má svou anglickou jazykovou mutaci – lze mít tudíž za to, že hraniční určovatel v podobě, jsou-li stránky v jazyce Evropské unie, nařízení by se na zpracování mělo

[6] Z hlediska věcné působnosti zůstává zachován princip osobní potřeby – viz například recitál č. 18.

vztahovat, sám o sobě nemůže obstát, jak se budou prokazovat ostatní recitálem č. 23 zmiňované momenty, zůstává otázkou.

Jakým způsobem se bude prosazovat a uplatňovat legislativa EU vůči správcům osobních údajů mimo její jurisdikci (jurisdikci členských států), zejména pokud správce nezmocní ve smyslu citovaného článku jinou odpovědnou osobu na území EU, zůstává taktéž otázkou.

Vedle řečeného lze poukázat na určité segmenty osobní a věcné působnosti. S ohledem na dílčí názory, z nichž některé prezentoval v minulosti i (český) Úřad pro ochranu osobních údajů, lze kladně hodnotit, že nařízení explicitně ze své působnosti vylučuje v pozici subjektu údajů právnické osoby (recitál č. 14), a stejně tak jako to, že se nevztahuje (recitál č. 27) na systematické dispozice s údaji o osobě, která již nežije. Dovodit lze i vyloučení působnosti na informace týkající se podnikání fyzické osoby podnikající.

2.2. PROFILOVÁNÍ

Lze kvitovat, že se v nařízení věnuje pozornost profilování, jako specifické formě zpracování osobních údajů, která může být relativně riziková zejména, je-li využívána, resp. zneužívána ve vztahu ke spotřebitelům nebo možná lépe řečeno osobám, které nemají podrobnou znalost zejména o fungování internetu a možnostech, které prostředky moderní techniky přináší ve směru k nabídce ochodu a služeb (podprahová reklama atp.).

V této souvislosti recitál č. 30 uvádí: „*Fyzickým osobám mohou být přiřazeny síťové identifikátory, které využívají jejich zařízení, aplikace, nástroje a protokoly, jako například adresy internetového protokolu či identifikátory cookies, nebo jiné identifikátory, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob a k jejich identifikaci*“

Definici profilování pak obsahuje čl. 4 odst. 4 nařízení. Dle jmenovaného ustanovení se profilováním rozumí „*jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.*“.

Ve vztahu k definici profilování lze mít jistou výhradu (nejméně z hlediska právní úpravy pracovněprávních vztahů). Zahrnutí predikce pracovního výkonu do definice profilování totiž není zcela pojmově přesné, neboť má-li zahrnovat i predikci ze strany zaměstnavatele, pak je zjevné, že motivace je oproti spotřebitelským vztahům významně odlišná. Pro pracovněprávní vztahy by mělo postačovat, co platí již dnes (viz ust. § 11 odst. 6 OchOúZ), tj. že žádné rozhodnutí správce osobních údajů v neprospěch subjektu údajů nelze založit pouze na výsledku automatizovaného zpracování osobních údajů (například nelze pouze na základě výpisu z elektronické docházky, kde jsou vykazovány neomluveně zmeškané části směn, je-li podle výpisu v úhrnu zmeškána celá směna, zaměstnanci zkrátit dovolenou). Má-li být výstup z automatizovaného zpracování osobních údajů podkladem pro rozhodnutí, musí být verifikována správnost záznamů (například svědecky osvědčeno, že v některý ze dnů, které jsou v elektronické docházce vykazovány jako neomluveně zmeškané části směn, zaměstnanec skutečně přišel o příslušnou dobu pozdě do práce).

Obecně se prozatím veřejnoprávní kontrola řádného plnění zákonných povinností správce osobních údajů, je-li zpracování prováděno v on-line prostředí, resp. za pomoci moderních technologií a internetu, ukazuje kvůli nedostatečné personální a technické vybavenosti (nejméně českého) úřadů pro ochranu dat (mírně řečeno) jako problematická. To z povahy věci platí a bude platit i ve vztahu k profilování. Bude jistě zajímavé sledovat, jak se s tímto úkolem úřady pro ochranu dat v budoucnu vypořádají (v dalším k těmto aspektům viz níže).

2.3. PRÁVO BÝT ZAPOMENUT

O institutu, pro který se vžilo označení, jež se následně prosadilo i v rámci jeho legislativního vyjádření, *právo být zapomenut*, byly vedeny diskuse (částečně pro jistou populární stránku institutu) v podstatě kontinuálně po celou dobu přípravy nařízení. Před přijetím platnosti nařízení byl předmětný institut v určité podobě vyjádřen v rozhodnutí Soudního dvora EU ve věci González vs. Google Spain SL, C-131/12, o němž byly následně rovněž vedeny rozsáhlé diskuse v rámci odborné veřejnosti.

Ve vztahu k právu být zapomenut obecné nařízení v recitálu č. 65 a č. 66 konkrétně stanoví „*Fyzická osoba by měla mít právo na opravu osobních údajů, které se jí týkají, a „právo být*

zapomenuta", pokud uchovávání těchto údajů porušuje toto nařízení nebo právo Unie či členského státu, které se na správce vztahuje. Subjekt údajů by zejména měl mít právo na to, aby jeho osobní údaje byly vymazány a nebyly dále zpracovávány, pokud již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány, pokud subjekt údajů odvolal svůj souhlas se zpracováním nebo pokud vznesl námitku proti zpracování osobních údajů, které se jej týkají, anebo pokud je zpracování jeho osobních údajů v rozporu s tímto nařízením z jiných důvodů. Toto právo je obzvláště důležité v případech, kdy subjekt údajů dal svůj souhlas v dětském věku a nebyl si plně vědom rizik spojených se zpracováním a později chce tyto osobní údaje zejména na internetu odstranit. Subjekt údajů by měl mít možnost toto právo uplatnit bez ohledu na skutečnost, že již není dítě. Další uchovávání osobních údajů by však mělo být zákonné, pokud je to nezbytné k uplatnění práva svobody projevu a informací, z důvodu splnění právní povinnosti, provádění určitého úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, z důvodů veřejného zájmu v oblasti veřejného zdraví, pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely nebo pro určení, výkon nebo obhajobu právních nároků." a dále *„Aby bylo v internetovém prostředí posíleno právo být zapomenut, mělo by být rozšířeno právo na výmaz tím, že by správce, který zveřejnil osobní údaje, měl povinnost informovat správce, kteří osobní údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či veškeré jejich kopie nebo replikace. Přitom by měl správce učinit vhodné kroky, s přihlédnutím k dostupné technologii a prostředkům, které má k dispozici, včetně uplatňování technických opatření, s cílem informovat správce, kteří tyto osobní údaje zpracovávají, o žádosti subjektu údajů."*

Normativně je pak předmětný institut vyjádřen v čl. 17 nařízení. Právo být zapomenut je zde chápáno v jádru shodně jako ve shora odkazovaném rozhodnutí SDEU.

Pro komplexní rozbor této figury zde není prostor, nabízí se tak poukázat alespoň na určité dílčí aspekty spíše principiálního charakteru.

Realizuje-li se právo být zapomenut ve vztahu k údajům, jejichž původcem není daný subjekt údajů, byly zpřístupněny nelegálně atp., nelze mít v podobě výhrad.

Nicméně, z jistého hlediska může být právo *být zapomenut* vnímáno i jako prostředek nápravy reliktů (nejen) mladické nerozvážnosti, kdy člověk v rámci své ještě nedostatečné zralosti (rozumové vyspělosti) umístí na internet texty, fotografie nebo jiné informace vztahující se k jeho osobě (o jeho sexuálním životě atp.), o nichž se (poměrně očekávaně) v budoucnu ukáže, že mu nějakým způsobem maří (nebo mohou mařit) nebo ztěžují (mohou stěžovat) buďto soukromý nebo pracovní život, a tyto informace chce následně odstranit. Takové opatření, které dává možnost „získat novou šanci", má samozřejmě v základu shodné pozitivní konotace jako je tomu v prvém naznačeném případě. Je zde však i několik podstatných odlišných momentů.

V prvé řadě se v této poloze nabízí možnost žádat si odstranění stavu, jehož původcem je sám žadatel (subjekt údajů). S ohledem na to, že v kontextu shora odkazovaného rozhodnutí SDEU bude adresátem žádosti primárně provozovatel internetového vyhledávače, mělo by se opatření realizovat na náklady za významné pomoci a iniciativy správce osobních údajů (v kontextu rozhodnutí SDEU provozovatele internetového vyhledávače), který na předmětném stavu, známosti informace ve veřejném prostoru, krom toho, že tuto k žádosti třetí osoby (která ji vyhledává) zprostředkovává, žádnou vinu nenese. Je zde tedy zásah do jeho majetkové sféry této osoby.

Dále je zde otázka, která úzce souvisí s technologickým řešením věci. Ve většině případů bude pravděpodobně efektivní opatření spočívat pouze v tom, že internetový vyhledávač nebude již požadovanou informaci zobrazovat, rozuměj, s ohledem na to, že informace může být uložena kdekoli, a původce může být odkudkoli, budou efektivní opatření končit u provozovatele vyhledávače.

A tak se lze ptát: Aby dosáhnul svého cíle, bude se muset dotčený člověk obrátit na všechny poskytovatele takových služeb? Co když některý bude mimo jurisdikci Evropské unie? Jak v této souvislosti řešit programová rozhraní jako je kupříkladu Tor?[7]

A ani to není zdaleka vše. Není vyloučeno, že může nastat situace obdobná jako je v současné době ohledně sdílení nelegálního obsahu prostřednictvím internetu (filmy, hudba atp. prostřednictvím rapidshare atp.); zde oficiální distributoři každodenně žádají o odstranění konkrétního nelegálního obsahu, správce jej ze stránky odstraní, přičemž shodný nelegální obsah (film atp.) je v podstatě obratem umístěn na stránku znovu a distributor musí celý proces opakovat.

[7] Viz https://www.torproject.org/

A konečně, což je zásadní, právo být zapomenut zasahuje již tak problematikou oblast, v níž v současné době trpíme významným deficitem, jíž je odpovědnost za vlastní chování. Vstupuje na místo, kde by měla prim hrát výchova – dítěti či nedospělci by mělo být vštěpováno, jak se má chovat a jaké důsledky může jeho stávající jednání (i třeba relativně daleko) v budoucnu a ono samo by mělo cítit, že takové jednání není dobré a může být závažné následky, které nebude možné odčinit. Bezpečí, které právo být zapomenut poskytuje, je totiž jen zdánlivé. Platí a pravděpodobně vždy bude platit, že jakmile je informace součástí veřejného prostoru na internetu, není možné jí zlikvidovat, neboť i když by po předchozím zpřístupnění třeba přechodně nebyla součástí sítě, bude uložena na osobních stanicích (počítačích), z nichž dříve nebo později opět pronikne do veřejné sféry.

Je to trochu jako s periodickým tiskem. Fakt, že vydání z minulého týdne není na stánku k dostání, neznamená, že informace již není dostupná. Je třeba jen hledat (vypravit se do knihovny, kde jsou všechny výtisky archivovány). Jsme-li v této rovině přirovnání, pak se nabízí (byť trochu nepřesně) podotknout, že byla-li před 20 lety otištěna informace o nějaké mladické nerozvážnosti, není možné si kdekoli žádat, aby byla z archivních vydání odstraněna, neboť již pominul účel, pro nějž byla zveřejněna, nebo se dotčený k lumpárně uvolil jako dítě, aniž by si byl vědom všech důsledků – pro tyto případy platí, že ten, koho se týká, musí ve svém životě počítat s tím, že tato informace může být opětovně vzpomenuta (to se z povahy věci zpravidla stane v momentě, kdy se to nejméně hodí).

Jinak řečeno, právo být zapomenut může v konečném důsledku vyznít i jako projev jisté nežádoucí paternalismu státu (EU), jehož důsledky ve směru k osobní odpovědnosti jednotlivce jsou krajně nežádoucí.

2.4. SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Samostatnou a významně problematickou kapitolou zůstává souhlas se zpracováním osobních údajů.

Nařízení oproti směrnici řeší souhlas a související záležitosti, včetně udělení souhlasu v rámci všeobecných obchodních podmínek atp., relativně komplexně. Otázkou však je, zda je tato materie řešena uspokojivě – v tomto bodě se nařízení více přiklání, což je do jisté míry pochopitelné, k ochraně subjektů údajů, což jej však částečně odvádí od reálné společenské situace.

Souhlas se zpracováním osobních údajů definuje primárně čl. 4 odst. 11 nařízení, na který dále navazuje čl. 7 upravující podmínky vyjádření souhlasu a čl. 8, který stanoví speciální podmínky pro udělení souhlasu dítěte v souvislosti se službami informační společnosti. Z hlediska recitálů lze pak zvlášť poukázat na recitály č. 42 a 43.

S ohledem na zaměření tohoto příspěvku se nabízí k problematice souhlasu tak, jak je obsažena v nařízení, připojit jen několik drobných kritických poznámek:

- **souhlas a všeobecné obchodní podmínky** – Dle čl. 7 odst. 2 a 4 nařízení platí „*Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná*“ a dále „*Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné*“

  Uvedené se úzce dotýká problematiky všeobecných obchodních podmínek a poskytování údajů podnikatelům v souvislosti s jejich podnikatelskou činností – za účelem prověření bonity klienta (typicky u bank v nebankovních registrech dlužníků), za účelem zasílání nabídky obchodu a služeb ze strany obchodních partnerů atp. Podnikatelé pravidelně realizují řadu zpracování osobních údajů, která přímo nesouvisí s primárním účelem smlouvy. Mají však význam z hlediska bezpečnosti podnikatele (ověření si identity a bonity zákazníka), či nějakým způsobem zlevňují poskytovanou službu nebo zboží (nabídka obchodu a služeb, reklama atp.).

  Pokud by souhlas k takto nesouvisejícím zpracováním osobních údajů měli být brány jako nesvobodné (ke svobodě souhlasu dále srov. rovně recitál č. 43), mohlo by se jednat o problém pro stávající fungování řady odvětví, v němž se využívají pro kontakt se zákazníkem moderní technologie.

Podobně problematická je fakticky ze stejných důvodů možnost odvolání souhlasu se zpracováním osobních údajů ve smyslu čl. 7 odst. 3 nařízení (k odvolání dále rovněž viz recitál č. 42), dle kterého „*Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.“* Z hlediska právní řádu České republiky se v tomto směru nařízení navíc odchyluje (minimálně částečně) od ust. § 87 zákona č. 89/2012 Sb., občanský zákoník.[8]

Co lze považovat, hodnoceno z hlediska zkušeností z advokátní praxe, za jen velice těžko řešitelské, je písemné vyjádření souhlasu subjektu údajů, který se týká jiných skutečností, než je primární účel smlouvy (typicky ve všeobecných obchodních podmínkách), srozumitelným a snadno přístupným (zřejmě tedy buďto vynětím z VOP nebo zvláštním zdůrazněním/zvýrazněním v jejich rámci – v oblasti internetu, zejména internetových obchodů, je tento aspekt překvapivě lépe řešitelný než mimo ni, když se dá vyřešit samostatným políčkem založeným na principu opt-in) způsobem za užití jasný a jednoduchých jazykových prostředků; z hlediska ObčZ by dle všeho mělo slovní vyjádření odpovídat ust. § 4 ObčZ, dle kterého „*Má se za to, že každá svéprávná osoba má rozum průměrného člověka i schopnost užívat jej s běžnou péčí a opatrností a že to každý od ní může v právním styku důvodně očekávat.“*

Již jen podle dnes platné a účinné právní úpravy, má-li mít souhlas se zpracováním osobních údajů všechny náležitosti a mají-li být subjektu údajů poskytnuta všechna poučení, jedná se o text na nejméně jednu celou stranu, přičemž z povahy věci v něm jsou užívána (aby byly naplněny všechny zákonné podmínky) slova jako správce osobních údajů, osobní údaj, zpracování osobních údajů atp., tedy slova, jejichž obsah není osobě, o které se hovoří v ust. § 4 ObčZ, zpravidla v podrobnostech znám. Jelikož je právní úprava na ochranu osobních údajů svou povahou veřejnoprávní, k uvedenému se dále přidává ještě to, že nařízení předmětné pojmy definuje pro sebe, tudíž dílčím způsobem dále specifikuje jejich obsah.

Tato problematika také úzce souvisí s ust. § 1751 an. ObčZ (obchodní podmínky) a § 1798 an. ObčZ (smlouvy uzavírané adhezním způsobem). Udělení a planost souhlasu bude v České republice třeba řešit mj. i v kontextu této právní úpravy.

Konečně si lze ve vztahu k problematice souhlasu subjektu údajů položit otázku, jak vnímat a hodnotit čl. 8 nařízení, tedy právní úpravu souhlasu se zpracováním osobních údajů ze strany dítěte ve vztahu ke službám informační společnosti (k tomuto rovněž viz recitál č. 38).

Moderní technologie přináší mnohé možnosti a mnohá nebezpečí. Mladší generace je umí zpravidla ovládat lépe než jejich rodiče (minimálně od určitého věku). To však nic nemění na tom, že primární odpovědnost musí být na straně rodičů – prostředky moderní techniky dávají rodičům poměrně dobré možnosti (alespoň v domácnosti) zamezit přístup ke službám či webovým stránkám, které považují za nevhodné. To však není řešení. Směřování dětí musí plynout primárně z výchovy; domácí technická sféra a z ní plynoucí omezení jsou jen drobným dílčím segmentem a nástrojem.

K tomu lze dodat, mj. i v návaznosti na dnes běžná opatření k ověření dosažení věkové hranice uživatelů internetu (typicky – napiš svůj věk, potvrď, že ti bylo více jak 18 let, potvrď, že souhlasí, tví rodiče), že aplikace čl. 8 odst. 1 a 2 nařízení[9] může poměrně snadno sklouznout k realizaci řady formálních opatření, která budou zvyšovat administrativní zátěž a zvyšovat náklady. Jejich faktické důsledky však budou minimální. Lze si samozřejmě představit i sofistikované systémy ověřující splnění příslušných podmínek prostřednictvím komunikace se vstupním rozhraním, v němž budou údaje o uživateli po ověření

[8] Dále jen „***ObčZ***“.

[9] „*Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.“* a dále „ *Správce vyvine přiměřené úsilí s ohledem na dostupnou technologii, aby v takovýchto případech ověřil, že byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.“*

nezaměnitelně zavedeny, takové systémy by však kladly značné nároky na uživatele i poskytovatele služeb a navíc *de facto* zakládaly rizika pro zpracovávané osobní údaje.

- **bezpečnost zpracovávaných osobních údajů** – shodně jako stávající právní úprava klade i nový právní rámec pro ochranu osobních údajů značné nároky na zabezpečení zpracovávaných osobních údajů.

V povinnostem na úseku zabezpečení zpracovávaných osobních údajů lze poukázat na jeden moment, jehož komplexní důsledky bude třeba ještě blíže zkoumat.

Konkrétně se jedná o povinnost oznámit (do 72 hodin) dozorovému úřadu, a případně i dotčeným subjektům údajům, porušení bezpečnostních opatření na úseku ochrany osobních údajů. Tato povinnost není úplnou novinkou, nově je však zaváděna v obecné rovině pro všechny případy – v současné době je formulována relativně úzce pro oblast služeb informační společnosti. Pokud se prosadí její široké pojetí tak, jak je možné jej vyčíst z čl. 33 nařízení, bude povinnost dopadat kupříkladu i na situace, kdy do e-mailové schránky užívané pro pracovní účely přistoupí člen domácnosti, který nemá s výkonem předmětné práce nebo podnikání žádnou vazbu (takový přístup by nicméně mohl vést k zahlcení dozorových úřadů, pokud by byla povinnost do důsledků plněna), což je (částečně) absurdní.

