Challenges of Law in Cyberspace

Výzvy práva v kyberpriestore

Guarantees of the Session / Garanti sekcie:
doc. JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA.
Mgr. Martin Daňko, PhD.

Reviewers of Papers / Recenzenti:
doc. JUDr. PhDr. Tomáš Gábriš, PhD., LLM, MA.
Mgr. Martin Daňko, PhD.

CONTENT / OBSAH

SLOVENSKÁ REPUBLIKA NA PRAHU KYBERNETICKEJ BEZPEČNOSTI

Jozef Andraško

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The author deals with legal regulation of cybersecurity de lege lata in the Slovak Republic, with regard to the international regulation of this issue regulated in documents adopted by the European Union and North Atlantic Treaty Organization. Within this international regulation is exerted the pressure on the Slovak Republic, in order to solve the issue of protection of cyberspace through a binding regulation that is currently absent in the Slovak legal order.

Abstrakt: Autor sa v príspevku zaoberá právnou úpravou kybernetickej bezpečnosti de lege lata v Slovenskej republike, s ohľadom na medzinárodnú reguláciu tejto problematiky upravenej v dokumentoch prijatých Európskou úniou a Organizáciou Severoatlantickej zmluvy. V rámci tejto medzinárodnej regulácie je vyvíjaný tlak, aby Slovenská republika riešila problematiku ochrany kybernetického priestoru formou záväznej právnej regulácie, ktorá v súčasnosti v slovenskom právnom poriadku absentuje.

Key words: cybersecurity, protection, cyberspace, information and communication technologies

Kľúčové slová: kybernetická bezpečnosť, ochrana, kybernetický priestor, informačné a komunikačné technológie

1 ÚVOD

Enormné zavádzanie informačných a komunikačných technológií (ďalej len „IKT“) do väčšiny oblastí života prináša mnohé pozitíva, ktoré vedú k rozvoju informačnej spoločnosti, urýchleniu komunikácie a rozvoju služieb. Na druhej strane, závislosť spoločnosti a jej fungovania na takýchto technológiách so sebou prináša aj riziká v podobe zneužitia IKT a útokov na uvedené technológie. Cielené útoky proti IKT nie sú len otázkou, ktorú je potrebné riešiť na národnej úrovni, ale nadobudla globálny charakter a stala sa celospoločenským fenoménom. Výsledkom takýchto aktivít sú škody nie len vo verejnom sektore, ale aj súkromnom sektore. Nové formy kybernetických útokov predstavujú ohrozenie pre dôležité riadiace, technologické, komunikačné a bezpečnostné systémy, ako aj služby, ktorých nefunkčnosť, alebo chybná funkčnosť, by mala vážny dopad na fungovanie štátu, najmä v jeho základných bezpečnostných oblastiach. V dôsledku dynamicky sa rozvíjajúcich technológií sa zvyšuje riziko vzniku ďalších nových bezpečnostných hrozieb. Preto je viac ako potrebné, zaoberať sa problematikou zabezpečenia potrebnej ochrany IKT pred zásahmi, ktoré môžu ochromiť ich riadne fungovanie a v konečnom dôsledku ohroziť aj riadne fungovanie štátu.

Slovenskej republike ako členovi Organizácie Severoatlantickej zmluvy (ďalej len „NATO“) a členovi Európskej únie vznikajú záväzky týkajúce sa kybernetickej bezpečnosti, konkrétne ochrana kybernetického priestoru, ochrana pred útokmi a hrozbami, ktoré sa objavujú v tomto priestore. Spomínané útoky sú stále komplikovanejšie a sofistikovanejšie, nehovoriac o tom, že často smerujú proti prvkom kritickej infraštruktúry. S ohľadom na skutočnosť, že kybernetický priestor nie je teritoriálne ohraničený, je potrebné pozerať sa na problematiku kybernetickej bezpečnosti perspektívou medzinárodného spoločenstva a v dôsledku všade prítomných kybernetických hrozieb, rozvíjať intenzívnu medzinárodnú spoluprácu. Nakoľko v Slovenskej republike pretrváva rôzna úroveň spôsobilosti a pripravenosti na kybernetické hrozby a útoky proti IKT, je nutné riešiť ochranu kybernetického priestoru formou záväznej právnej regulácie.

2 ZÁKLADNÉ POJMY KYBERNETICKEJ BEZPEČNOSTI

Kybernetická bezpečnosť je v súčasnosti považovaná za jednu z najdynamickejších otázok, avšak málokto si uvedomuje jej skutočný význam a rozmer. Jedným z hlavných dôvodov pre túto nejasnosť je absencia záväznej terminológie v tejto oblasti. Preto je viac ako potrebné, vymedziť pojem kybernetická bezpečnosť a pojmy s ňou súvisiace.[1]

Napriek tomu, že pojem **kybernetická bezpečnosť** sa v súčasnosti nevyskytuje v žiadnej právnej norme, nachádzame definíciu tohto pojmu v dokumente „Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020" (ďalej len „Koncepcia"). V zmysle Koncepcie predstavuje kybernetická bezpečnosť určujúci prvok bezpečnostného prostredia a na úrovni štátu predstavuje: „*systém nepretržitého a plánovitého zvyšovania politického, právneho, hospodárskeho, bezpečnostného, obranného a vzdelanostného povedomia, ktorý zahŕňa aj zvyšovanie účinnosti prijatých a aplikovaných technicko-organizačných opatrení riadenia rizík v kybernetickom priestore za účelom jeho transformácie do dôveryhodného prostredia, ktoré umožnia bezpečné fungovanie spoločenských a hospodárskych procesov pri zaistení akceptovateľnej úrovne rizík v kybernetickom priestore.*"[2] V zmysle prílohy Koncepcie, ktorá vymedzuje vybrané pojmy, ako aj význam kľúčových pojmov pre účely Koncepcie, je kybernetická bezpečnosť vymedzená ako: „*súhrn právnych, organizačných a technických prostriedkov na zaistenie ochrany kybernetického priestoru.*"[3] Koncepcia vníma kybernetickú bezpečnosť ako súčasť bezpečnostného systému štátu a poukazuje na základné bezpečnostné oblasti (bezpečnostné záujmy Slovenskej republiky v zahraničnej a obrannej politike; ochrana ústavného zriadenia, verejného poriadku, bezpečnosť občana a štátu; sociálna stabilita štátu; ekonomická stabilita štátu; ochrana životného prostredia), ktoré by mohli byť ohrozené v prípade nezabezpečenia dostatočnej ochrany a obrany pred bezpečnostnými incidentmi.

Ďalšími dôležitými pojmami sú **kybernetický priestor** *(cyberspace)* a **národný kybernetický priestor**.[4] Pojem kybernetický priestor pôvodne slúžil na označenie prostredia, v ktorom prebieha prenos a spracovanie digitálne zaznamenanej informácie. V súčasnosti označuje informačnú a komunikačnú infraštruktúru organizácie, štátu, alebo globálnu informačnú a komunikačnú infraštruktúru.[5] Podobne ako pojem kybernetická bezpečnosť, ani kybernetický priestor nemá svoju legálnu definíciu, ale možno poznamenať, že je obsahom viacerých dokumentov, ktoré nie sú záväzné.[6] Kybernetický priestor je v zmysle prílohy Koncepcie vymedzený ako: „*virtuálny priestor bez hraníc zložený z celosvetovo prepojených sietí z hardvéru, softvéru a dát.*"[7] Národný kybernetický priestor Slovenskej republiky zahŕňa jednotlivé systémy kybernetického priestoru, ktoré sa nachádzajú na území Slovenskej republiky, ako aj ďalšie systémy kybernetického

[1] Zdrojom pre objasnenie týchto pojmov sú najmä akademické publikácie a rôzne dokumenty nezáväzného charakteru, nakoľko v súčasnosti neexistuje právna úprava, ktorá by sa danou problematikou komplexne zaoberala a zároveň legálne vymedzovala pojmy týkajúce sa kybernetickej bezpečnosti.

[2] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. s.4.

[3] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. Príloha č. 1. s. 2.

[4] Pojem *cyberspace* bol prvýkrát použitý v poviedke Williama Forda Gibsona „Burning Chrome" (1982) a následne v jeho sci-fi románe „Neuromancer 1984". Postupne sa tento pojem stal veľmi populárny.

[5] OLEJÁR, D.: Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. s. 150. [online]. Dostupné na internete:
http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s

[6] Ide o dokumenty ako: Národná stratégia pre informačnú bezpečnosť Slovenskej republiky, Akčný plán informačnej bezpečnosti, Legislatívny zámer zákona o informačnej bezpečnosti, Návrh zákona o informačnej bezpečnosti alebo Koncepcia kybernetickej bezpečnosti v Slovenskej republike na roky 2015 - 2020.