Bude zajímavé sledovat, jak se dozorové úřady vypořádají s touto povinností v kontextu zásady, která je pozitivně vyjádřena i v Ústavním pořádku České republiky v čl. 37 Listiny základních práv a svobod, tedy v kontextu zákazu nucení k sebeobviňování.

3. ZÁVĚR

Nový právní rámec pro ochranu osobních údajů slibuje řadu pozitivních momentů, současně však vzbuzuje i určité kontroverze a pochybnosti.

O pravdivosti tvrzení evropského zákonodárce, který uvádí (a při zdůvodňování proč přijmout nový právní rámec a nařízení uváděl), že přijetím nové legislativy dojde ke snížení administrativní zátěže, lze v kontextu dikce obecného nařízení poměrně úspěšně pochybovat.

Je sice pravda, že dojde k zániku oznamovací povinnosti, kterou známe z ust. § 16 OchOúZ. Zavádí se však nová obdobná povinnost (čl. 35 a 36 nařízení). Vedle toho bude správce povinen vést (čl. 30 a recitál 80 nařízení) záznamy o zpracování osobních údajů a o činnostech zpracování. Dojde k jisté standardizaci informační povinnosti (standardizované samolepky, tabulky a ikony – vzory budou vydány v prováděcím právním předpise ze strany Komise EU). Zavádí se lhůty pro splnění této povinnosti správce osobních údajů. Spolu s tím se mění i právní úprava práva subjektu údajů na přístup k informacím, když se stanoví lhůty pro splnění předmětné povinnosti ze strany správce. Stanoví se (nově), že subjekt údajů, který si informace žádá (a který prokázal svou totožnost), má právo na bezplatnou kopii.

Bez pozornosti nelze nechat ani plošné zavedení pověřenců pro ochranu osobních údajů, standardizovaných kodexů chování, osvědčení, známek a pečení, které se budou vydávat ve vztahu k povinnosti zabezpečení zpracovávaných osobních údajů.

Z uvedeného se rovněž podává, že bude-li chtít správce plnit všechny své povinnosti řádně, a bude-li chtít využít možností různých standardizovaných certifikátů, bude nový právní rámec pro ochranu osobních údajů představovat vedle zvýšení administrativní zátěže i zvýšení zátěže finanční.

Z hlediska právního prostředí a právního řádu České republiky je v souvislosti s novým právním rámcem pro ochranu osobních údajů třeba vnímat jeden významný aspekt, který může být v konečném důsledku i významnější než samotné věcné změny. Jedná se o nikoli nepatrné zvýšení administrativní zátěže oproti stávajícímu stavu. Zde je třeba poukázat na to, že i když tento nárůst administrativní zátěže sám o sobě nemusí být fatální, v kontextu dalších probíhajících či připravovaných legislativních změn by již bylo možné učinit i jiný závěr – z hlediska podnikatelské sféry lze poukázat například na povinné hlášení k DPH, elektronickou evidenci tržeb, povinnost přijmout určitou formu compliance programů (compliance programy a politiky se částečně mohou překrývat s kodexy chování ve smyslu čl. 40 an. nařízení) vyplývající ze zákona o trestní odpovědnosti právnických osob, z hlediska pracovněprávního pak samozřejmě neustálou změnu legislativy, v mnoha případech nedostatečně zdůvodněnou, jejímž primárním důsledkem je právě zvýšení administrativní a finanční zátěže (například stávající návrh na změnu v oblasti dovolené – viz Parlament České republiky, Poslanecká sněmovna VII. volební období, tisk 903/0).

Zvyšování administrativní zátěže lze považovat za obecný znak (nejen) legislativy Evropské unie. Tato je zjevně z části důsledkem snahy vše v maximální míře ideálně a jasně regulovat tak, aby byla poskytnuta nejlepší možná ochrana příslušným hodnotám za současného naplňování cílů Evropské unie. Jakýmsi nedostižným ideálem je koncept vlády práva, jinak řečeno situace, kdy se společnost řídí dobrými pravidly, které jsou v souladu s vnitřním hodnotovým uspořádáním společnosti a směřují k dobru s velkým D, pravidly, která jsou internalizována ve vzorcích chování členů společnosti (ti je s ohledem na svůj hodnotový náhled na svět a společnost vycítí a spontánně je dodržují; porušují je jen v přiměřené/přirozené míře). V takové představě pak neplatí, že jde o vládu lidí nad lidmi, nýbrž o vládu pravidel. Pro naplnění takového předpokladu je rozhodných několik základních a výchozích premis, mezi něž spadá plnění pravidel vnitřní morálky práva,[10] rozdíl mezi recentní objektivní morálkou a ideální objektivní morálkou, včetně souladu recentních subjektivních hodnotových vzorů ve vztahu k recentní objektivní a ideální morálce atp.[11] Jednou z těchto premis, ať je aktuální stav v rámci právě označených zbylých kategorií jakýkoli, je, že právní pravidla nelze napsat odděleně od lidí, odděleně od společenské reality, ve které se mají realizovat, bez reálného zohlednění všech možných důsledků ve všech možných souvislostech.

Lze mít poměrně přesvědčivě za to, že touto cestou (komplexních analýz dopadů zamýšlené právní regulace, reflexe socioekonomické reality atd.) se jak český, tak evropský zákonodárce prozatím rozhodl nevydat. Setrvání na stejné pozici pak může v konečném důsledku vést k právnímu řádu sestávajícímu se z formálně bezvadných pravidel, jejichž faktická proveditelnost a respekt k nim bude pro jejich složitost, administrativní náročnost a odtržitost od společenské reality mizivý, tedy k právnímu řádu, který bude mít jen velmi pochybnou platnost.

S platností právního řádu úzce souvisí ještě jeden zde zmiňovaný aspekt. Aby mohl být učiněn závěr o platnosti právního řádu (nebo jeho některé části), musí být jím formulovaná pravidla, nejsou-li dodržována, efektivně (včas, důsledně atp.) vynucována státní/veřejnou mocí. Lze mít jistou pochybnost, s ohledem na prozatímní zkušenosti z oblasti státní kontroly a správního řízení v oblasti ochrany osobních údajů, že (nejméně v České republice) budou mít správní úřady (Úřad pro ochranu osobních údajů) dostatečné personální kapacity a materiální zabezpečení k tomu, aby se efektivně ujaly dozorování v oblasti zpracování osobních údajů v prostředí internetu; je v podstatě nepředstavitelné, aby státní úřad s rozpočtem, který je zhruba dvacetinou toho, co mobilní operátor v kalendářním roce vynaloží na zabezpečení svých systémů, mohl jakkoli do hloubky ověřit těsnost a zabezpečení systémů zpracování osobních údajů, které operátor realizuje. Nedostatek efektivní dozoru a faktické nevymáhání právních norem dělá z příslušného zákonodárství jen soubor prázdných proklamací, zda takový osud stihne nový právní rámec pro ochranu osobních údajů, ukáže až čas.

Literatura:

Fuller, L. L. Morálka práva, OIKOYMENH, Praha, 1998

Morávek, J. Model práva – vztah práva a morálky. Praha: Linde, a.s.2013

.

[10] Srov. *Fuller, L. L.* Morálka práva, OIKOYMENH, Praha, 1998

[11] K tomuto srov. *Morávek, J.* Model práva – vztah práva a morálky. Praha: Linde, a.s.2013.

DIFAMÁCIA NA INTERNETE

Soňa Ralbovská Sopúchová

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: In the presented article the author analyses an issue of defamation in the Slovak Republic. At the beginning of the article, the author aims to clarify the new phenomenon of our time, defamation, which is increasingly appearing in the online environment. In the next part of the article, the author tries to answer questions such as assessing of defamation in the legal system of the Slovak Republic, how defamation modifies with respect to the Internet and who is responsible for defamation proceedings on the Internet. Within the related judicial decisions, the author reflects on the legislation in cases of defamation on the Internet in the Slovak Republic. In the final part of the article the author provides suggestions and options for legislation of liability relations and for avoiding of negative consequences of defamation on the Internet.

Abstrakt: Autorka v predkladanom článku rozoberá problematiku difamácie v podmienkach Slovenskej republiky. V úvode článku sa zameriava na objasnenie nového fenoménu dnešnej doby, ktorým je difamácia objavujúca sa čoraz častejšie v internetovom prostredí. V ďalšej časti príspevku sa autorka snaží odpovedať na otázky, ako sa posudzuje difamácia v právnom poriadku Slovenskej republiky, ako sa modifikuje vzhľadom na Internet a kto je zodpovedný za difamačné konanie na Internete. Na pozadí súdnych rozhodnutí sa autorka zamýšľa nad právnou úpravou prípadov difamácie na Internete v Slovenskej republike. V záverečnej časti článku uvádza návrhy pre právnu úpravu zodpovednostných vzťahov a pre odstránenie negatívnych následkov difamácie na Internete.

Key words: defamation, defamation on the Internet, defamation proceedings

Kľúčové slová: difamácia, ohováranie na internete, difamačné konanie

1 ÚVOD

Pojem difamácia je cudzí výraz pochádzajúci z anglického jazyka, ktorému nie je v podmienkach Slovenskej republiky priradený žiadny konkrétny slovenský ekvivalent. Podľa Jazykovedného ústavu Ľudovíta Štúra rozumieme difamáciou *nactiutŕhanie, ohováranie, hanobenie, zneúctenie* či *znevažovanie*.[1] Teoretická základňa problematiky difamácie vznikla v Spojených štátoch amerických, kde sa v 90. rokoch minulého storočia začali rozhodovať prvé spory, ktorých predmetom bola difamácia uskutočňovaná na Internete.

Naša spoločnosť zaznamenala v posledných rokoch veľké zmeny súvisiace s vedou a technikou. Koniec 20. storočia a začiatok 21. storočia možno označiť za modernú dobu, charakteristickú rozsiahlym využívaním informačno-komunikačných technológií, akými sú počítače, mobilné telefóny, platobné karty či televízia. Jedným z najvýznamnejších informačno-komunikačných technológií je bezpochyby celosvetová sieť sietí – Internet, ktorý významnou mierou prispel k zmene fungovania viacerých procesov od obojsmernej komunikácie cez elektronický obchod až po autorské právo. Momentálne stále prebieha explozívny rozvoj novodobých technológií a tento postupne mení industriálnu spoločnosť na spoločnosť informačnú, pričom vzhľadom na rýchlosť a globálnosť týchto zmien sa niekedy hovorí aj o informačnej revolúcii.[2] Uvedené skutočnosti a predovšetkým Internet majú obrovský dopad na práva a záujmy fyzických a rovnako právnických osôb, a prinášajú viaceré výzvy, ktorým musí súčasná právna úprava neustále čeliť.

---

1 Slovník Jazykovedného ústavu Ľudovíta Štúra. Dostupné na: http://slovnik.juls.savba.sk/

2 VLÁDA SLOVENSKEJ REPUBLIKY: Politika informatizácie spoločnosti v Slovenskej republike. Bratislava, 2001.

Je zrejmé, že téma difamácie na Internete je v súčasnosti pertraktovaná čoraz častejšie, a to nielen v spomínaných Spojených štátoch amerických, ale tiež v jednotlivých štátoch Európskej únie, vrátane Slovenskej republiky. Z týchto a ďalších dôvodov sme si položili otázky, či je internetová difamácia v slovenskom právnom poriadku upravená dostatočne a či jednotlivé zákony príslušných oblastí regulujú všetky vznikajúce spoločenské vzťahy s ohľadom na rozmáhajúci sa Internet. Cieľom príspevku je zanalyzovať difamáciu a jej právny stav de lege lata v podmienkach Slovenskej republiky a upriamiť pozornosť na prienik informačno-komunikačných technológií do tejto oblasti. Na základe analýzy je potrebné poukázať na zistené nedostatky a v nadväznosti na ne poskytnúť úvahy a návrhy na odstránenie nežiaducich následkov difamačného konania, ktoré sú mnohokrát veľmi vážne. Pri rozbore problematiky difamácie na Internete je nutné vychádzať z teoretických prameňov, ktorými sú najmä zahraničné a domáce publikácie venované tejto a súvisiacim témam, taktiež pozitívnoprávna úprava jednotlivých konaní, ktoré možno identifikovať ako difamáciu, predovšetkým slovenské zákony, ale i dokumenty Európskej únie.

2 TEORETICKÉ VÝCHODISKÁ DIFAMÁCIE

2.1 Objasnenie pojmu difamácia

Judikatúra amerického common law systému postupne definovala difamáciu ako: *„publikáciu alebo komunikáciu nepravdivého tvrdenia, ktoré sa odráža na reputácii osoby (obchodnej spoločnosti, produktu, skupiny osôb, náboženstva alebo národa) a smeruje k zníženiu jej vážnosti v očiach iných osôb alebo smeruje k tomu, aby sa verejnosť tejto osoby stránila alebo sa jej vyhýbala."* [3] Tu je potrebné zdôrazniť, že difamácia neevokuje iba zásah do osobnostných práv jedinca, ale týka sa aj porušovania práv podnikateľov či skupín osôb a taktiež ju možno vzťahovať na veci a produkty.

Teoretici, ktorí spracovali problematiku difamácie (vrátane jej internetovej podoby) stanovili schému, ktorá charakterizuje určité pojmové znaky difamácie. Sú nimi:

- *nepravdivé alebo falošné tvrdenie o niekom (niečom inom),*
- *zverejnenie nepravdivého alebo falošného tvrdenia tretím osobám,*
- *spôsobenie škody / ujmy*.[4]

Na základe uvedenej schémy môžeme opačne konštatovať, že difámacie sa nedopustí ten, kto len vyjadruje svoj osobný názor, uverejňuje pravdivý fakt, komunikuje nepravdivé alebo falošné tvrdenie iba osobe, ktorej sa týka alebo svojim konaním nespôsobí škodu, resp. ujmu.

2.2 Difamácia na internete

Difamačné konanie možno spáchať verbálne na verejnosti alebo prostredníctvom písaného textu, a to buď v tlačenej alebo elektronickej podobe. Práve posledná uvedená forma sa stáva čoraz viac využívanou a najmä zneužívanou. Internetové prostredie poskytuje možnosť vyjadriť sa, uviesť vyhlásenie či zverejniť článok v podstate všetkým osobám, ktoré sú pripojené k tejto globálnej sieti, a to v rámci takmer neobmedzeného priestoru, v jednom okamihu a bez predchádzajúcej kontroly. Najobávanejším faktorom v rámci Internetu je skutočnosť, že umožňuje anonymné pôsobenie, ktoré prináša viacero právnych i neprávnych problémov. Z právnej stránke ide predovšetkým o sťažené identifikovanie totožnosti páchateľov a taktiež zabezpečovanie dôkazov v prípadnom súdnom alebo priestupkovom konaní. Z tých neprávnych možno spomenúť porušovanie etiky či morálnych noriem.

Vzhľadom na celosvetový rozmach spoločnej siete a prudký rozvoj ďalších informačno-komunikačných technológií vznikla postupne kybernetická difamácia,[5] ktorá v sebe zahŕňa okrem iného aj užšiu skupinu prípadov, a to internetovú difamáciu, teda difamáciu páchanú vo virtuálnom

---

[3] DRAHAMAN, C. Defamation on the Internet, s. 3.
LeROY MILLER, R. Business Law Today: The Essentials, s. 127.

[4] O'CONNELL, K. INTERNET LAW - UNDERSTANDING INTERNET DEFAMATION. DOSTUPNÉ NA: HTTPS://WWW.IBLS.COM/INTERNET_LAW_NEWS_PORTAL_VIEW.ASPX?S=LATESTNEWS&ID=1874

[5] Difamáciu možno spáchať v kyberpriestore, ktorým označujeme celý virtuálny svet vytváraný modernými technológiami. Môže teda ísť aj o prostredie fungujúce mimo svetovej siete Internet. V príspevku sme sa však zamerali na difamáciu páchanú na Internete a z toho dôvodu sa budeme v jeho ďalších častiach venovať len tejto vymedzenej oblasti.

prostredí Internetu. Jej osobitosť spočíva práve v spomínanej možnosti pôsobiť a konať anonymne.

Okrem toho možno kybernetickú difamáciu spáchať aj prostredníctvom elektronických komunikácií, ktoré nie sú nutne spojené s Internetom. Podľa autora Schwabacha riešenie difamácie vzťahujúcej sa na Internet samo o sebe nevytvára žiadny právny problém, avšak globálna povaha Internetu znamená, že vyhlásenie urobené v jednej právnej jurisdikcii môže byť prijímané kdekoľvek na svete, napríklad v krajine, kde by táto problematika mohla byť upravená inak alebo vôbec.[6] Napriek tomu, že základné ponímanie ochrany práv človeka sa príchodom Internetu nezmenilo, podstatne sa zmenilo, resp. doplnilo prostredie, v ktorom majú byť tieto práva chránené. Je preto potrebné zdôrazniť, že ľudia majú svoje práva aj vo virtuálnom prostredí a taktiež, že Internet nie je anonymný absolútnym spôsobom.

3 DIFAMÁCIA V PRÁVNOM PORIADKU SLOVENSKEJ REPUBLIKY

Predmetom a primárnym cieľom predkladaného príspevku je uskutočnenie analýzy internetovej difamácie v prostredí právneho poriadku Slovenskej republiky. Konkrétne, v akých ustanoveniach a akých právnych odvetví môžeme identifikovať konania spĺňajúce znaky difamácie, ako je upravená právna zodpovednosť za tieto konania a či je národná právna úprava postačujúca.

Na základe štúdia dostupných prameňov, predovšetkým právnych predpisov a odborných článkov, môžeme konštatovať, že difamácia sa dotýka tak práva súkromného, ako i práva verejného. Vo všetkých zistených prípadoch ide o delikty a z toho dôvodu rozdeľujeme ďalšiu časť príspevku na dve samostatné podkapitoly – súkromnoprávne delikty a verejnoprávne delikty, ktoré budeme ďalej rozčleňovať.

3.1 Súkromnoprávne delikty

Súkromnoprávne delikty predstavujú protiprávne konania najmä v oblasti občianskeho práva, obchodného práva a pracovného práva, ktoré zakladajú zodpovednostný vzťah medzi protiprávne konajúcim a poškodeným. V nadväznosti na to uvádzame dve skupiny prípadov, v rámci ktorých sme vymedzili znaky difamácie. Kritériom pre rozdelenie bolo právne postavenie poškodenej strany, a teda buď ide o konanie porušujúce práva fyzických osôb alebo práva právnických osôb. Na základe uvedeného uvádzame nasledujúce porušenia:

a) porušenie práva na ochranu osobnosti,
b) nekalá súťaž.

Ad a) Porušenie práva na ochranu osobnosti

V prípade porušovania osobnosti možno za difamáciu považovať občianskoprávny delikt, ktorý predstavuje porušenie práva na ochranu osobnosti podľa ustanovenia § 11 Zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov (ďalej len ako „Občiansky zákonník“).[7] Ochrana osobnosti, resp. osobnostné práva majú viac zložiek a v prípade difamácie môžeme hovoriť o porušení práva na česť a ľudskú dôstojnosť. Táto právna ochrana je výrazom článku 10 ods. 1 Listiny základných ľudských práv a slobôd.[8]

Občianskoprávna ochrana sa poskytuje len proti takým konaniam, ktoré sú objektívne spôsobilé privodiť ujmu na osobnosti subjektu práva tým, že znižujú jeho česť u iných ľudí a pritom ohrozujú vážnosť jeho postavenia a uplatnenie v spoločnosti. Predmetom práva na česť v zmysle občianskeho práva tak nie je česť abstraktná, ale výlučne vážnosť, ktorú subjekt práva na česť požíva v očiach členov spoločnosti, ku ktorej náleží. Preto nie je porušením práva na česť napr. slovná urážka prenesená len medzi štyrmi očami a ani akékoľvek iné konanie, ktoré nie je objektívne spôsobilé česť subjektu práva u iných ľudí znížiť.[9] S týmto tvrdením sa stotožňujeme a dopĺňame, že korešponduje s druhým bodom schémy difamácie.