[7] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. Príloha č. 1. s. 2.

priestoru, ktoré obsahujú dáta a informácie smerované na Slovenskú republiku, alebo majúce vplyv na Slovenskú republiku.[8]

S problematikou kybernetickej bezpečnosti úzko súvisí aj pojem **kritická infraštruktúra a kritická informačná a komunikačná infraštruktúra**. Prvý pojem predstavuje v zmysle Koncepcie: „*systémy a služby, ktorých nefunkčnosť, alebo chybná funkčnosť by mala závažný dopad na bezpečnosť štátu, jeho ekonomiku, verejnú správu a v konečnom dôsledku na zabezpečenie základných životných potrieb obyvateľstva.*“[9] V rámci kritickej infraštruktúry je často definovaných päť sektorov: sektor informačných a komunikačných technológií, energetický sektor, bankový a finančný sektor, fyzická distribúcia – dopravná infraštruktúra (čiže hlavne prepravné a dopravné systémy) a sektor významných služieb pre ľudí.[10] Podľa Koncepcie predstavuje kritická informačná a komunikačná infraštruktúra: „*sústavu systémov, infraštruktúr, sietí a služieb informačných a komunikačných technológií, ktorých narušenie, zničenie alebo nedostupnosť by mali vážny dosah na fungovanie ďalších sektorov kritickej infraštruktúry a životne dôležitých spoločenských funkcií, vrátane národnej, ekonomickej a verejnej bezpečnosti.*“[11] Inými slovami možno povedať, že kritická informačná a komunikačná infraštruktúra, ktorá je súčasťou národnej informačnej a komunikačnej infraštruktúry (NIKI), ktorá slúži na získavanie, prenos, spracovávanie a uchovávanie informácií, pozostáva jednak z hmotných prvkov, ktorými sú počítače, ďalšie IKT zariadenia, počítačové a komunikačné siete, ktoré jednotlivé komponenty vzájomne prepájajú, ale aj z nehmotných prvkov, predstavujúcich informácie, ktoré prúdia v tejto infraštruktúre, ale aj služby, ktoré sú prostredníctvom nej poskytované.

Cieľom kybernetických útokov, ktoré môžu ohroziť kritickú infraštruktúru sú najmä **informačné a komunikačné technológie**. V širšom slova zmysle predstavujú IKT akýkoľvek nástroj, zariadenie alebo prostriedok, ktorý sa dá používať na spracovávanie informácie. V súčasnosti však IKT slúžia na spracovanie informácií spojením počítačov, telekomunikačných systémov a masovokomunikačných prostriedkov.[12] IKT zaradzujeme do kritickej infraštruktúry spoločnosti, nakoľko sa využívajú aj na spracovanie dôležitých informácií, riadenie zložitých systémov a vykonávanie činností, od ktorých závisí riadny chod spoločnosti.

3 KYBERNETICKÁ BEZPEČNOSŤ SLOVENSKEJ REPUBLIKY

Problematika kybernetickej bezpečnosti nie je v súčasnosti komplexne upravená v právnom poriadku Slovenskej republiky. Čiastočne sa tejto problematike venujú dokumenty „Národná stratégia pre informačnú bezpečnosť“ a nadväzujúci „Akčný plán informačnej bezpečnosti“.[13] Na tomto mieste treba podotknúť, že v prípade pojmov informačná bezpečnosť a kybernetická bezpečnosť sa v odborných kruhoch vedie mnoho diskusií tykajúcich sa ich vzájomného vzťahu.[14]

---

[8] Tamtiež, s. 2.

[9] Tamtiež, s. 2.

[10] Pojem kritická infraštruktúra je definovaný v § 2 písm. a), b) a c) zákona č. 45/2011 Z.z. o kritickej infraštruktúre. Kritická infraštruktúra Slovenskej republiky je podobná ako kritická infraštruktúra iných štátov (doprava, energetika, chemický priemysel, vojenský priemysel, výroba a transport nebezpečných látok, informačné technológie a telekomunikácie, finančné inštitúcie a poisťovne, zásobovanie pitnou vodou, potravinami, zdravotné a záchranné služby, odstraňovanie odpadu, štátna administratíva, verejná správa, súdy, polícia, armáda, colná správa, médiá, výskumné a vzdelávacie inštitúcie, národné kultúrne pamiatky). Každá zo súčastí kritickej infraštruktúry spadá do pôsobnosti niektorého z ústredných orgánov štátnej správy, resp. orgánov územnej samosprávy.