---

[6] SCHWABACH, S. Internet and the Law. Technology, Society, and Compromises, s. 68.

[7] Ustanovenie § 11 Občianskeho zákonníka: „*Fyzická osoba má právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy*.“

[8] Článok 10 ods. 1 Listiny základných ľudských práv a slobôd: *„Každý má právo na zachovanie svojej ľudskej dôstojnosti, osobnej cti, dobrej povesti a na ochranu mena.“*

[9] KNAP, K. a kol. Ochrana osobnosti podle občanského práva, s. 305.

Fyzická osoba, ktorá bola dotknutá zásahom do svojej osobnosti, je oprávnená sa domáhať prostredníctvom žaloby na príslušnom súde viacerých zákonných nárokov, a to najmä:

- *upustenia od neoprávnených zásahov,*
- *odstránenia následkov týchto zásahov,*
- *primeraného zadosťučinenia* (napr. vo forme ospravedlnenia).[10]

Domnievame sa, že pre osobu poškodenú difamáciou bude významná práve ochrana spočívajúca v primeranom zadosťučinení, pretože zastavenie porušovania cti alebo ľudskej dôstojnosti či odstránenie následkov môže byť v niektorých situáciách nepostačujúce. V týchto prípadoch ide mnohokrát „len" o aktuálny výsledok obrany, ktorý však nemá vplyv na ďalšie vonkajšie vnímanie danej osoby, ktorej česť alebo dôstojnosť bola na verejnosti už raz napadnutá. Okrem toho môže poškodený vymáhať primerané zadosťučinenie v peniazoch, a to vtedy, ak by sa vzhľadom na značnú mieru zníženia dôstojnosti alebo vážnosti nezdalo dané primerané zadosťučinenie postačujúce.[11]

Ad b) Nekalá súťaž

Iným súkromnoprávnym deliktom, konkrétne obchodnoprávnym, ktorý vykazuje znaky difamácie, je nekalá súťaž, ktorá poškodzuje právnické osoby. Táto problematika je upravená v ustanovení § 44 Zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len ako „Obchodný zákonník").[12] Nekalosúťažné konanie je v nasledujúcich zákonných ustanoveniach priblížené na základe demonštratívneho výpočtu skutkových podstát, napr. parazitovanie na povesti, klamlivá reklama alebo porušovanie obchodného tajomstva. V súčasnej dobe, ktorá je charakteristická veľkým konkurenčným bojom o zákazníka za použitia rôznorodých praktík, sa čoraz častejšie objavujú ďalšie konania, ktoré spĺňajú definíciu nekalej súťaže a môžu predstavovať difamáciu. Ide napríklad o osočovanie, poškodzovanie dobrého mena či povesti.

Zákonodarca upravil v Obchodnom zákonníku možnosť podnikateľa brániť sa proti nekalej súťaži, a to prostredníctvom žaloby na príslušnom súde. Podnikateľ má právo najmä sa domáhať:

- *zdržania sa nekalosúťažného konania,*
- *odstránenia závadného stavu,*
- *primeraného zadosťučinenia* (napr. vo forme ospravedlnenia),
- *náhrady škody a vydania bezdôvodného obohatenia.* [13]

Forma primeraného zadosťučinenia môže v týchto prípadoch predstavovať peniaze, ale taktiež ospravedlnenie, ktoré je v podmienkach Slovenskej republiky pomerne využívané, a to najmä v televíznych médiách. Aj v prípade podnikateľských subjektov je na mieste zvýrazniť, že obchodné meno a dobrá povesť sú jednými z najdôležitejších elementov úspechu a prípadná ujma spôsobená difamáciou môže mať aj nehmotnú podobu. Najčastejšie pôjde o prípady zníženia potenciálneho zisku, značný pokles zákazníkov, zníženie hodnoty značky či narušenie budovaného vzťahu medzi zákazníkmi a spoločnosťou.

3.2 Verejnoprávne delikty

Verejnoprávne delikty predstavujú protiprávne konania v oblasti verejného práva, pri ktorých vzniká zodpovednostný vzťah medzi štátom a porušiteľom právnej povinnosti, ktorý je povinný niesť zodpovednosť za vlastné zavinené protiprávne konanie. Medzi verejnoprávne delikty patria trestné činy, priestupky a iné správne delikty. Pri štúdiu súvisiacich zákonov sme dospeli k záveru, že aj v rámci tejto kategórie možno nachádzať prípady difamácie, ktoré môžu dosahovať negatívne následky najmä v širokom internetovom prostredí. Konkrétnymi prípadmi, ktoré považujeme za difamáciu sú:

a) trestný čin ohovárania,
b) priestupok proti občianskemu spolunažívaniu.

---

[10] Ustanovenie § 13 Občianskeho zákonníka.
[11] Ustanovenie § 12 ods. 2 Občianskeho zákonníka.
[12] Ustanovenie § 44 ods. 1 Obchodného zákonníka: *„Nekalou súťažou je konanie v hospodárskej súťaži, ktoré je v rozpore s dobrými mravmi súťaže a je spôsobilé privodiť ujmu iným súťažiteľom alebo spotrebiteľom. Nekalá súťaž sa zakazuje."*
[13] Ustanovenie § 53 ods. 1 Obchodného zákonníka.

Ad a) Trestný čin ohovárania

Trestnoprávny delikt s názvom Ohováranie je upravený v ustanovení § 373 Zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov (ďalej len ako „Trestný zákon"), a to v troch odsekoch.[14] Na základe legálnej definície ohovárania a jednotlivých znakov tejto skutkovej podstaty môžeme konštatovať, že sa najviac približuje objasneniu difamácie, ktorú sme rozoberali v druhej časti predkladaného príspevku. Kvalifikovaná skutková podstata tohto trestného činu predpokladá jeho spáchanie jedným z uvedených spôsobov, medzi ktorými je prípad, kedy je ohováranie spáchané verejne. Z iných ustanovení Trestného zákona je zrejmé, že spáchať trestný čin verejne možno aj použitím počítačovej siete, čo v tomto prípade napĺňa jeden zo znakov internetovej difamácie. Negatívom páchania trestného činu v prostredí siete Internet je jeho spomínaná eventualita anonymity, ktorá môže predstavovať podstatné sťaženie v procese pátrania po páchateľovi a jeho identifikovania. Súhlasíme s názorom autora Smejkala, že kvalifikácia skutku bude evidentná, ale problémy môžu nastať v rovine dôkaznej.[15]

Pre tento trestný čin sa vyžaduje úmyselné zavinenie a ochrana sa uplatňuje na základe trestného oznámenia. Trestná sadzba sa pohybuje v rámci jednotlivých skutkových podstát od dvoch do osem rokov, čo v prípade uvedenej najvyššej hranice predstavuje najprísnejší trest spomedzi všetkých členských štátov Európskej únie, ktoré majú vo svojich právnych poriadkoch upravený tento typ deliktu.[16] Zaujímavosťou je fakt, že niektoré štáty nemajú ohováranie zaradené medzi trestnoprávne konania a vyvodzujú voči nemu iba súkromnoprávnu zodpovednosť. Ide napríklad o Rumunsko, Veľkú Britániu či Estónsko.[17] Podľa porovnávacej správy Medzinárodného tlačového inštitútu z roku 2015 vzniká v Európskej únii postupne trend smerujúci k zrušeniu trestnoprávnej zodpovednosti za ohováranie.[18] Vzhľadom na neustále sa rozširujúci Internet a rozvoj ďalších informačno-komunikačných technológií sa na to možno pozerať z dvoch strán. V prvom rade ide o nebezpečné, virtuálne a nikde nekončiace prostredie, ktoré umožňuje páchať ohováranie v obrovskom rozmere a z toho dôvodu je potrebné prísne strážiť práva poškodených a pôsobiť tiež preventívne. Na strane druhej, ten istý fakt, teda globalizácia a všadeprítomné prepojenie reálneho a virtuálneho sveta prináša novú éru spoločnosti, v ktorej moderné technológie napredujú veľkou rýchlosťou a doterajšie postupy ochrany možno nebudú ďalej postačovať.

Ad b) Priestupok proti občianskeho spolunažívaniu

Jednou z kategórií verejnoprávnych deliktov, ktoré sme podrobili analýze sú správne delikty, konkrétne jeden druh, ktorým je priestupok. Priestupky sú, okrem početného množstva osobitných predpisov, upravené v Zákone č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (ďalej len ako „Zákon o priestupkoch"). Spomedzi viacerých priestupkov sme identifikovali znaky difamácie v prípade priestupku proti občianskemu spolunažívaniu podľa ustanovenia § 49 ods. 1, písm a) Priestupkového zákona.[19] Ublíženie na cti urazením alebo vydaním na posmech môže byť vykonané rôznymi spôsobmi, pričom spáchanie prostredníctvom Internetu nie je vylúčené.

Pre vznik zodpovednosti za tento priestupok postačuje zavinenie z nedbanlivosti a ide o návrhový priestupok. Po uznaní viny možno páchateľovi uložiť pokutu do výšky 33 Eur. Sme toho názoru, že rovnako ako v prípade trestných činov spáchaných na Internete, aj v tomto prípade môže dôjsť k zhoršeniu pozície objasňujúcich orgánov, ktoré musia disponovať vyspelou technikou a modernými metódami, aby odhalili páchateľa, ktorý vo väčšine prípadov dokáže svoje konanie anonymizovať dokonalým spôsobom.

---

[14] Ustanovenie § 373 ods. 1 Trestného zákona: *„Kto o inom oznámi nepravdivý údaj, ktorý je spôsobilý značnou mierou ohroziť jeho vážnosť u spoluobčanov, poškodiť ho v zamestnaní, v podnikaní, narušiť jeho rodinné vzťahy alebo spôsobiť mu inú vážnu ujmu."*

[15] SMEJKAL, V. Kybernetická kriminalita, s. 341.

[16] INTERNATIONAL PRESS INSTITUTE. Out of Balance: Defamation Law in the European Union. Dostupné na:
http://legaldb.freemedia.at/wp-content/uploads/2015/05/IPI-OutofBalance-Final-Jan2015.pdf

[17] Tamtiež.

[18] Tamtiež.

[19] Ustanovenie § 49 ods. 1, písm. a) Priestupkového zákona: *„Priestupku sa dopustí ten, kto inému ublíži na cti tým, že ho urazí alebo vydá na posmech."*

4 ZODPOVEDNOSŤ ZA DIFAMÁCIU NA INTERNETE

Vyvodzovanie zodpovednosti za protiprávne konanie je jedným zo základných znakov právneho štátu a je nevyhnutné pre ochranu práv a záujmov fyzických i právnických osôb. Vyššie rozoberané klasifikácie difamácie (identifikované v rámci súkromnoprávnych a verejnoprávnych deliktov) možno spáchať rôznymi spôsobmi. V ďalšej časti príspevku priblížime, kto v daných prípadoch prichádza do úvahy ako osoba zodpovedná za difamáciu a jej následky. Konkrétne spôsoby, ktorými možno spáchať porušenie ochrany osobnosti, nekalú súťaž, trestný čin ohovárania alebo priestupok urážky na cti a vydania na posmech sú, ako formy difamácie, nasledovné:

a) verbálne na verejnosti,
b) prostredníctvom tlače,
c) prostredníctvom rozhlasu a televízie,
d) prostredníctvom Internetu.

Ad a) Difamácia páchaná verbálne na verejnosti

V tomto prípade sa volá na zodpovednosť osoba, ktorá povedala difamačné tvrdenie a jej konaním boli naplnené znaky niektorého z deliktov. Pripomíname, že o difamáciu ide vždy vtedy, ak dôjde k zverejneniu difamačného tvrdenia na verejnosti, to znamená, že okrem osoby, voči ktorej tvrdenie smeruje, sa na mieste musí nachádzať aj iná osoba.

Ad b) Difamácia páchaná prostredníctvom tlače

Ohováranie, porušenie ľudskej dôstojnosti alebo povesti podnikateľa je možné spáchať aj prostredníctvom tlače. Na prvom mieste je vždy zodpovedná osoba, ktorá difamačný príspevok zverejnila, teda vydavateľ, ktorý zodpovedá za obsah konkrétnych novín alebo časopisu. Jeho práva a povinnosti upravuje Zákon č. 167/2008 Z. z. o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon) v znení neskorších predpisov (ďalej len ako „Tlačový zákon“). Zákonodarca v tomto zákone upravil inštitút práva na odpoveď [20], ktorý poskytuje priamu ochranu osobe, voči ktorej bol v tlači uverejnený difamačný príspevok. Podrobnosti o uplatnení tohto práva a o vylúčení zodpovednosti vydavateľa sú obsahom nasledujúcich odsekov uvedeného paragrafu.

Ad c) Difamácia páchaná prostredníctvom rozhlasu a televízie

Ďalším spôsobom, ktorým môže dôjsť k difamácii, je prostriedok rozhlasu alebo televízie. Postavenie, poslanie a úlohy týchto inštitúcií upravuje Zákon č. 532/2010 Z. z. o Rozhlase a televízii Slovenska a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len ako „Zákon o rozhlase a televízii“). Samotné vysielanie je následne upravené v Zákone č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov (ďalej len ako „Zákon o vysielaní“). Tento predpis zakazuje vysielateľom zasahovať spôsobom svojho spracovania a svojím obsahom do ľudskej dôstojnosti a základných práv a slobôd iných.[21] Okrem toho zákon obsahuje inštitút práva na opravu, a to v podobnom znení ako Tlačový zákon[22], ale neupravuje právo na odpoveď, ktorá sa týka prípadov zásahov do ľudskej osobnosti alebo cti. To znamená, že ak dôjde k takýmto neoprávneným aktom v televízii alebo v rozhlase, poškodené osoby sa môže brániť súdnou cestou.

Ad d) Difamácia páchaná prostredníctvom Internetu

---

[20] Ustanovenie § 8 ods. 1, prvá veta Tlačového zákona: *„Ak periodická tlač alebo agentúrne spravodajstvo obsahuje nepravdivé, neúplné alebo pravdu skresľujúce skutkové tvrdenie, ktoré sa dotýka cti, dôstojnosti alebo súkromia fyzickej osoby, alebo názvu alebo dobrej povesti právnickej osoby, na základe ktorého možno osobu presne určiť, má táto osoba právo žiadať uverejnenie odpovede.“*

[21] Ustanovenie § 19 ods. 1, písm. a) Zákona o vysielaní.

[22] Ustanovenie § 21 ods. 1 Zákona o vysielaní: *„Ak bol vo vysielaní odvysielaný nepravdivý alebo pravdu skresľujúci údaj o právnickej osobe alebo o fyzickej osobe, ktorú možno na základe tohto údaja presne určiť, táto právnická osoba alebo fyzická osoba má bez ohľadu na svoju štátnu príslušnosť, miesto trvalého pobytu alebo dlhodobého pobytu právo požadovať odvysielanie opravy bezplatne. Vysielateľ je povinný na žiadosť tejto osoby opravu uverejniť.“*

Ak dôjde k difamácii v internetovom prostredí, zodpovednou osobu bude v prvom rade páchateľ, ktorého buď možno identifikovať alebo nemožno. Okrem neho prichádza do úvahy aj poskytovateľ služby informačnej spoločnosti (napr. poskytovateľ siete Internet alebo prevádzkovateľ webovej stránky).[23]

Táto problematika je podrobne upravená v Smernici č. 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (ďalej len ako „Smernica o elektronickom obchode"), podľa ktorej je poskytovateľ služieb informačnej spoločnosti zodpovedný za jej obsah, ak:

- *iba ukladá informácie, resp. obsah poskytnutý užívateľom webovej stránky na jeho žiadosť,*
- *nemá vedomosť o protiprávnosti ukladaného obsahu alebo nezákonnej činnosti užívateľa,*
- *po zistení takej skutočnosti neodkladne koná a dotknutý obsah odstráni.*[24]

Podobným spôsobom upravuje zodpovednosť poskytovateľa služieb informačnej spoločnosti za obsah tretích strán aj náš Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. (ďalej len ako „Zákon o elektronickom obchode"). Vo svojich súvisiacich paragrafoch stanovuje, že: *„poskytovateľ služieb informačnej spoločnosti nie je povinný sledovať informácie ani nie je oprávnený vyhľadávať informácie, ktoré sa prenášajú alebo ukladajú. Ak sa však dozvie o protiprávnosti takých informácií, je povinný odstrániť ich z elektronickej komunikačnej siete. Súd môže nariadiť poskytovateľovi služieb ich odstránenie z elektronickej komunikačnej siete aj vtedy, ak sa poskytovateľ služieb o ich protiprávnosti nedozvedel."* [25] Zákon o elektronickom obchode neupravuje iné nároky poškodenej osoby a v prípade záujmu sa táto môže obrátiť na súd a žiadať primerané zadosťučinenie vo forme peňazí alebo verejného ospravedlnenia.

V tejto súvislosti možno upriamiť pozornosť na rozsudok senátu Krajského súdu v Trenčíne, ktorý je prvým slovenským druhostupňovým rozhodnutím týkajúcim sa zodpovednosti na Internete za užívateľský obsah. Súd v tomto spore rozhodol v zmysle ustálenej európskej judikatúry, že prevádzkovateľ webovej stránky s nemoderovanou diskusiou (alebo poskytovateľ diskusného fóra) v zásade nezodpovedá za obsah diskusie. Ide o správnu aplikáciu bezpečného prístavu hosting podľa ustanovenia § 6 ods. 4 Zákona o elektronickom obchode, ktorý vyplýva zo Smernice o elektronickom obchode. Na druhej strane súd taktiež rozhodol, že diskusný príspevok musí byť zmazaný, pretože: *„Výrazy, ktoré sú obsiahnuté v príspevkoch, súd vyhodnotil ako protiprávne, a preto je žalovaný povinný ich odstrániť."* [26] Krajský súd ďalej rozhodol, že žalovaný nemusí zaplatiť náhradu nemajetkovej ujmy v peniazoch a tiež nemusí zverejniť ospravedlnenie, ktoré predstavovali nároky uplatnené zo strany poškodeného. Súhlasíme s názorom autora Husovca, že Najvyšší súd Slovenskej republiky by sa mal seriózne zaoberať otázkou, kedy a za akých okolností by mali poskytovatelia diskusného fóra niesť zodpovednosť aj za peňažné nároky (škoda, nemajetková ujma v peniazoch, prípadne bezdôvodné obohatenie), ak neodstránili určité príspevky alebo výrazy ihneď ako o to boli požiadaní, či inak nadobudli o ich existencii skutočnú vedomosť. V týchto prípadoch, keď poskytovateľ stratí "plátený štít" bezpečného prístavu podľa ustanovenia § 6 ods. 4 Zákona o elektronickom podpise, musí totiž všeobecný súd na základe konkrétnych okolností prípadu posúdiť, či poskytovateľ diskusného fóra sám spáchal delikt tým, že ponechal príspevky na svojej

---

[23] Ustanovenie § 2 písm. a) Zákona o elektronickom obchode: *„Poskytovateľom služieb informačnej spoločnosti je fyzická osoba alebo právnická osoba, ktorá na účely podnikania alebo na iné účely poskytuje služby informačnej spoločnosti; ak je poskytovateľ služieb podnikateľom, umiestnenie elektronických zariadení potrebných na poskytovanie služieb informačnej spoločnosti nie je pre určenie sídla alebo miesta podnikania rozhodujúce."*

[24] Článok 14 Smernice o elektronickom obchode. Dostupné na: http://eurlex.europa.eu/legalcontent/sk/ALL/;jsessionid=F8p2TxKGP5vkfM7TCJKp9HZ2R5sX7m85wWLCxjr46KhQqrhdhvDm!-1847652702?uri=CELEX:32000L0031

[25] Ustanovenie § 6 ods. 5 Zákona o elektronickom obchode.

[26] Rozhodnutie Krajského súdu Trenčín zo dňa 26. apríla 2012 vydané vo veci *Stacho v Klub Strážov, o.z.,* sp. zn. 19Co/35/2012.

platforme, a to aj napriek žiadosti o ich odstránenie pre údajnú protiprávnosť. Najvyšší súd Slovenskej republiky by mal preto formulovať určitý test, ktorý predvídateľne stanoví, kedy takáto omisia zo strany poskytovateľa diskusného fóra zakladá jeho zodpovednosť za škodu alebo náhradu nemajetkovej ujmy v peniazoch za osobnostnoprávny delikt. Takýto test pritom vyžaduje citlivý ústavnoprávny balans.[27]

5 ZÁVER

Internet sa stal globálnym fenoménom otvárajúcim nové možnosti fungovania rôznych procesov a konaní, čo na jednej strane prináša mnohé pozitíva, ktoré možno vnímať tak v sociologickom ponímaní, ekonomickom, ako i právnom. Na druhej strane nemožno opomínať riziká a nevýhody, ktoré so sebou prináša. Moderné technológie majú vždy náskok, sú krok vpred a právna úprava na ne musí neustále reagovať. Za najkritickejší bod považujeme možnosť fungovať v tomto priestore anonymne, čo sťažuje identifikáciu osôb a okrem právnych následkov môžeme hovoriť aj o negatívnom psychologickom hľadisku, pretože páchatelia sú si vedomí tejto „výhody" a dodáva im to sebadôveru konať ďalej a mnohokrát výraznejšie. Ďalším faktorom je, že Internet má takmer neobmedzený územný, osobný i časový dosah. Oproti minulosti dokáže zverejniť informáciu a v danej sekunde je táto rozšírená na celom svete, pričom navrátenie predchádzajúceho stavu je vzhľadom na eventuálne sťahovanie údajov, nemožné. Okrem toho, príspevky na Internete nepodliehajú v niektorých prípadoch žiadnej kontrole, ako tomu je pri iných nástrojoch verejnej publikácie (napr. tlač alebo televízia).

Za konkrétne nedostatky v právnej úprave považujeme to, že žiaden z rozoberaných právnych predpisov neupravuje právo fyzickej osoby alebo právnickej osoby na ospravedlnenie, odpoveď alebo inú podobnú priamu reakciu v prípade uverejnenia difamácie na Internete. Sme toho názoru, že systém upravený v Tlačovom zákone by sa mohol adekvátne uplatniť aj pre podobné prípady, ktoré sa udejú vo virtuálnom priestore. Toho času sa Tlačový zákon vzťahuje iba na periodickú tlač a agentúrne spravodajstvo. Následky difamácie (napr. poškodenie reputácie, zníženie vážnosti, zosmiešnenie, urazenie na cti) sú vážne, ale v prípade difamácie na Internete môžu byť pre poškodeného mnohokrát závažnejšie. Avšak, poškodený má v tomto prípade nerovnaké možnosti ochrany svojich práv v porovnaní s inými formami difamácie (napr. prostredníctvom spomínanej tlače), pretože jeho jedinou možnosťou je podať žalobu alebo trestné oznámenie.

Na základe uvedeného navrhujeme zapracovať rýchlejší a jednoduchší spôsob ochrany práv pre prípady ich porušovania difamáciou na Internete. V niektorých krajinách Európskej únie, napríklad v Írsku alebo vo Veľkej Británii existujú samostatné zákony upravujúce rôzne druhy difamačného konania na Internete. Jedným zo spôsobov je právna úprava doteraz neregulovaných spôsobov uverejňovania informácií, akými sú napríklad webové noviny, časopisy, súkromné blogy, diskusie či portály prezentujúce videá. Samostatnou kapitolou sú sociálne siete, ktoré fungujú na princípe registrácie, na základe ktorej užívateľ súhlasí s podmienkami prevádzkovateľa.

Na záver by sme chceli upriamiť pozornosť na riešenie anonymity Internetu, ktoré zatiaľ funguje v oblasti verejnej moci, a to vo viacerých štátoch sveta. Ide o tzv. digitálnu identitu predstavujúcu informácie o konkrétnej osobe uchovávané a prenášané v elektronickej forme. Digitálna identita už nie je len problematikou sociálnych médií, ale v súčasnej informačnej spoločnosti, kedy entity vstupujú do rôznych právnych vzťahov prostredníctvom virtuálneho priestoru, sa stáva viac a viac relevantnou.[28] Fyzické osoby môžu identifikovať a tiež autentifikovať svoju totožnosť aj vo virtuálnom priestore, a to prostredníctvom elektronických občianskych preukazov. To, či by bolo možné použiť tieto prostriedky na overenie totožnosti aj v komerčnej sfére, je zatiaľ otázne.

Tento príspevok vznikol v rámci riešenia vedeckého projektu s názvom: "Identifikácia a autentifikácia ako základné predpoklady poskytovania a využívania elektronických služieb verejnej správy." Grant UK č. UK/270/2016.

[27] HUSOVEC, M. Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osôb, s. 47.

[28] ANDRAŠKO, J. Digitálna identita vo verejnej správy, s. 59.

Použitá literatúra

ANDRAŠKO, J. Digitálna identita vo verejnej správy. In: Kontroverzní názory v právu. Sborník z konference Olomoucké debaty mladých právniku 2015. Praha: Leges, 2015. s. 59 - 64. ISBN: 978-80-7502-3.

c) O'CONNELL, K. Internet Law - Understanding Internet Defamation. www.ibls.com

DRAHAMAN, C. Defamation on the Internet. Malaysia: Business Law Review, 2006. č. 1.

HUSOVEC, M. Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osôb. In: Revue pro právo a technologie, 2012. č. 6, s. 45 - 48. ISSN 1805-2797 (Online).

KNAP, K. a kol. Ochrana osobnosti podle občanského práva. Praha: Linde, 2004. 435 s. ISBN 80-7201-484-6.

INTERNATIONAL PRESS INSTITUTE. Out of Balance: Defamation Law in the European Union. Austria: International Press Institute, 2015. 88 s.

LeROY MILLER, R. Business Law Today: The Essentials. United States: South-Western Cengage Learning, 2001. ISBN 1-133-19135-5.

SCHWABACH, S. Internet and the Law. Technology, Society, and Compromises. Oxford: ABC-CLIO, 2014. 352 s. ISBN 978-1-61069-349-3.

SMEJKAL, V. Kybernetická kriminalita. Praha: Alex Čeněk, 2015. 640 s. ISBN: 9788073805012.

d) VLÁDA SLOVENSKEJ REPUBLIKY: Politika informatizácie spoločnosti v Slovenskej republike. Bratislava, 2001.

Smernica č. 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode

Ústavný zákon č. 23/1991 Zb. Ústavný zákon, ktorým sa uvádza LISTINA ZÁKLADNÝCH PRÁV A SLOBÔD ako ústavný zákon Federálneho zhromaždenia Českej a Slovenskej Federatívnej Republiky

Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z.

Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

Zákon č. 167/2008 Z. z. o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon) v znení neskorších predpisov

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov

Zákon č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov

Zákon č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov

Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

Zákon č. 532/2010 Z. z. o Rozhlase a televízii Slovenska a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Rozhodnutie Krajského súdu Trenčín zo dňa 26. apríla 2012 vydané vo veci Stacho v Klub Strážov, o. z., sp. zn. 19Co/35/2012

http://slovnik.juls.savba.sk/

Kontaktné údaje:

JUDr. Soňa Ralbovská Sopúchová, PhD.
sona.sopuchova@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta
Šafárikovo nám. 6, P. O. Box 313
810 00 Bratislava 1
Slovenská republika

KYBERNETICKÝ PRIESTOR A MEDZINÁRODNÉ PRÁVO

Jozef Valuch

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: What is cyberspace? Do established principles of international law apply to this kind of space? ... These and other similar issues related to cyberspace and security are frequently discussed topics in the area of international law nowadays. The author presents the approach adopted by jurisprudence to these and other related issues.

Abstrakt: Čo je to kybernetický priestor? Je možné aplikovať ustálené zásady medzinárodného práva v tomto priestore? ... Tieto a podobné otázky súvisiace s kybernetickým priestorom a bezpečnosťou sú častou témou medzinárodného práva. Autor približuje pohľad právnej vedy na tieto a ďalšie relevantné otázky.

Key words: cyberspace, international law, security

Kľúčové slová: kybernetický priestor, medzinárodné právo, bezpečnosť

1 ÚVOD

O tom, že veda a technika ovplyvňujú život každého jedného z nás omnoho intenzívnejšie ako v minulosti, niet pochýb. S ich výdobytkami prichádzame do kontaktu deň čo deň a mnohí si bežný deň bez nich už ani nevedia predstaviť. Často si pri ich využívaní ani neuvedomujeme, že prekračujeme vnútroštátny rozmer. Mnohé z výdobytkov vedy a techniky už berieme ako samozrejmosť a to vrátane internetu a využívania kybernetického priestoru. V nasledujúcom texte sa snažíme priblížiť túto oblasť z pohľadu medzinárodného práva. Rovnako tak ako rastú možnosti využívania kybernetického priestoru rastie totiž aj počet otázok súvisiacich s ich právnym vymedzením, s ich rozmerom, úpravou a pod. Vyvstávajú tak otázky ako napr.: čo je to vlastne kybernetický priestor? Je možné aplikovať ustálené zásady medzinárodného práva v tomto priestore? Prípadne, ktorá z oblastí medzinárodného práva je najvhodnejšia k tejto aplikácii? Práve tieto a im podobné otázky sú v súčasnosti častou témou odborníkov na medzinárodné právo.

O tom, že ide o tému ktorej je venovaná pozornosť na rôznych fórach, univerzitách, i na pôde medzinárodných organizácií svedčia viaceré fakty. Napríklad na Harwarde existuje Berkmanovo stredisko pre internet a spoločnosť. V rámci Harward Law School pôsobí aj tzv. kyberneticko-právna klinika (*Cyber law clinic*), ktorá poskytuje vysoko kvalifikované právne služby vládnym entitám, neziskovým organizáciám i jednotlivcom. Jej služby sú využívané v rôznych oblastiach právnej praxe ako je činnosť advokátov, legislatíva, riešenie súdnych sporov a pod. Výskumom medzinárodného práva kybernetického priestoru sa zaoberá napr. univerzita v Georgetowne alebo Inštitút OSN pre odzbrojenie (UNIDIR). S výskumom obdobného charakteru sa však možno stretnúť tiež v Ázii a na ďalších kontinentoch.[1]

V súvislosti s otázkami spätými s kybernetickou bezpečnosťou nemožno opomenúť Centrum výnimočnosti pre oblasť spoločnej kybernetickej obrany spolupracujúce s NATO[2] v Tallinne a pod. Okrem viacstranných fór sa problematike kybernetického priestoru venujú aj jednotlivé štáty, keď predovšetkým v súvislosti so zaistením vlastnej bezpečnosti vytvárajú organizačné zložky a inštitúcie rôznej povahy. Tak už v roku 2009 vytvorilo Francúzsko Agentúru pre sieťovú a informačnú bezpečnosť a v tom istom roku zriadila Veľká Británia v rámci Vládneho komunikačného ústredia aj Stredisko kyberneticko-bezpečnostných operácií.[3] Spojené štáty americké zriadili v roku 2010 pri

1 MRÁZEK, J.: Mezinárodní právo v kybernetickém prostoru, s. 538
2 *NATO Cooperative Cyber Defence Centre of Excellence*, https://ccdcoe.org
3 *Cyber Security Operations Centre*

Ministerstve obrany tzv. kybernetické velenie[4] so sídlom v Marylande. V Nemecku funguje Centrum kybernetickej obrany,[5] v Rusku môže riešiť otázky kybernetickej bezpečnosti Ministerstvo obrany i Federálna bezpečnostná služba a v Číne podľa niektorých informácií existujú dve oddelenia generálneho štábu, pričom kybernetickou obranou sa zaoberá viacero útvarov.[6]

2 POJMOVÉ VYMEDZENIE

V nadväznosti na vyššie uvedené považujeme za vhodné hneď na začiatku ozrejmiť niektoré relevantné pojmy, pričom jedným z kľúčových je pojem „kybernetický priestor". Medzinárodní právnici, resp. ich poňatie kybernetického priestoru, je totiž ovplyvnené ich vnímaním toho, ako sú jednotlivé priestory poňaté medzinárodným právom.[7]

Pojem „kybernetický priestor" použil po prvýkrát W. F. Gibson vo svojej krátkej poviedke „*Burning Chrome*" v roku 1982 a následne vo svojej sci-fi novele „*Neuromancer*" v roku 1984.[8] Od tej doby rástla celosvetová popularita tohto pojmu, v súvislosti s rýchlym a nezastaviteľným využívaním kybernetického priestoru vo svete. Kybernetický priestor tak vytvoril špecifickú komunikačnú sieť s osobitým statusom, nepodriadenú v celosti konkrétnej krajine, právu alebo jurisdikcii. V dnešnom novodobom svete tak už nie je pravdou tvrdenie nemeckého filozofa K. Jaspersa, v zmysle ktorého nik nemôže žiadať, aby ho bolo na verejnosti počuť a súčasne aby ostal nepozorovaný.[9] Internet je totiž pavučina sietí (prepojených sietí)[10] v rámci ktorej môže mať elektronická komunikácia presne túto formu, v rámci ktorej bude niekto vypočutý a zároveň zostane nespozorovaný. Toto je to, čo je považované za skutočný „kybernetický priestor".[11]

Inými autormi je kybernetický priestor definovaný napr. ako globálne vzájomne prepojená sieť digitálnych informačných a komunikačných infraštruktúr, vrátane internetu, telekomunikačných sietí, počítačových sietí a informácií v nich obsiahnutých.[12]

Spomedzi rôznych dokumentov možno uviesť napr. americkú Národnú vojenskú stratégiu týkajúcu sa tohto typu priestoru z roku 2006, ktorá kybernetický priestor definuje ako doménu charakterizovanú použitím elektronického a elektromagnetického spektra na ukladanie, úpravu a výmenu dát cez sieťové systémy a pridružené fyzické infraštruktúry.[13]

V súvislosti s bezpečnosťou sa dokonca rôzne ozbrojené zložky zaoberajú kybernetickou bezpečnosťou do tej miery, že kybernetický priestor definovaný americkým Ministerstvom obrany za „globálnu doménu v rámci informačného prostredia pozostávajúcu zo vzájomne prepojenej siete informačných technológií a rezidentných údajov, vrátane internetu, telekomunikačných sietí, počítačových systémov a vstavaných procesorov a riadiacich jednotiek" považujú popri zemskom povrchu, vodnej ploche, vzdušnom priestore a vesmíre za piatu domému na vedenie vojny. Na rozdiel od „tradičných domén" na vedenie vojny je však kybernetický priestor vytvorený človekom a nemá žiadne konkrétne hranice.[14]

---

4 *U.S. Cyber Command - USCYBERCOM*
5 *Cyber - Abwehrzentrum*
6 MRÁZEK, J.: Mezinárodní právo v kybernetickém prostoru, s. 548
7 Bližšie pozri: TSAGOURIAS, N.: The legal status of cyberpsace, s. 15, dostupné na: http://www.e-elgar.com/shop/eep/preview/book/isbn/9781782547396/ (stránka navštívená dňa 19.09.2016)
8 KNORR, A.: The Stability of Cyberspace, s. 194, cit. Podľa: GÁBRIŠ, T.: Cyber Law, s. 14
9 JASPERS, K.: (preklad: Elexová, P.): Malá škola filozofického myslenia, s. 108
10 Interconnected networks = internet
11 GÁBRIŠ, T.: Cyber Law, s. 14 - 15
12 MELZER, N.: Cyber Warfare and International Law, s. 4
13 US, The National Military Strategy for Cyberspace Operations, s. 3 a taktiež napr. Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, Joint Terminology for Cyberspace Operations, November 2010, s. 7, dostupné na: http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (stránka navštívená dňa 11.09.2016)
14 ROSCINI, M.: Cyber Operations and the Use of Force in International Law, s. 9. Porovnaj: Center for Strategic and International Studies, Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization (UNIDIR, 2011), dostupné na: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (stránka navštívená dňa 13.09.2016)

Komplexnejšiu definíciu ponúka D. T. Kuehl, ktorý uvádza, že kybernetický priestor je globálna doména v rámci informačného prostredia, ktorej osobitý a jedinečný charakter je tvorený použitím elektronického a elektromagnetického spektra na tvorbu, ukladanie, úpravu, výmenu a využívanie informácií prostredníctvom vzájomne závislých a vzájomne prepojených sietí s využitím informačno – komunikačných technológií.[15]

Kybernetický priestor sa tak v mnohých ohľadoch odlišuje od doposiaľ známych a využívaných úrovní priestoru. Dlhý čas totiž ľudstvo využívalo len dve úrovne priestoru a to zemský povrch a vodu (resp. more). Neskôr, v dôsledku rozvoja technológií, k nim pribudol aj vzdušný priestor a kozmický priestor a dnes už vieme, že okrem týchto štyroch úrovní priestoru existuje aj piaty a to kybernetický priestor. Práve tento piaty sa však od predošlých uvedených výrazne odlišuje. Má globálny rozmer, ktorý stiera hranice medzi štátmi a funguje bez ohľadu na politický systém, s mimoriadne širokou paletou aktérov od jednotlivcov, cez rôzne zoskupenia až po štáty.[16]

Experti na oblasť informačných technológií dokonca uvádzajú, že nič také ako absolútna bezpečnosť v tomto priestore neexistuje. Pre porovnanie možno uviesť, že v prípade vyššie uvedených štyroch úrovní priestoru bolo na ovládnutie každej z nich v minulosti potrebné disponovať dostatočnými kapacitami. Napríklad pre zaistenie prevahy na mori bolo potrebné disponovať prevažujúcou námornou silou. Oproti tomu je v kybernetickom priestore takmer nemožné dosiahnuť čo i len na kratší čas absolútnu hegemóniu a to vzhľadom na množstvo aktérov, jednoduchosť prístupu a anonymitu. Mimo iného je veľmi náročné určiť napr. zdroj kybernetického útoku.[17] Aj z uvedených dôvodov ide o úroveň priestoru poskytujúcu okrem množstva výhod aj priestor pre kybernetické hrozby a informačnú kriminalitu, ktoré zahŕňajú širokú škálu negatívnych fenoménov rôzneho stupňa závažnosti. Môže ísť o kybernetickú špionáž, hackerstvo, DDoS útoky,[18] či iné nežiaduce aktivity vrátane prejavov extrémizmu a zneužívania internetu k teroristickým aktivitám a propagande (v podobe napr. zverejňovania návodov na konštrukciu výbušnín) a pod.[19] Hrozby tak dnes už nepochádzajú len zo strany hackerov, ale aj zo strany ideologicky motivovaných jednotlivcov (tzv. „*hacktivists*“), štátov, či kriminálnych a teroristických organizácií. Pomerne jednoducho a lacno sa totiž dajú získať kybernetické technológie a potrebné zručnosti, umožňujúce aj slabším štátom a dokonca neštátnym aktérom, spôsobiť značné škody štátom disponujúcim vyspelou konvenčnou armádnou silou. Platí, tak ako sa uvádza aj v „Austrálskej stratégii kybernetickej bezpečnosti“,[20] že predovšetkým v súvislosti s kybernetickým priestorom sa rozdiel medzi tradičnými aktérmi hrozieb – hackermi, teroristami, organizovanými zločineckými sieťami, priemyselnými špiónmi a zahraničnými spravodajskými službami – stále viac stiera.[21]