[11] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. Príloha č. 1. s. 2.

[12] OLEJÁR, D.: Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. s. 147. [online]. Dostupné na internete:
http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s

[13] Problematike informačnej bezpečnosti sa venuje aj „Legislatívny zámer zákona o informačnej bezpečnosti“ schválený uznesením vlády SR č. 136/2010. Návrh zákona o informačnej bezpečnosti je stále v legislatívnom procese.

[14] Napriek nejednotnosti názoru na problematiku vzťahu medzi pojmami informačná bezpečnosť a kybernetická bezpečnosť je potrebné podotknúť, že v oboch prípadoch ide o zaistenie bezpečnosti kybernetického priestoru. Zatiaľ čo predmetom informačnej bezpečnosti je ochrana záujmov

Kybernetickej bezpečnosti sa ďalej venuje dokument „Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany, vyplývajúcich z cieľov spôsobilostí Slovenskej republiky“. Tento dokument vymedzuje národné spôsobilosti Slovenskej republiky v oblasti kybernetickej obrany, ktoré bude nevyhnutné vybudovať a rozvíjať do konca roka 2017. V zmysle tohto dokumentu Národný bezpečnostný úrad bude plniť úlohy, ktoré súvisia so zabezpečením a koordinovaním vybudovania spôsobilostí Slovenskej republiky v oblasti kybernetickej obrany.[15]

V súčasnosti absentuje právna úprava kybernetickej bezpečnosti, ktorá by komplexne riešila problematiku ochrany kybernetického priestoru. Čiastkové aspekty ochrany Slovenskej republiky pred kybernetickými útokmi sú predmetom nasledujúcich právnych predpisov:

- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre,
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.[16]

S cieľom zabezpečenia primeranej úrovne ochrany národnej informačnej a komunikačnej infraštruktúry (NIKI) a kritickej informačnej a komunikačnej infraštruktúry bol Ministerstvom financií SR zriadený Národný útvar pre riešenie počítačových incidentov (CSIRT.SK, *Computer Security Incident Response Team Slovakia*), ktorý je etablovaný aj v rámci príslušných medzinárodných štruktúr. CSIRT.SK vznikol v súlade s Národnou stratégiou pre informačnú bezpečnosť v Slovenskej republike a je zriadený ako špecializovaný útvar DataCentra, ktorý je rozpočtovou organizáciou Ministerstva financií Slovenskej republiky. Hlavnou úlohou CSIRT.SK je najmä iniciovať a koordinovať reakcie štátnej správy, verejného a súkromného sektora na bezpečnostné incidenty, ktoré ohrozujú nie len národnú informačnú a komunikačnú infraštruktúru Slovenskej republiky (NIKI).

Hlavnými cieľmi CSIRT.SK sú:[17]

- riešenie informačno-bezpečnostných incidentov v Slovenskej republike v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí národnej informačnej a komunikačnej infraštruktúry (NIKI), telekomunikačnými operátormi, poskytovateľmi internetových služieb a so štátnymi orgánmi,
- budovanie a rozširovanie znalostí verejnosti vo vybraných oblastiach informačnej a kybernetickej bezpečnosti,
- kooperácia so zahraničnými sesterskými organizáciami a reprezentácia Slovenskej republiky v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

Na účely dosiahnutia týchto cieľov poskytuje CSIRT.SK služby aktívne, ktoré zahŕňajú najmä analýzu, varovanie, reakciu a koordináciu činností pre prípad vzniku bezpečnostného

---

organizácie v kybernetickom priestore, v prípade kybernetickej bezpečnosti ide o zabezpečenie záujmov štátu v tomto priestore.

[15] Ďalšími strategickými, resp. koncepčnými dokumentmi, ktorých obsah sa čiastočne venuje problematike ochrany kybernetického priestoru resp. kybernetickej bezpečnosti sú:

- Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, schválená uznesením vlády SR č. 120/2007.
- Národná politika pre elektronické komunikácie na roky 2009 - 2013, schválená uznesením vlády SR č. 360/2009.
- Správy o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR, materiály vláda SR vzala každoročne na vedomie od roku 2010 do roku 2014.
- Biela kniha o obrane Slovenskej republiky, schválená uznesením vlády SR č. 326/2013.
- Správa o bezpečnosti Slovenskej republiky za rok 2012, schválená uznesením vlády SR č. 325/2013.
- Operačný program Integrovaná infraštruktúra 2014 - 2020, schválený uznesením vlády SR č. 171/2014.
- Správa o bezpečnosti Slovenskej republiky za rok 2013, schválená uznesením vlády SR č. 276/2014.