Podľa viacerých autorov sa kybernetický priestor skladá z troch vrstiev: z fyzickej, syntaktickej a sémantickej. Prvá, fyzická časť, zahŕňa hardware, satelity, káble a iné vybavenie. Syntaktickú časť tvoria počítačové operačné systémy a iný softvér. Sémantická vrstva následne zahŕňa vzájomné pôsobenie ľudského činiteľa a informácií získaných z počítačov, ich vyhodnotenie a využitie

---

15 KUEHL, D. T.: From cyberspace to cyberpower: Defining the problem, s. 28 cit. podľa: TSAGOURIAS, N.: The legal status of cyberpsace, s. 15, dostupné na: http://www.e-elgar.com/shop/eep/preview/book/isbn/9781782547396/ (stránka navštívená dňa 19.09.2016)

16 Bližšie pozri: MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti, s. 55-56

17 Tamtiež, s. 57; Porovnaj: KRAMER, D. F., STARR, H. S., WENTZ, L. KUEHL,D.: Cyberpower and National Security, 664 s.

18 *Distributed Denial of Service* (DDoS)

19 K negatívnym fenoménom spätým s kybernetickým priestorom možno okrem vyššie uvedeného radiť aj internetové podvody a krádeže, zneužívanie osobných údajov, šírenie detskej pornografie, predaj drog na internete, pranie špinavých peňazí s pomocou virtuálnej meny, stalking a pod. Bližšie pozri: Ministerstvo vnútra Českej republiky, Odbor bezpečnostnej politiky: Kybernetické hrozby, 07.05.2014 Dostupné na: http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3d%3d (stránka navštívená dňa 11.09.2016)

20 *Australian Cyber Security Strategy*, 2009

21 ROSCINI, M.: Cyber Operations and the Use of Force in International Law, s. 1-2. Porovnaj: Australian Government, Cyber Security Strategy, 2009, s. 3, dostupné na: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf (stránka navštívená dňa 13.09.2016)

užívateľom.[22] Prípadné kybernetické útoky potom môžu smerovať proti všetkým alebo len niektorým z uvedených vrstiev kybernetického priestoru.[23]

Pri poňatí tohto priestoru medzinárodným právom musíme vychádzať aj z osobitého charakteru medzinárodného práva, ktoré možno definovať aj ako štandard správania, v danom momente pre štáty a ďalšie entity ktoré mu podliehajú.[24] Jedným zo špecifických znakov, plne sa prejavujúcim aj v tejto sfére je skutočnosť, že vzťahy v rámci medzinárodného práva sú založené v zásade na koordinačnom a nie subordinačnom princípe (na rozdiel od vnútroštátneho práva). Štáty ako tradičné subjekty medzinárodného práva spolupracujú v zmysle základných zásad a princípov na báze rovnoprávnosti. Koordinačný charakter medzinárodného práva je potom zdôraznený práve tým, že suverénne štáty majú plnú normotvornú spôsobilosť čo znamená, že nielen že užívajú práva a plnia povinnosti vyplývajúce z medzinárodného práva, ale spoločne s inými štátmi tieto práva a povinnosti aj vytvárajú.[25] Z toho vyplýva, že medzinárodné právo je právom kompromisu, pričom normatívna kvalita pravidla medzinárodného práva závisí od miery kompromisu, ktorý bol potrebný na jej prijatie.[26] Táto skutočnosť sa prejavuje aj v súvislosti s nazeraním na vzťah medzinárodného práva a kybernetického priestoru.

3 VZŤAH KYBERNETICKÉHO PRIESTORU A MEDZINÁRODNÉHO PRÁVA

Napriek tomu, že pokrok vedy a techniky je zjavný, nejde o prvý kontakt medzinárodného práva s technologickým pokrokom. Už predchádzajúce obdobie nám ponúka minimálne dva príklady, kedy bolo medzinárodné právo podobne náhlym spôsobom konfrontované s výdobytkami doby. Išlo o kontakt s rádiovými vlnami prekračujúcimi hranice a s ľudskou schopnosťou dosiahnuť mimozemské telesá. V každom prípade však bolo považované za samozrejmosť, že aj takého správanie sa človeka podliehalo existujúcim normám medzinárodného práva.[27]

V súčasnosti sa už dlhšie diskutuje o aplikovateľnosti medzinárodného práva v kybernetickom priestore. Väčšina západných krajín sa prikláňala k aplikácii existujúceho medzinárodného práva. Niektoré krajiny ako Rusko a Čína však navrhli osobitnú sústavu noriem. Tieto mali v súlade s Chartou OSN a všeobecne uznávanými normami upravujúcimi medzinárodné vzťahy obsahovať mimo iného aj nasledovné záväzky:

- nevyužívať informačné a komunikačné technológie ani informačné a komunikačné siete na vykonávanie činností, ktoré sú v rozpore s úlohou zachovania medzinárodného mieru a bezpečnosti;
- nevyužívať informačné a komunikačné technológie ani informačné a komunikačné siete na zasahovanie do vnútorných záležitostí iných štátov alebo s cieľom narušiť ich politickú, ekonomickú a sociálnu stabilitu;
- spolupracovať v boji proti trestnej činnosti a teroristickým aktivitám v tejto oblasti;
- uznanie, že práva jednotlivca v *off-line* prostredí musia byť chránené aj v *on-line* prostredí;
- pomoc rozvojovým krajinám pri posilňovaní kapacít v oblasti informačnej bezpečnosti a preklenutí digitálnej priepasti;
- podpora všestrannej spolupráce v tejto oblasti;

---

[22] SHELDON, J., B.: Cyberwarfare: The Invisible Threat, s. 182 – 183, cit. podľa: MRÁZEK, J.: Mezinárodní právo v kybernetickém prostoru, s. 541

[23] Tamtiež, s. 541. Iní autori zase uvádzajú, že kybernetický priestor má síce tri vrstvy, avšak rozlišujú ich nasledovne: fyzickú vrstvu, ktorá sa skladá z počítačov, integrovaných obvodov, káblov, komunikácií a podobne; druhú vrstvu, ktorá sa skladá zo softvéru a tretiu vrstvu, ktorá sa skladá z dátových balíčkov a elektroniky. Bližšie pozri: TOBANKSY, L.: Basic concepts in cyber warfare, s. 75, 77-78, cit. podľa: TSAGOURIAS, N.: The legal status of cyberpsace, s. 15, dostupné na: http://www.e-elgar.com/shop/eep/preview/book/isbn/9781782547396/ (stránka navštívená dňa 19. 09. 2016)

[24] GRANT, J., P., BARKER, J. C.: Parry & Grant Encyclopaedic Dictionary of International Law, Third Edition, s. 300

[25] VRŠANSKÝ, P., VALUCH, J. a kol.: Medzinárodné právo verejné. Všeobecná časť, s. 51

[26] Tamtiež, s. 52

[27] ZIMMERMANN, A.: International Law and 'Cyber Space', dostupné na: http://www.esil-sedi.eu/node/481 (stránka navštívená dňa 19.09.2016)

- urovnať prípadné spory vyplývajúce z tohto dokumentu mierovými prostriedkami a zdržať sa hrozby silou alebo použitia sily.[28]

Doposiaľ bolo viac právnych otázok súvisiacich s činnosťou v kybernetickom priestore rozpracovaných v súvislosti s "kybernetickou vojnou", a teda z hľadiska *ius ad bellum* a *ius in bello.* Osobitnú výzvu existujúcemu medzinárodnému právu predstavujú totiž pravidlá týkajúce sa samotného kybernetického konfliktu. V súčasnosti v tejto oblasti neexistuje úplná zhoda medzi predstaviteľmi národov. Zaujímavé je, že v rámci práce Skupiny vládnych expertov v roku 2015, ktorá mala skúmať otázku aplikácie medzinárodného práva na kybernetický konflikt,[29] sa táto téma ukázala ako najnáročnejšia. Nezhody prevládajú medzi Ruskom, Čínou a niekoľkými ďalšími krajinami na jednej strane a členskými štátmi NATO na strane druhej. Jadrom sporu bolo uplatňovanie osobitných ustanovení Charty OSN[30] a to najmä použiteľnosť článku 2 ods. 4 (vzdanie sa použitia sily) a článku 51 (prirodzené právo na sebaobranu).

Jednou z otázok týkajúcich sa vývoja noriem v oblasti kybernetického konfliktu je, či je možné prekonať normy zakotvené v Charte OSN a medzinárodných dohodách, upravujúce priebeh vojny a ozbrojených konfliktov a vytvoriť normy, ktorými by sa riadil tento nový druh konfliktu. Niektorí autori ako jednu z možností, ktoré by mohli viesť k pokroku uvádzajú rozšírenie záväzkov Charty OSN vyhýbať sa akciám, ktoré ohrozujú územnú celistvosť alebo politickú nezávislosť štátu (obsiahnuté v čl. 2 ods. 4) na výslovne zahrnuté kybernetické akcie.[31]

Pokiaľ ide o vzťah kybernetického útoku k *ius ad bellum* ako aj *ius in bello*,[32] mimoriadne významnú úlohu v tejto súvislosti zohráva medzinárodná expertná skupina, ktorá bola prizvaná Centrom výnimočnosti pre oblasť spoločnej kybernetickej obrany spolupracujúcim s NATO, za účelom objasnenia uvedeného vzťahu. Výsledkom bol tzv. Tallinnský manuál,[33] vypracovaný v roku 2012. Pozostáva z dvoch častí – časť I je venovaná kybernetickej bezpečnosti a *ius ad bellum* a časť II sa zaoberá *ius in bello* alebo právom ozbrojených konfliktov.[34] Ide o výsledok činnosti nezávislých expertov, ktorý však nemá záväzný charakter.

Pohľad Spojených štátov amerických na otázky týkajúce sa aplikácie medzinárodného práva v kybernetickom priestore bol predmetom analýzy, ktorú prezentoval na medzinárodnej konferencii[35] v roku 2012 prof. H. H. Koh.[36] Ten svoju prednášku rozdelil na tri časti, pričom prvá niesla názov „Medzinárodné právo v kybernetickom priestore: čo vieme“ a obsahovala desať otázok a odpovedí. Stručne na tomto mieste priblížime jeho závery: 1) Napriek tomu, že nemusí ísť nutne o všeobecne prijímaný názor v rámci medzinárodného spoločenstva, Spojené štáty uznávajú, že ustálené zásady medzinárodného práva je možné aplikovať aj v kybernetickom priestore. 2) Kybernetický priestor nie je bezprávnou zónou kde môže ktokoľvek vykonávať nepriateľské aktivity, bez pravidiel a obmedzení.

---

28 United Nations, General Assembly, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, A/69/723, 2015.

29 Group of Governmental Experts: Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, UNODA, http://www.un.org/ga/search/view_doc.asp?symbol= A/70/174 (stránka navštívená dňa 16.09.2016)

30 Všeobecná použiteľnosť Charty bola odsúhlasená v rámci predchádzajúcej práce Skupiny – bližšie pozri v ďalšom texte.

31 LEWIS, J. A.: Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In: GEERS K. (Ed.).: Cyber War in Perspective: Russian Aggression against Ukraine, s. 42-43

32 K vzťahu kybernetických útokov a medzinárodného práva bližšie pozri: ŠMIGOVÁ, K.: Kybernetické útoky a medzinárodné právo, s. 1224-1230

33 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2012

34 GÁBRIŠ, T.: Cyber Law, s. 174, porovnaj: CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn Manual, dostupné na: https://ccdcoe.org/research.html (stránka navštívená dňa 13.09.2016)

35 18. september 2012, the USCYBERCOM Inter-Agency Legal Conference on the Roles of Cyber in National Defence, at Fort Meade, Maryland

36 Legal Adviser, U. S. Department of State, Professor of International Law (on leave), Yale Law School.

3) Kybernetické aktivity môžu za určitých okolností predstavovať použitie sily v zmysle čl. 2 ods. 4 Charty OSN a obyčajového medzinárodného práva.[37] 4) Právo štátu na sebaobranu, uvedené v čl. 51 Charty OSN, môže byť vyvolané aj aktivitami počítačovej siete, ktoré predstavujú ozbrojený útok alebo jeho bezprostrednú hrozbu. 5) V kontexte ozbrojeného konfliktu sa právo ozbrojeného konfliktu aplikuje aj na reguláciu použitia kybernetických nástrojov pri nepriateľských akciách, rovnako ako pri iných nástrojoch. Princípy nutnosti a proporcionality limitujú použitie sily v sebaobrane a upravujú aj to, čo môže za daných okolností predstavovať zákonnú reakciu. 6) Princíp rozlišovania medzi vojenskými a nevojenskými cieľmi (obsiahnutý v *ius in bello*) sa v kontexte ozbrojeného konfliktu aplikuje aj na útoky v rámci počítačových sietí. 7) Princíp proporcionality (obsiahnutý v *ius in bello*) sa vzťahuje aj na útoky v počítačovej sieti vykonávané v rámci ozbrojeného konfliktu. 8) Štáty by mali vykonať právnu analýzu svojich zbraní, vrátane tých kt. majú kybernetickú spôsobilosť. Táto by mala obsahovať zistenie, či sú prirodzene nediskriminačné, resp. či je ich použitie v súlade s princípom rozlišovania a proporcionality. 9) Štáty vykonávajúce aktivity v kybernetickom priestore musia brať do úvahy suverenitu iných štátov a to aj mimo kontextu ozbrojených konfliktov. 10) Štáty sú právne zodpovedné za činnosti osôb, ktoré konajú na základe inštrukcií štátu, pod jeho vedením alebo kontrolou. Druhá časť prednášky mala názov: „Medzinárodné právo v kybernetickom priestore: výzvy a neistoty“. V tejto časti mimo iného pripomenul, že pravidlá *ius ad bellum* sú podľa názoru Spojených štátov aplikovateľné aj na použitie sily v kybernetickom priestore. Podľa prof. Koha ani náročnosť dosiahnutia definitívneho právneho záveru alebo konsenzu medzi štátmi o tom, kedy nepriateľské kybernetické akcie predstavujú ozbrojený útok neznamená, že potrebujeme úplne nový právny rámec špecifický pre kybernetický priestor. V súvislosti s dvojitým užívaním infraštruktúry kybernetického priestoru (armádou štátu a civilným sektorom) uviedol, že vojnové právo vyžaduje, aby civilná štruktúra nebola využívaná na „imunizáciu“ vojenských objektov pred útokom (vrátane kybernetickej oblasti) a každá situácia si bude vyžadovať starostlivú právnu analýzu. Ako ďalšiu naznačil otázku pripísateľnosti správania v kybernetickom priestore, pričom zdôraznil, že vo viacerých ohľadoch ide o otázku viac technickú a politickú ako čisto právnu. V tretej časti, ktorá niesla názov: „Úloha medzinárodného práva v rozumnom silovom prístupe ku kybernetickému priestoru“ konštatoval, že medzinárodné humanitárne právo nie je jediným medzinárodným právom aplikovateľným v kybernetickom priestore. Existujú ďalšie oblasti a normy tak medzinárodného ako i národného práva, ktoré sa týkajú ľudských práv, medzinárodného obchodu, kybernetických zločinov a pod., ktoré môžu nájsť vyjadrenie aj v rámci kybernetického priestoru. Na záver konštatoval, že medzinárodné právo nepredstavuje len obmedzenia, ale umožňuje zároveň vykonávať činnosti, ktoré by boli len ťažko predstaviteľné bez toho aby boli právne legitímne. Rešpektovanie noriem medzinárodného práva preto umožňuje vláde Spojených štátov správať sa v kybernetickom priestore viac legitímne ...[38]

Vráťme sa však ku vzťahu medzinárodného práva a kybernetického priestoru v čase mieru. Dnes už možno povedať, že je všeobecne uznávaná aplikácia medzinárodného práva, čo potvrdzuje správa Skupiny vládnych expertov zriadenej Valným zhromaždením OSN z roku 2013. Táto uvádza, že medzinárodné právo a najmä Charta OSN je použiteľná a nevyhnutná k udržaniu mieru a stability a k podpore otvoreného, bezpečného, mierového a dostupného prostredia informačných a komunikačných technológií.[39] Skupina pozostávala zo zástupcov 15 krajín, vrátane Spojených

[37] Ako príklady kybernetickej aktivity, kt. by mohla predstavovať použitie sily prof. Koh uvádza: a) operácie kt. spôsobia zlyhanie jadrových zariadení; b) operácie kt. spôsobia deštrukciu priehrad nad osídlenými oblasťami; alebo c) operácie kt. narušia riadenie letovej prevádzky a spôsobia nehodu lietadla.

[38] KOH, H., H.: International Law in Cyberspace, online. - Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012, dostupné na: http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1. pdf, porovnaj: MRÁZEK, J.: Mezinárodní právo v kybernetickém prostoru, s. 555-557

[39] United Nations, General Assembly, Group of Governmental Experts (GGE): Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.

štátov amerických, Ruska a Číny. Vo svojej správe z júla 2015 odporučili súbor noriem týkajúcich sa správania štátov v kybernetickom priestore.[40]

Zároveň ale vyvstáva rovnako vážna otázka, ako aplikovať toto medzinárodné právo v danej sfére a toto nie je otázka, ktorá bude pravdepodobne záväzným spôsobom vyriešená v blízkej budúcnosti.[41]

Z uvedeného však vyplýva, že rovnako ako v predchádzajúcich prípadoch, aj aktivity v kybernetickom priestore sa riadia medzinárodným právom ako takým a v prípade, že neexistuje pravidlo zakazujúce správanie v určitej oblasti, štáty si ponechávajú slobodu konať. Zároveň však treba doplniť, že tak ako v predošlých prípadoch, je dôsledkom nedostatku v súčasnosti viac špecifických pravidiel, že len základné a všeobecné normy medzinárodného práva upravujú kybernetické aktivity vrátane konceptov ako je jurisdikcia a pripísateľnosť správania. S ohľadom na neurčitosť niektorých týchto všeobecných pravidiel, ich neprimeranosť vo vzťahu ku kybernetickým aktivitám ako aj nedostatok všeobecne akceptovaných, účinných a na pravidlách založených medzištátnych riadiacich štruktúr, predstavuje kybernetický priestor veľkú výzvu pre medzinárodné právo v jeho súčasnej podobe.[42] To však nič nemení na skutočnosti, že aj NATO dnes uznáva, že medzinárodné právo, vrátane medzinárodného humanitárneho práva a Charty OSN sa aplikuje v kybernetickom priestore.[43]

V čase mieru budú teda relevantné všeobecné pravidlá medzinárodného práva. Pozornosť venujeme najmä všeobecnému konceptu *due dilligence* (povinnosť náležitej starostlivosti), ako uvádza okrem iného aj Medzinárodný súdny dvor v prípade Korfský prieplav.[44] Uvedené pravidlo zaväzuje štáty, aby zabezpečili, že ich územie (vrátane kybernetického priestoru - súvisiacej infraštruktúry umiestnenej na ich území) nie je využívané na úkony, ktoré nezákonne poškodzujú iné štáty.[45] Práve v súvislosti s aplikáciou tohto všeobecne uznávaného konceptu na kybernetický priestor sa však vynárajú ďalšie otázky týkajúce sa obsahu príslušných povinností. Otázky teda znejú: akú úroveň opatrení je štát povinný podniknúť, s prihliadnutím na jeho úroveň technologického rozvoja? Spadá aj tranzitný štát (t. j. štát cez ktorý škodlivé dáta prechádzajú) alebo poškodený štát (t. j. štát kde sa škoda zhmotňuje) tiež pod povinnosti vyplývajúce z konceptu *due dilligence* a ak áno, do akej miery?[46] Ide o právne otázky na ktoré zatiaľ hľadá medzinárodné spoločenstvo všeobecne akceptovanú odpoveď, nakoľko v tejto oblasti (ako i v mnohých ďalších) je náročné nájsť zhodu.

---

40 STINISSEN, J.: A Legal Framework for Cyber Operations in Unkraine. In: GEERS K. (Ed.).: Cyber War in Perspective: Russian Aggression against Ukraine, s. 124

41 Tamtiež, s. 124

42 ZIMMERMANN, A.: International Law and 'Cyber Space', dostupné na: http://www.esil-sedi.eu/node/481 (stránka navštívená dňa 19.09.2016)

43 „*Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace*." Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014, para 72.

44 *Corfu Channel Case* (U.K. v. Albania), I.C.J. Reports 1949; Išlo o prípad kedy dva britské torpédoborce sprevádzajúce britské obchodné lode narazili v albánskych pobrežných vedách Korfského prieplavu na míny. Následkom bola smrť a zranenie viacerých britských námorníkov. Spojené kráľovstvo sa obrátilo so žalobou na Medzinárodný súdny dvor, pričom žiadalo náhradu škody s argumentom, že Albánsko o mínach muselo vedieť a že zanedbalo svoju povinnosť informovať o tom iné štáty. Albánsko ako protiargument uviedlo, že Spojené kráľovstvo prítomnosťou torpédoborcov narušilo suverenitu ich pobrežného mora. MSD mimo iného konštatoval, že Albánsko porušilo svoje záväzky založené na určitých všeobecne uznaných zásadách ... a záväzok každého štátu vedome nepripustiť, aby jeho územie bolo využívané na konania, ktoré sú v rozpore s právnymi záujmami iných štátov ... Bližšie pozri: BUCHTA, T., SÝKOROVÁ, M.: Najdôležitejšie rozsudky v medzinárodnom práve verejnom, s. 13-14

45 ZIMMERMANN, A.: International Law and 'Cyber Space', dostupné na: http://www.esil-sedi.eu/node/481 (stránka navštívená dňa 19.09.2016)

46 Tamtiež

4 ZÁVER

Kybernetický priestor, označovaný aj za piatu doménu na vedenie vojny, predstavuje svojim jedinečným charakterom veľkú výzvu pre súčasné medzinárodné právo. Aj z toho dôvodu je mu venovaná značná pozornosť zo strany jednotlivých štátov i rôznych multilaterálnych fór. Nielen predstavitelia štátov, ale i medzinárodných organizácií a tiež vedy tak ponúkajú zaujímavý pohľad na vzťah kybernetického priestoru a medzinárodného práva. Avšak tak ako kybernetický priestor nemá žiadne hranice, môže sa zdať akoby aj viaceré otázky s ním súvisiace boli bez konečnej odpovede. Pri bližšom pohľade na viaceré otázky sa totiž vynárajú ďalšie a ďalšie otázky a podnety na diskusiu.

Veľkú úlohu v tejto oblasti zohráva aj osobitá povaha medzinárodného práva, pre ktoré je príznačný koordinačný charakter, nakoľko ide o „právo kompromisu". A v mnohých uvedených otázkach sa kompromis rodí veľmi ťažko. Dôvodom je okrem národných záujmov jednotlivých štátov aj skutočnosť, že samotný kybernetický priestor predstavuje oblasť mimoriadne širokých možností. V súčasnosti ale už možno povedať, že aký taký kompromis existuje v otázke aplikovateľnosti všeobecného medzinárodného práva aj na tento typ priestoru.

Rovnako tak ako pri iných, relatívne nových oblastiach medzinárodného práva, ktoré boli vyvinuté v posledných desaťročiach (napr. medzinárodné právo v oblasti životného prostredia), aj v tomto prípade len čas ukáže, či medzinárodné spoločenstvo štátov bude schopné a ochotné prísť s konkrétnymi a príslušnými pravidlami medzinárodného práva vzťahujúcimi sa na kybernetický priestor. Čakajúc na takýto vývoj sa štáty a iné subjekty môžu spoliehať iba na všeobecné, a teda nutne relatívne vágne pravidlá medzinárodného práva, ako je napríklad koncept *due diligence* a pokúsiť sa aplikovať ich na základe ľudskej činnosti v kybernetickom priestore.[47] Pri bližšom nahliadnutí na špecifiká medzinárodného práva na jednej strane a technologický pokrok na strane druhej nás však optimizmus opúšťa.

Vzhľadom na rýchlosť technologického pokroku si len ťažko reálne predstaviť v súvislosti s využívaním kybernetického priestoru tradičný spôsob tvorby adekvátnych noriem medzinárodného práva v podobe multilaterálnych zmlúv, či medzinárodnej obyčaje. Tento zdĺhavý proces nemá reálnu šancu postihnúť aktuálnu problematiku a pri rýchlosti akou sa veda a technika rozvíja nám zatiaľ zostávajú len všeobecné normy medzinárodného práva aplikovateľné aj na tento typ priestoru.

V súčasnosti tiež prebiehajú práce nadväzujúce na vyššie uvedený dokument: „*Tallinn Manual on the International Law Applicable to Cyber Warfare"*. Práce na projekte Tallin Manual 2.0 by mali prebiehať od roku 2013 do roku 2016 a mali by predstavovať rozšírenú analýzu aplikovateľnosti medzinárodného práva v čase mieru. Je pokračovaním pôvodného projektu a výsledkom by malo byť druhé, rozšírené vydanie. Práve tento projekt skúma aplikovateľnosť všeobecných zásad medzinárodného práva v kybernetickom kontexte.[48]

Použitá literatúra:

BUCHTA, T., SÝKOROVÁ, M.: Najdôležitejšie rozsudky v medzinárodnom práve verejnom. Bratislava: C. H. Beck, 2016,

GÁBRIŠ, T.: Cyber Law. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2014,

GRANT, J., P., BARKER, J. C.: Parry & Grant Encyclopaedic Dictionary of International Law, Third Edition. Oxford: Oxford University Press, 2009,

KOH, H., H.: International Law in Cyberspace, In: Harvard International Law Journal Online 1 (2012), Vol. 54

JASPERS, K.: (Elexová, P. preklad): Malá škola filozofického myslenia. Bratislava: Kalligram, 2003,

KNORR, A.: The Stability of Cyberspace. In: Cyberspace 2005,

KRAMER, D. F., STARR, H. S., WENTZ, L. KUEHL,D.: Cyberpower and National Security. National Defense University: Potomac Books Inc., 2009,

LEWIS, J. A.: Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In: GEERS K. (Ed.).: Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015,

---

47 ZIMMERMANN, A.: International Law and 'Cyber Space', dostupné na: http://www.esil-sedi.eu/node/481 (stránka navštívená dňa 19.09.2016)

48 CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn 2.0, dostupné na: https://ccdcoe.org/research.html; (stránka navštívená dňa 05.10.2016)

MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti. In: Bezpečnostné fórum 2015. I. zväzok. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela - Belianum, 2015, s. 54-64
MELZER, N.: Cyber Warfare and International Law, UNIDIR Resources, 2011,
MRÁZEK, J.: Mezinárodní právo v kybernetickém prostoru. Právník 7/2014, roč. 153, s. 537 - 561
ROSCINI, M.: Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014,
SHELDON, J., B.: Cyberwarfare: The Invisible Threat. Encyclopaedia Britannica, Book of the Year 2011,
STINISSEN, J.: A Legal Framework for Cyber Operations in Unkraine. In: GEERS K. (Ed.).: Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015,
ŠMIGOVÁ, K.: Kybernetické útoky a medzinárodné právo. In: Bratislavské právnické fórum 2013. Bratislava: Univerzita Komenského, Právnická fakulta, 2013,
TOBANKSY, L.: Basic concepts in cyber warfare, In: Military and Strategic Affairs 2011, 3 (1);
VRŠANSKÝ, P., VALUCH, J. a kol.: Medzinárodné právo verejné. Všeobecná časť. Bratislava: Eurokódex, 2012,
ZIMMERMANN, A.: International Law and 'Cyber Space'. ESIL Reflections: European Society of International Law, 2014, Vol 3, Issue 1

Internetové zdroje:
CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn Manual, dostupné na: https://ccdcoe.org/research.html
CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): Tallinn 2.0, dostupné na: https://ccdcoe.org/research.html;
Center for Strategic and International Studies, Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization (UNIDIR, 2011), dostupné na: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf
KOH, H., H.: International Law in Cyberspace. In: Harvard International Law Journal, december 2012, Vol. 54, online. - Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012, dostupné na: http://www.harvardilj.org/wp-content/uploads/2012/12/ Koh-Speech-to-Publish1.pdf,
Ministerstvo vnútra Českej republiky, Odbor bezpečnostnej politiky: Kybernetické hrozby, Dostupné na: http://www. mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3d%3d
TSAGOURIAS, N.: The legal status of cyberpsace. In: Research Handbook on International Law and Cyberspace, dostupné na: http://www.e-elgar.com/shop/eep/preview/book/isbn/978178254739 6/

Dokumenty:
Australian Government: Cyber Security Strategy, 2009,
Group of Governmental Experts: Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015,
Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates, Joint Terminology for Cyberspace Operations, November 2010,
Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012
United Nations, General Assembly, Group of Governmental Experts (GGE): Report on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013.
United Nations, General Assembly, Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, A/69/723, 2015.
US: The National Military Strategy for Cyberspace Operations
Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014,

Prípad:
Corfu Channel Case (U.K. v. Albania), I.C.J. Reports 1949;

Kontaktné údaje:
JUDr. Jozef Valuch, PhD.
jozef.valuch@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

HYPERLINKY PORUŠUJÚ AUTORSKÉ PRÁVA NA INTERNETE IBA ZA URČITÝCH OKOLNOSTÍ

Martin Daňko, Petra Žárská

Právnická fakulta, Univerzita Komenského

ABSTRACT
Hyperlinks can represent a palpable problem for internet users. A hyperlink is a word, phrase, or image that can be click on to jump to a new document or allows users to click their way from page to page. In the last decade the Court of Justice of the European Union (CJEU) issued several major decision adressing rules of hyperlinking. A very recent case GS Media v Sanoma has established new standars within European copyright law such as „knowledge requirement" or „commercial requirement" in order to infringe copyright online. At the same time this decison diverted CJEU's opinion from the famous Svensson case to more favourable approach for internet consumers. This article critically evaluates hyperlink's cases decided by CJEU and the possible impact on users. The analyse focus on different approches in the chosen cases..

Hyperlinky môžu byť pálčivým problémom pre internetových užívateľov. Hyperlink je slovo, fráza alebo obraz ktorý vás po kliknutí naň presmeruje na nový dokument alebo vás presmeruje na z jednej internetovej stránky na inú internetovú stránku. V uplynulej dekáde Súdny dvor Európskej únie (ďalej len „súdny dvor" alebo „SDEU") vydal niekoľko významných rozhodnutí zaoberajúcich sa hyperlinkami. Nedávne rozhodnutie SDEU, nazývané GS Media v Sanoma, zakotvilo nové štandardné požiadavky na porušenie autorských práv na internete v európskom autorskom práve ako napríklad tzv. požiadavka vedomosti alebo požiadavka ekonomického použitia. Zároveň sa rozhodnutie odklonilo od názoru SDEU vyjadreného v známom rozhodnutí Svensson a to viac prospech internetových užívateľov. Tento článok hodnotí prípady SDEU zaoberajúce sa hyperlinkami a ich možný dopad na užívateľov. Právna analýza sa sústreďuje na odlišné prístupy k problematike vo vybraných prípadoch.

Key words: hyperlink, infringement, copyright, GS Media, Svensson, Bestwater,

1 ÚVOD

Rozhodnutie Súdneho dvora Európskej únie v právnej veci GS Media BV proti Sanoma Media Netherlands BV C-160/15 z 8. septembra 2016 (ďalej len GS Media)[1] vyvolalo vášnivú diskusiu nielen medzi internetovými užívateľmi a rozvírilo stojaté hladiny v odbornej verejnosti, nakoľko je v problematike vzťahov medzi hyperlinkov a ochrany autorských práv k dielam prostredníctvom nich šírených najvýznamnejším rozhodnutím od roku 2014, t.j. od vydania prelomového rozhodnutia v prípade Svensson (ďalej len Svensson)[2].

Cieľom tejto práce je poukázať prostredníctvom analýzy uvádzaných 3 prípadov na zmenu prístupu k šíreniu autorského obsahu po rozhodnutí GS Media, upriamiť pozornosť na praktické nezrovnalosti, ktoré uvedené rozhodnutia priniesli a poskytnúť nové pohľady nad používaním hyperlinkov bežnými konzumentmi v súlade s uvádzanými rozhodnutiami.

[1] GS Media BV proti Sanoma Media Netherlands BV C-160/15 z 8. septembra 2016 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62015CJ0160&qid=1475322738656&from=EN

[2] http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62012CJ0466&qid=1475844652774&from=EN

2 DEFINÍCIA VEREJNÉHO PRENOSU

V početných prípadoch bol Súdny dvor Európskej únie žiadaný presnejšie definovať význam pojmu „verejný prenos“ v súvislosti s článkom 3 ods. 1 Smernice 2001/29 o harmonizácii niektorých aspektov autorského práva a súvisiacich práv
v informačnej spoločnosti (ďalej len „Smernica 2001/29“)[3]. Išlo o rôzne typy prenosov (napr. prenos rádiom,), kedy národné súdy žiadali Súdny dvor určiť či daný typ prenosu napĺňa znaky „verejného prenosu“. Súdny dvor prípady cez prípady *SGAE (ďalej len „SGAE“)*[4], *FAPL (ďalej len „FAPL“)*[5], *OSA*[6], *Svensson*, *BestWater (ďalej len „Bestwater“)*[7], *Sociedade Portuguesa de Autores*[8], and *Reha Training (ďalej len „Reha Training“)*[9], identifikoval dve kumulatívne kritéria konceptu “verejný prenos”, a to “prenos” a “verejný”[10], pričom iba tri prípady sa týkajú verejného prenosu na internete formou hyperlinkov - hypertextových odkazov. Problematiku “verejného prenosu“ v prostredí internetu prostredníctvom hyperlinkov si môžeme predstaviť ako dom. Hyperlink možeme prirovnať k oknu na dome, zatiaľ čo internetová stránka ako prvá uskotučňujúca verejný prenos autorského diela môže byť priprovnaná ku slnečným lúčom vonku, mimo domu. Iba užívatelia, ktorí navštívia stránku prvého verejného prenosu, majú prístup k dielam a tí predstavujú osoby užívajúce si slnečné lúče mimo domu. Ustanovenie či použitie hyperlinku k chráneným dielam môžeme vnímať ako okno na dome. Keď je okno otvorené aby vpustilo slnečné lúče do domu (niekto klikne na hyperlink), osoby v dome si užívajú slnečné lúče v dome bez toho, aby vyšli z domu von. Podobne internetoví užívatelia cez hyperlink majú prístup k autorským dielam na inej internetovej stránke (ďalej len „stránka“) než stránke prvého verejného prenosu bez toho, aby strávili čas hľadím prvého verejného prenosu diela na stránke tohto prenosu a návštevou tejto stránky. Vďaka hyperlinkom sú pre užívateľov sprístupnené diela o ktorých nevedia, neboli by ich schopní nájsť bez správnych kľúčových slov alebo správneho indexovania vyhľadávačmi, ktoré by hľadané dielo posunulo na prvé miesto v internetovom mori informácii[11]. Dôležitosť a efektivita hyperlinkov na internete je nespochybniteľná, autori tohto článku by neboli schopní napísať svoje odborné články a záverčné práce bez ich pomoci.

2.1 Prípad Svensson

Historicky prvým a prelomovým rozhodnutím o používaní hyperlinkov – hypertextových odkazov je prípad Svensson – Nils Svensson, Sten Sjögren, Madelaine Sahlman a Pia Gadd proti Retriever Sverige AB C-466/12 z 13. februára 2014[12]. Žalobcovia – novinári a autori článkov uverenených v novinách *Göteborgs-Posten* na internetovej stránke novín podali proti spoločnosti Retriever Sveringe žalobu na náhradu škody vzniknutej sprístupnením niektorých článkov na jej internetovej stánke bez ich súhlasu. Spoločnosť Retriever Sveringe poskytuje na tejto stránke zoznamy internetových hypertextových odkazov na články uverejnené na iných internetových stránkach. Okresný súd v Štokholme žalobu zamietol, no žalobcovia sa odvolali. Následne odvolací súd vo Svea položil 4 prejudiciálne otázky Súdnemu dvoru Európskej únie.

Je nesporné, že články boli na internetovej stránke novín *Göteborgs-Posten* voľne prístupné. Podľa žalobcov zákazník po kliknutí na jeden z týchto odkazov nepostrehne, že je za účelom prístupu

---

3 Smernica EU 2001/2009 o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti

4 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62005CJ0306&qid=1475913469915&from=EN

5 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62008CJ0403&qid=1475913617540&from=EN

6 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62012CJ0351&qid=1475913718830&from=EN

7 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62013CO0348_INF&qid=1475928960123&from=EN

8 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62015CB0151&qid=1475920388026&from=EN

9 http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:62015CJ0117&qid=1475920475233&from=EN

10 http://ipkitten.blogspot.sk/2016/06/communication-to-public-is-that-effect.html

11 Viď 12

12 Viď 3

k dielu, ktoré ho zaujíma, presmerovaný na inú stránku. Žalovaný proti tomuto tvrdeniu žalobcov namietal tvrdením, že zákazníkovi je jasné, že v prípade ak klikne na niektorý z týchto odkazov, je presmerovaný na inú stránku. Žalobcovia tvrdili, že spoločnosť Retriever Sverige porušila ich výlučné právo sprístupniť svoje diela verejnosti prostredníctvom služieb poskytnutých na jej internetovej stránke, kde mali jej zákazníci prístup k ich dielam. Spoločnosť Retriever Sverige na svoju obranu tvrdila, že poskytovanie zoznamu internetových odkazov na diela, v súvislosti s ktorými došlo k verejnému prenosu na iných internetových stránkach, nepredstavuje úkon, ktorý by mohol zasiahnuť do autorského práva. Retriever Sverige rovnako tvrdila, že nevykonala nijaký prenos chráneného diela, lebo svojim zákazníkom len odporučila internetové stránky, na ktorých sa nachádzajú diela, o ktoré sa zaujímajú.

Najdôležitejšie pre právne posúdenie veci bolo zodpovedanie prvej otázky. Odvolací súd chcel vedieť či skutočnosť, že iná osoba ako nositeľ autorského práva k určitému dielu poskytne hypertextový odkaz na toto dielo na svojej internetovej stránke, predstavuje verejný prenos diela v zmysle článku 3 ods. 1 smernice 2001/29 a či takéto konanie je porušením autorského práva, konkrétne práva na verejný prenos. Ďalšia otázka skúma faktor obmedzeného a neobmedzeného prístupu k dielu, t.j. či pri posudzovaní porušenia autorských práv je podstatný fakt, že užívateľ musel prekonať zabepečovacie opatrenia ako napr. platený prístup k dielu alebo bolo dielo prístupné na stránke bez obmedzenia. Tretia otázka sa týkala miesta zobrazenia diela, teda či sa dielo po tom, čo užívateľ klikol na odkaz, zobrazí na inej internetovej stránke, alebo sa zobrazí takým spôsobom, ktorý vzbudzuje dojem, že je zobrazené na tej istej internetovej stránke. Otázka smeruje k úvahe, či nie je zobrazenie diela zavádzajúce vo vzťahu k užívateľovi, ktorý môže alebo nemusí postrehnúť presmerovanie na inú stránku. Posledná otázka mala priamo za úlohu stanoviť či rozsah pojmu „verejný prenos“ v zmysle článku 3, ods. 1 Smernice 2001/29 môže byť rozšírený právom členského štátu a či členský štát môže poskytnúť právam autora väčšiu ochranu, tým že stanoví, že pojem „verejný prenos“ zahŕňa viac úkonov, než tie, ktoré vyplývajú z článku 3 ods. 1 Smernice 2001/29.

Súdny dvor skúmal prvé tri otázky spoločne za predpokladu, že ku každému verejnému prenosu diela musí autor udeliť súhlas a sústredil sa na fakt, či v tomto prípade došlo k verenému prenosu. SDEU analyzoval právny pojem „verejný prenos“ rozdelený na 2 kumulatívne časti „prenos“ a „verejný“. Pri pojme „prenos“ uviedol, že skutočnosť, že sú na určitej internetovej stránke poskytnuté hypertextové odkazy na chránené diela, ktoré sú bez akéhokoľvek obmedzenia prístupu uverejnené na inej stránke – stránke prvého verejného prenosu, ponúka užívateľom tejto určitej stránky priamy prístup k uvedeným dielam. Z článku 3 ods. 1 Smernice 2001/29 však vyplýva, že na to, aby išlo o „prenos“, okrem iného postačuje, aby bolo dielo verejnosti sprístupnené takým spôsobom, že osoby, ktoré ju tvoria, môžu mať k tomuto dielu prístup bez ohľadu na skutočnosť, či túto možnosť využijú. Z tohto vylýva, že v tomto prípade sa poskytnutie hypertextových odkazov na chránené diela musí kvalifikovať ako „sprístupnenie“, teda ako „prenos“. Pokiaľ ide o 2. časť „verejný“ z článku 3 ods. 1 Smernice 2001/29 vyplýva, že tento pojem sa týka neurčitého počtu potenciálnych adresátov a okrem toho vyžaduje dosť významný počet osôb. Prenos, ktorý uskutočňuje prevádzkovateľ internetovej stránky prostredníctvom hyperlinkov sa pritom týka všetkých potenciálnych užívateľov stránky, ktorú táto osoba spravuje, teda neurčitého a dosť významného počtu adresátov. Súdny dvor skonštatoval, že práve za týchto podmienok žalovaný uskutočnil „verejný prenos“.

Ďalšou nemenej významnou podmienkou potrebnou k tomu, aby prenos v tomto prípade bol podľa ustálenej judikatúry „verejným prenosom“ je, aby bol určený novej verejnosti, teda verejnosti, ktorú autori pri udeľovaní súhlasu nebrali do úvahy. Podľa súdneho dvora podmienka „novej verejnosti“ v tomto prípade nebola splnená, nakoľko verejnosť, ktorej bol prvotný prenos určený, tvorili všetci potenciálni návštevníci dotknutej stránky. Podstatné je tu slovo „všetci“, lebo vzhľadom na to, že prístup k dielam na tejto stránke nepodliehal nijakému obmedzujúcemu opatreniu, mohli mať k týmto dielam teoreticky aj prakticky prístup „všetci“ užívatelia internetu. Ak všetci užívatelia inej stránky ako bola stránka novín, ktorým boli články sprostredkované prostredníctvom hyperlinku, mohli mať prístup k stránke novín, kde došlo k prvotnému prenosu a to bez zásahu prevádzkovateľa tejto inej stránky, treba užívateľov tejto inej stránky považovať za potenciálnych adresátov prvotného prenosu. Tým pádom sú všetci títo užívatelia súčasťou verejnosti branej do uváhy samotnými autormi pri udelení súhlasu s prvým prenosom. Z tejto úvahy vyplýva, že súhlas nositeľov autorského práva s verejným prenosom ako je prenos v tomto prípade, sa pri neexistencii „novej verejnosti“ nevyžaduje. Toto zistenie platí aj v prípade, ak užívatelia internetu kliknú na dotknutý odkaz, dielo sa zobrazí spôsobom vyvolávajúci dojem, že je zobrazené na stránke, na ktorej sa tento odkaz nachádza, zatiaľ

čo toto dielo v skutočnosti pochádza z inej internetovej stránky. Súdny dvor týmto konštatovaním zodpovedal 2. položenú otázku.

Súdny dvor sa ďalej „pohral" s možnosťou bezpečnostných prístupových opatrení, v prípade, že by vlastník stránky zdieľajúce diela so súhlasom autora zabezpečil prístup k nim, čím pravdepodobne zámerne poskytol držiteľom autorských práv návod ako speňažiť výsledky ich tvorivej činnosti. Súdny dvor má za to, že ak hypertextový odkaz umožňuje užívateľom stránky, na ktorej sa tento odkaz nachádza, obísť obmedzujúce opatrenia na stránke, na ktorej sa nachádza chránené dielo, použité s cieľom obmedziť prístup verejnosti k tomuto dielu len na predplatiteľov stránky (zásah, bez ktorého by uvedení užívatelia nemohli mať šírené diela k dispozícii), treba všetkých týchto užívateľov považovať za novú verejnosť. Táto nová verejnosť nebola braná do úvahy nositeľmi autorského práva pri udelení súhlasu s prvotným prenosom, takže súhlas nositeľov práv sa pri takomto verejnom prenose vyžaduje. Tak je to najmä vtedy, ak dielo už nie je verejnosti sprístupnené na stránke, na ktorej bolo pôvodne šírené, alebo ak je na tejto stránke nabudúce sprístupnené len obmedzenej skupine verejnosti, zatiaľ čo na inej internetovej stránke je prístupné bez súhlasu nositeľov autorského práva. Veľmi správne je tu spomenutá aj situácia prvotného zverejnenia chránených diel bez zamedzenia prístupu. Autori logicky prišli k záveru, že zverejniť dielo obidvoma spôsobmi si odporuje, pretože internetoví užívatelia by siahli po diele bez platenia, respektíve bez obmedzení. V súvisloti s týmto problémom Súdny dvor zohľadnil aj situáciu, keď je dielo prvotne verejne sprístupnené bez obmedzení so súhlasom autora, následne stiahnuté z internetu a potom so súhlasom autora sprístupnené s bezpečnostnými obmedzeniami. Môže sa stať, že internetoví užívatelia si dielo nezákonne stiahli a začali ho šíriť na interenete bez súhlasu autora, pričom je dielo zároveň zverejnené na inej stránke s bezpečnostými obmedzeniami. Analogicky, internetoví užívatelia v tomto prípade porušujú právo nositeľov autorských práv na verejný prenos sprístupnením diela bez ich súhlasu.

Štvrtá otázka mala významný dosah na samotnú definíciu pojmu „verejný prenos" a to z toho dôvodu, že Súdny dvor odmietol možnosť rozšírenia tohto pojmu vnútroštátnym právom. Zdôvodnil to tým, že ak by sa pripustilo, že členský štát môže poskytnúť nositeľom autorského práva väčšiu ochranu stanovením, že pojem „verejný prenos" zahŕňa aj iné úkony než tie, ktoré sú uvedené v článku 3 ods. 1 smernice 2001/29, malo by to za následok vytváranie rozdielov v právnych predpisoch, a teda právnu neistotu pre tretie osoby. Autori súhlasia s týmto záverom a zdôrazňujú, že legislatívna úprava pojmu „verejný prenos" musí byť riešená celoplošne tým istým spôsobom, najma v prostredí internetu, ktorý presahuje hranice štátov.

Napriek tomu, že prípad Svensson veľmi jasne definoval, že hyperllink k chránenému dielu zverejnenému na inej stránke so súhlasom autora nie je porušením autorských práv, čo sa stane ak by tento link viedol k autorskému dielu zverenenému bez autorského súhlasu na inej stránke? Samotné zverejnenie autorského obsahu bez súhlasu autora na internetovej stánke je porušením autorských práv podľa európskeho a slovenského práva, avšak čo hyperlink, ktorý nás iba navedie k samotnému obsahu na inej stránke? Môže tento akt subsumovať pod pojem „verejný prenos" alebo nenapĺňa jeho znaky?

2.2 Prípad Bestwater

V prípade Svensson Súdny dvor prvý krát analyzoval verejný prenos autorského diela umiestneného na internete so súhlasu autora. Avšak internet je miesto plné neoprávneného obsahu (obsahu umiestneného na stránkach bez súhlasu autora), a preto sa čakalo na prípad, v ktorom by Súdny dvor riešil situáciu hyperlinku vedúceho k neoprávnenému obsahu. A práve takáto situácia bola riešená Súdnym dvorom vo veci Bestwater. Hoci v tomto prípade súd len zopakoval závery o verejnom prenose vyplývajúce z prípadu Svensson, rozhodnutie SDEU malo dôsledky pre vkladanie hypertextových odkazov alebo aj tz. „postovanie" odkazov na legálne a ilegálne sprístupnené diela na stránkach tretích osob.

V predchádzajúcom spore figurovali dve strany. Prvou stranou bol autor, ktorý sprístupnil diela s jeho súhlasom - legálne na zvolenej stránke a druhou stranou bola osoba, ktorá skopírovala hypertextový odkaz a zverejnila ho na svojej stránke. V prípade Bestwater do hry vstupuje tretia strana – osoba, na ktorej internetovej stánke/profile je hyperlink umiestnený, pričom toto umiestnenie je vykonané stranou č. 2. V praxi táto situácia nastáva, keď skopírujete hyperlink obsahujúci napríklad pieseň z youtube.com a vložíte ho na stránku svojho priateľa alebo známeho.

Presne tento postup prebehol v prípade Bestwater v Nemecku s tým rozdielom, že z prípadu nebolo jasné, či bol autorský obsah zdieľaný bez súhlasu autora. Zaujímavosťou tohto rozhodnutie je že, SDEU sa túto skutočnosť vôbec nezaoberal a iba skonštatoval, že samotnú skutočnosť, že chránené dielo, ktoré je voľne dostupné na internetovej stránke, je vložené na inú internetovú stránku prostredníctvom odkazu používajúceho techniku „framing", ako je tá použitá v spore vo veci samej, nemožno považovať za „verejný prenos" v zmysle článku 3 ods. 1 Smernice 2001/29, ak predmetné dielo nie je šírené novej verejnosti a ani nedochádza k jeho prenosu za použitia špecifickej technológie, ktorá sa odlišuje od pôvodného prenosu.[13]

V prípade Bestwater došlo k zdieľaniu hyperlinku k 2-minutovému filmu nahraného na plaforme youtube.com, pričom popis okolností je vágny a nie je možné určiť či bol obsah zverejnený so súhlasom autora alebo bez jeho súhlasu. Dôležitejší je však fakt, že Súdny dvor to nepovažoval za kľúčové pri rozhodovaní a ponechal otázku vkladania (zdieľania) autorského obsahu na stránkach tretích osôb nezodpovedanú. O porušenie autorských práv, konkrétne práva na verejný prenos, by išlo v prípade hyperlinku s chráneným obsahom, ak by verejný prenos zahrňoval novú verejnosť. Napríklad ak by osoba vkladajúca hyperlink narušila technické opatrenia určené na ochranu prístupu k dielu. V praxi by išlo o prípad, kedy by užívateľ obišiel paypal účet alebo login a heslo na stránku s chráneným autorským obsahom. Z vyššie uvedeného je možné vyvodiť záver, že samotná zákonnosť zverejneného obsahu – prvého verejného prenosu na internetovej stránke so súhlasom autora, pri hyperlinkoch a ich vkladaní nemá váhu na určení či ide o verejný prenos. Možeme predpokladať, že za týchto podmienok je rozhodujúci fakt, že hyperlink nebol sprístupnený novej verejnosti. Okrem iného je možné z tohto rozhodnutia vyvodiť, že autori sú zodpovední za sledovanie a zdieľanie svojho autorského obsahu na internete a osoby, ktoré vkladajú a zdieľaju hyperlinky, nemajú povinnosť sa ubezpečiť, či je zdieľaný autorský obsah umiestený na internet so súhlasom autora.[14]

2.3 Prípad GS Media[15]

Spoločnosť Sanoma vlastniaca časopis Playboy v Holandsku zaplatila za vyhotovenie fotografií pani Dekkerovej z úmyslom ich v tomto časopise zverejniť. Predmetné fotografie sa objavili na internete pred ich zverejnením v časopise bez súhlasu spoločnosti, ktorá mala výhradný súhlas na uverejnenie fotografií udelený autorom. Dňa 26. októbra 2011 redakcia internetovej stránky GeenStijl dostala správu od osoby vystupujúcej pod pseudonymom, ktorá obsahovala hypertextový odkaz na elektronický súbor uložený na internetovej stránke Filefactory.com (ďalej len „internetová stránka Filefactory") nachádzajúcej sa v Austrálii a určenej na ukladanie dát. Tento elektronický súbor obsahoval predmetné fotografie. Sanoma ešte v ten deň vyzvala spoločnosť GS Media prevádzkujúcu internetovú stránku GeenStijl, aby zabránila zverejneniu predmetných fotografií na tejto internetovej stránke. Dňa 27. októbra 2011 bol v súvislosti s týmito fotografiami o pani Dekkerovej uverejnený článok na internetovej stránke GeenStijl, s názvom „…!… fotografie nahej Dekkerovej", na okraji ktorej sa nachádzala časť jednej z predmetných fotografií a ktorá sa končila týmto textom: „A teraz stránka s fotografiami, na ktorú čakáte". Na základe jedného kliknutia na hypertextový odkaz, ktorý bol súčasťou tohto textu, boli používatelia internetu presmerovaní na internetovú stránku Filefactory, na ktorej im ďalší hypertextový odkaz umožňoval stiahnuť si jedenásť elektronických súborov, z ktorých každý obsahoval jednu z uvedených fotografií. V ten istý deň Sanoma zaslala spoločnosti GS Media e-mail, ktorým ju vyzvala, aby potvrdila, že hypertextový odkaz na predmetné fotografie bol z internetovej stránky GeenStijl odstránený. GS Media na túto výzvu nereagovala. Na žiadosť Sanoma však boli predmetné fotografie, ktoré sa nachádzali na internetovej stránke Filefactory, odstránené. Listom zo 7. novembra 2011 Sanoma vyzvala GS Media, aby z internetovej stránky GeenStijl odstránila článok z 27. októbra 2011, vrátane hypertextového odkazu a fotografií, ktoré obsahoval, ako aj reakcie používateľov internetu zverejnené na tej istej internetovej stránke. V ten istý deň bol na internetovej stránke uverejnený článok týkajúci sa sporu medzi GS Media a Sanoma a i. v súvislosti s predmetnými fotografiami. Tento článok sa končil vetou: „Aktualizácia: ešte ste nevideli fotografie nahej [Dekkerovej]? TU ich nájdete". Tento oznam opäť dopĺňal hypertextový odkaz umožňujúci prístup na internetovú stránku Imageshack.us, na ktorej sa objavila jedna alebo viacero

[13] Viď 8

[14] http://ipkitten.blogspot.sk/2014/10/that-bestwater-order-its-up-to.html

[15] http://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1477833496043&uri=CELEX:62015CJ0160

z predmetných fotografií. Správca tejto internetovej stránky však tiež vyhovel žiadosti Sanoma na odstránenie týchto fotografií. Tretí článok, s názvom „Bye Bye, adieu Playboy“, ktorý opäť obsahoval hypertextový odkaz na predmetné fotografie, sa 17. novembra 2011 objavil na internetovej stránke GeenStijl. Používatelia internetu, ktorí navštívili fórum tejto internetovej stránky, tam vložili nové odkazy na iné internetové stránky, na ktorých bolo možné vidieť predmetné fotografie. V decembri 2011 boli predmetné fotografie uverejnené v časopise *Playboy*.

Sanoma podala žalobu na Rechtbank Amsterdam (Súd Amsterdam, Holandsko) tvrdiac, že GS Media tým, že vložila hypertextové odkazy a sčasti zverejnila jednu z predmetných fotografií na internetovej stránke GeenStijl, porušila autorské práva pána Hermèsa a konala nezákonne vo vzťahu k Sanoma a i. Rechtbank Amsterdam tejto žalobe v prevažnej časti vyhovel. Gerechtshof Amsterdam (Odvolací súd Amsterdam, Holandsko) zrušil toto rozhodnutie, pričom konštatoval, že GS Media vložením hypertextových odkazov neporušila autorské práva pána Hermèsa (autor fotografií), lebo fotografie už boli uverejnené ich vložením na internetovú stránku Filefactory. Tento súd však zároveň rozhodol, že GS Media tým, že vložila tieto odkazy na internetovú stránku Geenstijl, konala nezákonne vo vzťahu k Sanoma a i., lebo návštevníci tejto internetovej stránky boli takto nabádaní k oboznámeniu sa s predmetnými fotografiami, ktoré boli nezákonne vložené na stránku Filefactory. Ak by tieto odkazy neexistovali, bolo by ťažké tieto fotografie nájsť. Gerechtshof Amsterdam okrem toho skonštatoval, že GS Media čiastočným zobrazením jednej z fotografií na stránke GeenStijl porušila autorské práva pána Hermèsa.

Obidve strany podali kasačný opravný prostriedok na Najvyšší súd Holandska, v rámci ktorého Sanoma najmä odkazuje na rozsudok z 13. februára 2014, v právnej veci Svensson a i. , s tvrdením, že skutočnosť, že bol používateľom internetu sprístupnený hypertextový odkaz na internetovú stránku, na ktorú bolo vložené dielo bez súhlasu nositeľa autorských práv k tomuto dielu, predstavuje verejný prenos. Sanoma a i. navyše tvrdila, že sprístupnenie predmetných fotografií na internetovej stránke Filefactory bolo chránené obmedzujúcimi opatreniami v zmysle uvedeného rozsudku, ktoré mohli používatelia internetu obísť pomocou zásahu GS Media a jej internetovej stránky GeenStijl, takže tieto fotografie boli sprístupnené širšej skupine verejnosti, než je skupina, ktorej bol umožnený prístup k uvedeným fotografiám na internetovej stránke Filefactory. Najvyšší súd Holandska v rámci preskúmania vzájomného kasačného prostriedku konštatoval, že nie je možné s dostatočnou istotou vyvodiť ani z rozsudku z 13. februára 2014, vo veci Svensson, ani z uznesenia z 21. októbra 2014, vo veci BestWater, či ide o „verejný prenos“, ak bolo dielo skutočne vopred zverejnené, ale bez súhlasu nositeľa autorských práv. Najvyšší súd dospel k správnemu záveru, pretože ako autori tohto článku skonštatovali vyššie, tento problém SDEU nezodpovedal ani v jednom z predchádzajúcich prípadov. Na jednej strane z uvedenej judikatúry Súdneho dvora vyplýva, že treba preskúmať, či sa predmetný zásah môže vzťahovať na verejnosť, ktorú nemožno považovať za súčasť skupiny verejnosti, ktorej dal autor súhlas, čo je v súlade s jeho výlučným právom na využívanie jeho diela. Na druhej strane, keď je už dielo sprístupnené širokej verejnosti na internete, vloženie hypertextového odkazu, ktorý presmeruje na internetovú stránku, kde sa toto dielo už nachádza, v skutočnosti nezasahuje novú verejnosť. Okrem toho treba zohľadniť skutočnosť, že internet sa prepĺňa dielami, na zverejnenie ktorých nedal nositeľ autorských práv súhlas. Pre správcu internetu, ktorý chce vložiť na internetovú stránku hypertextový odkaz na internetovú stránku, na ktorej sa dielo nachádza, nie je vždy ľahké zistiť, či autor dal svoj súhlas na predchádzajúce zobrazenie.

Holandský súd ďalej priniesol otázku obmedzujúcich opatrení v zmysle rozhodnutí vo veci Svensson a Bestwater, pričom uviedol, že predmetné fotografie nebolo možné na internete nájsť predtým, ako GS Media vložila hypertextový odkaz na internetovú stránku GeenStijl. Skutočnosťou, že GS Media na svoju internetovú stránku vložila hypertextový odkaz, v širokej miere uľahčila prístup k týmto fotografiám. Za týchto podmienok Najvyšší súd Holandska položil 6 prejudiciálnych otázok.

V prvých 3 otázkach sa vnútroštátny súd spýtal, či a prípadne za akých okolností ide o „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29 v prípade, keď sa na internetovú stránku vloží hypertextový odkaz na chránené diela, ktoré sú voľne dostupné na inej internetovej stránke bez súhlasu nositeľa autorských práv. V tomto kontexte si je podstatná otázka, v akom

rozsahu je relevantná skutočnosť, že dotknuté diela ešte neboli zverejnené iným spôsobom so súhlasom tohto nositeľa, a že poskytnutie hypertextových odkazov na základe kliknutia v širokej miere uľahčuje objavenie autorových diel vzhľadom na to, že internetovú stránku, kde sú tieto diela sprístupnené všetkým používateľom internetu, nemožno ľahko nájsť, a že subjekt, ktorý vkladá uvedené odkazy, vedel alebo mal vedieť o týchto skutočnostiach, ako aj o tom, že uvedený nositeľ autorských práv nedal súhlas na zverejnenie dotknutých diel na danej internetovej stránke.

Súdny dvor zdôraznil, že vďaka tomu, že článok 3 ods. 1 Smernice 2001/29 nespresňuje pojem „verejný prenos“, je potrebné vymedziť jeho význam a rozsah z hľadiska cieľov sledovaných touto smernicou a kontextu, do ktorého vykladané ustanovenie spadá – rozhodnutí SGAE, FAPL a ďalších. Súdny dvor sa ďalej odvoláva na rozhodnutia vo veci Svensson a Reha Training, kde bol pojem “verejný prenos” upresnený. V nadväznosti na správne posúdenie predmetnej veci zdôrazňuje potrebu individuálneho posúdenia, posúdenia z hľadiska existencie viacerých kritérií, ktoré nie sú samostatné a sú navzájom závislé a v závislosti od prípadu sú posudzované jednotlivo alebo vo vzájomnej súvislosti. Súdny dvor medzi týmito kritériami po prvý krát zdôraznil nepopierateľnú úlohu používateľa a vedomú povahu jeho konania. Druhým kritériom je použitie špecifickej technológie na prenos a tretím je dosiahnutie zisku. Používateľ totiž uskutočňuje prenos, ak s vedomím dôsledkov svojho konania sprostredkúva svojim zákazníkom prístup k chránenému dielu, a to najmä vtedy, ak by bez tohto zásahu títo zákazníci nemohli mať v zásade prístup k zverejnenému dielu. Súdny dvor ďalej spresnil, že pojem „verejný“ sa týka neurčitého počtu potenciálnych adresátov a okrem toho zahŕňa pomerne vysoký počet osôb.

Okrem toho z ustálenej judikatúry Súdneho dvora vyplýva, že na to, aby bolo možné prenos kvalifikovať ako „verejný prenos“, prenos chráneného diela sa musí uskutočniť podľa špecifickej technológie, odlišnej od technológií, ktoré sa doteraz používali, alebo v prípade, že taká technológia neexistuje, musí byť dielo sprístupnené „novej verejnosti“, t. j. verejnosti, ktorú nositelia autorských práv pri udelení súhlasu na prvotný verejný prenos svojho diela ešte nebrali do úvahy. Súdny dvor ďalej rozhodol, že odplatná povaha verejného prenosu v zmysle článku 3 ods. 1 Smernice 2001/29 nie je irelevantná. Pri posudzovaní, či ide o verejný prenos Súdny dvor uviedol, v predchádzajúcich prípadoch sa vyjadril len k vloženiu týchto hypertextových odkazov na diela, ktoré boli voľne dostupné na inej internetovej stránke so súhlasom nositeľa práv, pričom dospel k záveru, že nejde o verejný prenos, lebo daný prenos sa neuskutočnil s cieľom zasiahnuť novú verejnosť. V kontexte tohto prípadu Súdny dvor uviedol, že vzhľadom na skutočnosť, že hypertextový odkaz a internetová stránke, na ktorú odkazuje, umožňujú prístup k chránenému dielu na základe tej istej technológie, a to internetu, musí byť takýto odkaz adresovaný novej verejnosti. Ak nejde o tento prípad, predovšetkým preto, že dielo už bolo voľne dostupné všetkým používateľom internetu na inej internetovej stránke s povolením nositeľov autorských práv, predmetné konanie nemožno klasifikovať ako „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29. Totiž vzhľadom na skutočnosť, že ak je toto dielo voľné dostupné na internetovej stránke, na ktorú hypertextový odkaz umožňuje prístup, treba konštatovať, že ak nositelia autorských práv k tomuto dielu dali súhlas na takýto prenos, všetkých používateľov brali do úvahy ako verejnosť. Z predchádazjúcich prípadov ako Svensson, Bestwater nie je možné vyvodiť, že vloženie hypertextových odkazov na internetovú stránku odkazujúcich na chránené diela, ktoré boli voľne sprístupnené na inej internetovej stránke, ale bez súhlasu nositeľov autorských práv k dielam, by v zásade bolo možné vylúčiť z pojmu „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29. GS Media, nemecká, portugalská a slovenská vláda, ako aj Európska komisia tvrdili, že ak by sa každé vloženie týchto odkazov na zverejnené diela na iných internetových stránkach malo automaticky kvalifikovať ako „verejný prenos“ a súčasne by existovala skutočnosť, že nositelia autorských práv týchto diel neudelili súhlas s týmto zverejnením na internete, malo by to vážne obmedzujúce dôsledky na slobodu prejavu a právo na informácie šírené prostredníctvom internetu a bolo by to v rozpore s primeranou rovnováhou, ktorú sa Smernica 2001/29 snaží zachovať medzi týmito slobodami a všeobecným záujmom na jednej strane a záujmom nositeľov autorských práv na účinnú ochranu ich duševného vlastníctva na druhej strane. V tejto súvislosti treba konštatovať, že internet má skutočne dôležitý vplyv na slobodu prejavu a právo na informácie a že hypertextové odkazy prispievajú k jeho riadnemu fungovaniu, ako aj k výmene názorov a informácií v rámci tejto siete, ktorá je charakteristická širokou dostupnosťou k množstvu

informácií. Navyše sa môže zdať zložitým, najmä pre jednotlivcov, ktorí chcú vložiť takéto odkazy, overiť si, či internetová stránka, na ktorú ich majú tieto odkazy presmerovať, umožňujú prístup k chráneným dielam, a prípadne, či nositelia autorských práv k týmto dielam dali súhlas s ich zverejnením na internete. Takéto overovanie sa zdá byť ešte zložitejšie, ak sú tieto práva predmetom licencie. Okrem toho obsah internetovej stránky, na ktorú hypertextový odkaz umožňuje prístup, môže byť po vytvorení tohto odkazu zmenený, vrátane chránených diel, bez toho, aby osoba, ktorá tento odkaz vytvorila, o tom nevyhnutne vedela.

Na účely individuálneho posúdenia toho, či ide o „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29, sa musí v prípade, že hypertextový odkaz na dielo, ktoré je voľné dostupné na inej internetovej stránke, vložila osoba bez toho, aby tým chcela dosiahnuť zisk, zohľadniť skutočnosť, že táto osoba nevie, a ani dôvodne nemôže vedieť, že toto dielo bolo zverejnené na internete bez súhlasu nositeľa autorských práv. Takáto osoba totiž tým, že sprístupni uvedené dielo verejnosti tak, že ďalším používateľom internetu umožní priamy prístup k tomuto dielu, vo všeobecnosti neposkytuje svojim zákazníkom prístup k nezákonne zverejnenému dielu na internete s plným vedomým dôsledkov svojho konania. Navyše, ak bolo dotknuté dielo už dostupné bez akéhokoľvek obmedzenia prístupu na internetovej stránke, na ktorú hypertextový odkaz umožňuje prístup, všetci používatelia internetu v zásade už mohli mať prístup k tomto dielu aj bez tohto zásahu. To neplatí v dvoch prípadoch. Ak sa však preukáže, že osoba vedela, alebo mala vedieť, že hypertextový odkaz, ktorý vložila, dáva prístup k nezákonne zverejnenému dielu na internete, napríklad preto, lebo bola na to upozornená nositeľmi autorských práv, treba konštatovať, že poskytnutie tohto odkazu predstavuje „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29. Je to tak aj za predpokladu, že tento odkaz umožňuje používateľom internetovej stránky, na ktorej sa nachádza, obísť obmedzujúce opatrenia, ktoré používa stránka obsahujúca chránené dielo, aby obmedzila prístup verejnosti len pre prihlásené osoby. Potom vloženie takého odkazu predstavuje vedomý zásah, bez ktorého by uvedení používatelia nemohli mať prístup k zverejneným dielam.

Okrem toho, ak je hypertextový odkaz vložený na účely dosiahnutia zisku, možno od autora tohto vloženia očakávať, že si overí, či dotknuté dielo nie je nezákonne zverejnené na stránke, ku ktorej vedú uvedené hypertextové odkazy. Potom sa možno domnievať, že toto vloženie bolo urobené s plným vedomím o chránenej povahe uvedeného diela a prípadnej neexistencii súhlasu nositeľa autorských práv so zverejnením na internete. Za týchto okolností a za predpokladu, že by táto vyvrátiteľná domnienka nebola vyvrátená, konanie spočívajúce vo vložení hypertextového odkazu, ktorým sa dá preklikať na nezákonne zverejnené dielo na internete, predstavuje „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29.

Pokiaľ ide o prípad vo veci samej, je nepopierateľné, že GS Media prevádzkovala internetovú stránku GeenStijl a že poskytla hypertextové odkazy na súbory obsahujúce predmetné fotografie, uložené na internetovej stránke Filefactory, s cieľom dosiahnutia zisku. Je tiež nepopierateľné, že Sanoma nedala súhlas na zverejnenie týchto fotografií na internete. Navyše z opisu skutkových okolností, ako vyplýva z rozhodnutia vnútroštátneho súdu o návrhu na začatie prejudiciálneho konania, zrejme vyplýva, že GS Media vedela o tejto poslednej uvedenej skutočnosti a nemôže teda vyvrátiť domnienku, že vloženie týchto odkazov bolo urobené s plným vedomím o nezákonnosti tohto zverejnenia. Za týchto podmienok je zrejmé, s výhradou, že vnútroštátny súd náležite overí tieto skutočnosti, že GS Media vložením týchto odkazov uskutočnila „verejný prenos“ v zmysle článku 3 ods. 1 Smernice 2001/29, pričom nie je potrebné v tomto kontexte posudzovať ďalšie skutočnosti, ako je napríklad že dotknuté diela ešte neboli zverejnené iným spôsobom so súhlasom tohto nositeľa.

Vzhľadom na predchádzajúce úvahy bolo potrebné na otázky položené Súdnemu dvoru odpovedať nasledovne: článok 3 ods. 1 Smernice 2001/29 sa má vykladať tak, že na účely preukázania toho, či skutočnosť, že na internetovú stránku boli vložené hypertextové odkazy na chránené diela, ktoré sú voľne dostupné na inej internetovej stránke, bez súhlasu nositeľa autorských práv k týmto dielam, predstavuje „verejný prenos“ v zmysle tohto ustanovenia, treba zistiť, či tieto odkazy poskytla osoba bez úmyslu dosiahnutia zisku, pričom nevedela alebo dôvodne nemohla vedieť o nezákonnej povahe zverejnenia týchto diel na tejto inej internetovej stránke, alebo naopak,

či uvedené odkazy boli poskytnuté s cieľom dosiahnutia zisku, kde sa v tomto prípade musí vychádzať z domnienky tejto vedomosti.[16] Na lepšiu orientáciu v problematike autori pripájajú prehľadne usporiadaný právny stav vo forme tabuľky a ďakujú za sprehľadnenie kolegovi Martinovi Husovcovi.

Tabuľka 1: Právny stav po GS Media[17]

Prístup k obsahu	Obsah publikovaný so súhlasom autora/držiteľa práv	Zámer produkovať zisk	Vedomosť o tom, či je obsah publikovaný zákonne	Verejný prenos	Potencionálne porušenie autorských práv
Voľne dostupný	Áno	neaplikované	neaplikované	Nie (Svensson, GS Media)	Nie
Nie je voľne dostupný	Áno	neaplikované	neaplikované	Áno (Bestwater, GS Media)	Áno
Voľne dostupný	Nie	Nie	Nie	Nie (GS Media)	Nie
Voľne dostupný	Nie	Nie	Áno (napríklad upozornenie)	Áno (GS Media)	Áno*
Voľne dostupný	Nie	Áno	Prepokladaná (vyvrátiteľná domnienka)	Áno (GS Media)	Áno
Nie je voľne dostupný	Nie	neaplikované	neaplikované	Áno	Áno

* Ak autor/držiteľ práv upozorní osobu, ktorá poskytuje hyperlink (bez prechádzajúcej vedomosti o nezákonnosti obsahu), že obsah ku ktorému vedie hyperlink, je nezákonne publikovaný a táto osoba odmietne vymazať hyperlink, potom výminka v čl. 5 ods. 3 Smernice 2001/2009 (výnimky a obmedzenia práva na rozmnoženie diela) nie je aplikovateľná.

3 ZÁVER

Z rozhodnutia SDEU v prípade GS Media vyplýva, že ak užívateľ zdieľa hyperlink, ktorý odkazuje na diela zverejnené na inej stránke bez súhlasu autora, nejde o verejný prenos ak ide o zdieľanie bez dosiahnutia zisku a užívateľ nevedel, či je obsah zverejnený na tejto stránke bez súhlasu autora alebo o tom dôvodne nemohol vedieť. Ak by užívateľ zdieľal tento hyperlink za účelom dosiahnutia zisku, prepokladáme, že mal vedomosť o zverejnení obsahu bez súhlasu autora. V prípade GS Media boli obidve podmienky kumulatívne splnené, pretože stránka zdieľala hyperlinky za účelom dosiahnutia zisku a bola viac krát upozornená na fakt, že fotografie ku ktorým viedol hyperlink, boli zverejnené bez súhlasu autora.[18] Predmetná konštrukcia pripomína svojim črtami zákonné licencie, v tom zmysle, že zdielanie autorského obsahu je právne tolerované v prípadoch nesledujúcich dosiahnutie zisku, zatiaľ čo pri generovaní zisku zákon označuje rovnaké použite za porušenie autorských práv. Autori majú za to, že tu dochádza k preberaniu tzv. testu komerčného použitia z iných odvetví práv duševného vlastníctva, napríkla z práva ochranných známok.

[16] Viď 16
[17] Martin Husovec, viď na http://ipkitten.blogspot.sk/2016/09/linking-after-gs-media-in-table.html
[18] http://ipkitten.blogspot.sk/2016/09/hyperlinks-and-communication-to-public.html

Z vyššie uvedeného je zrejmé že, rozhodnutie GS Media je v prospech užívateľov. Poskytuje im možnosť vyvrátit domienku vedomosti a generovania zisku. V praxi si zatiaľ autori nevedia predstaviť tento proces vyvrátenia domnienok. Pri domienke generovania zisku by mohlo postačovať, že užívateľ žiadnym spôsobom nenadobudol zisk po umiestnení hyperlinku na svoju alebo inú stánku. Preukazovanie subjektívnej vedomostnej podmienky je komplikovanejšie, autori predpokladajú, že dôkazom by mohol byť výpis použitých stránok s prehliadača užívateľa zo všetkých zariadení, ktoré používa ako tablet, telefon a počítač. Aj tento predpoklad má svoje limity, pretože užívateľ mohol nadobudnúť vedomosť aj cez prístup v knižnici či cez akýkoľvek verejný internetový prístup.

Pri domnienke „nemohol dôvodne vedieť" vyvstáva otázka významu slova „dôvodne". Môže byť dôvodom, že preukázateľne nemal prístup k internetovému pripojeniu lebo bol 3 mesiace na púšti? Alebo ležal rok v kóme? Akoľvek sa zdajú predmetné príklady extrémne až absurdné, v dnešnej dobe internetizácie a mobiného prístupu takmer v každom kúte planéty, si je veľmi ťažké predstaviť solídne zdôvodnenie nevedomosti. Autori aplikujú myšlienkovú konštrukciu SDEU, kedy Súdny dvor prepokladá, že keď je dielo zverejnené na stránke so súhlasom autora, verejnosťou sú všetci užívatelia internetu, teda sa predpokladá vedomosť všetkých užívateľov o exitencii diela, čo vyvracia predpokladanú nevedomosť. Je tomu tak z dôvodu voľného prístupu k internetu pre každého. Uvedené skutočnosti dostávajú autorov diel, ktoré sú neoprávnené zverejnené a následne používané na internete v rozsahu pravidiel vytvorených v prípade GS Media do role „všedarcov" v záujme zabezpečenia práva na informácie šírených na internete pre všetkých jeho užívateľov, čo nemožno považovať z pohľadu ochrany autorských práv na internete za správne.

Použitá literatúra:

HANUŠ, L.: Právní argumentace nebo svévole. Úvahy o právu, spravedlnosti a etice. Praha: C.H.Beck, 2008. 221 s.
CHRIS, R.: Computer Law, Oxford: Oxford University Press, 2011. 656 s.
MURRAY, A.: Information technology law. The law and society, New York: Oxford University Press, 2013. 640 s.
ROWLAND D., KOHL U., CHARLESWORT, A.: Information technology law, Abingdon: Routledge, 2012. 592 s.

Kontaktné údaje

Mgr. Martin Daňko, PhD.
martin.danko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

Mgr. Petra Žárská, LLM .
petra.zarska@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

Information About the Publication in English

Internet as a space of possible rights infringement

Conference Proceeding Collection

EVENT: International Academic Conference **Bratislava legal forum 2016**

DATE: 21st – 22nd of October 2016

LOCATION: Bratislava, Slovak republic

ORGANIZER: Faculty of Law, Comenius University in Bratislava, Slovak republic

SUMMARY:

This publication represents the research papers presented on the International Academic Conference Bratislava legal forum 2016 which will was held on 21st and 22nd October 2016 under the auspices of Andrej Danko, the Chairman of the National Council of the Slovak Republic. The major topic of the plenary session was "Alternatives for the Direction of the EU – Integration or Disintegration". The conference was held on the occasion of the 95th anniversary of delivering the very first lecture at the Faculty of Law by Professor Augustín Ráth who was the first dean of the Faculty of Law at CU in Bratislava and the first Slovak rector of Comenius University in Bratislava. The primary objective of the conference is to interconnect legal science with practice, present up-to-date issues and challenges faced by EU law and thus provide an excellent opportunity for holding discussions. In accordance with this objective, the conference is divided into plenary session and thematically oriented parallel sessions organized within sections which focus on current issues and challenges of modern Slovak, European and international law.

Each Paper includes the summary and key words in English.

Each Paper was peer reviewed by the autonomous reviewer.

CONTENT


BRATISLAVA LEGAL FORUM
BRATISLAVSKÉ PRÁVNICKÉ FÓRUM
2016