[16] Neformálnym gestorom nad oblasťou informačnej bezpečnosti neutajovaných informácií, sa v zmysle zákona č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy, stalo Ministerstvo financií Slovenskej republiky.

[17] [online]. Dostupné na internete: http://www.informatizacia.sk/csirtsk/7648s

incidentu, ale aj proaktívne, ako napríklad vzdelávanie, distribúciu informácií o incidentoch a konzultačnú podporu v oblasti kybernetickej bezpečnosti

3.1 Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020

Problematika kybernetickej bezpečnosti je na národnej úrovni predmetom **Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020**.[18] K vypracovaniu tohto dokumentu sa vláda Slovenskej republiky zaviazala do konca roka 2014 v Správe o bezpečnosti Slovenskej republiky za rok 2013. Koncepcia vychádza z uvedenia a opisu základných pojmov, základných princípov, charakteristiky aktuálneho stavu strategického, legislatívneho a inštitucionálneho rámca v oblasti kybernetickej bezpečnosti v Slovenskej republike, ako aj zo strategického a metodického rámca formovaného dokumentmi NATO a Európskej únie a z nich následne formuluje princípy, ciele a návrhy riešení.

Predmetný dokument poukazuje na značné nedostatky v oblasti kybernetickej bezpečnosti, a to najmä v absentujúcej právnej úprave, ktorá by regulovala ochranu národného kybernetického priestoru. Práve chýbajúcu legislatívu v tejto oblasti považuje Koncepcia za najzávažnejší problém a na viacerých miestach poukazuje na nutnosť prijatia komplexnej právnej úpravy v tejto oblasti. Ďalej predmetný dokument poukazuje na nedostatočnú inštitucionálnu základňu v oblasti kybernetickej bezpečnosti, nedostatočne rozvinutú spoluprácu medzi verejným sektorom a súkromným sektorom, akademickou sférou a občianskou spoločnosťou.

Strategickým cieľom kybernetickej bezpečnosti Slovenskej republiky je: „*otvorený, bezpečný a chránený národný kybernetický priestor, t.j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku.*“[19]

Koncepcia sa zaoberá taktiež otázkou inštitucionálneho rámca kybernetickej bezpečnosti. V zmysle Koncepcie by mala na národnej úrovni patriť problematika kybernetickej bezpečnosti do pôsobnosti príslušného ústredného orgánu štátnej správy, ktorého kompetencie a pôsobnosť všeobecne vymedzí kompetenčný zákon a konkrétne stanoví osobitný právny predpis (zákon o kybernetickej bezpečnosti). Koncepcia odporúča aby túto pôsobnosť zákonodarca zveril **Národnému bezpečnostnému úradu.**

V rámci otázky inštitucionálneho rámca sa navrhuje zriadiť:[20]

- **Ústredný orgán štátnej správy pre kybernetickú bezpečnosť** - rozšírená pôsobnosť existujúceho odvetvovo nezávislého ústredného orgánu štátnej správy o ďalší úsek štátnej správy.
- **Národná jednotka pre riešenie incidentov (národný CERT/CSIRT)** - osobitné pracovisko s vecnou pôsobnosťou v oblasti kybernetickej bezpečnosti na národnej úrovni v riadiacej pôsobnosti Ústredného štátneho orgánu pre kybernetickú bezpečnosť[21] (plní tiež úlohy „tímu reakcie na núdzové počítačové situácie“ v zmysle článku 7 návrhu smernice[22]).
- **Vecne príslušná autorita pre kybernetickú bezpečnosť** - organizačný útvar existujúcich ústredných štátnych orgánov. V rámci svojej vecnej pôsobnosti zaisťuje kybernetickú bezpečnosť.

---

[18] Schválená vládou Slovenskej republiky dňa 17.06.2015. [online]. Dostupné na internete: http://www.rokovanie.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702

[19] ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. s.9.

[20] Koncepcia v rámci riešenia inštitucionálneho rámca v porovnaní s prvou verziou návrhu Koncepcie, ktorá bola v odborných kruhoch podrobená vlne kritiky, už nespomína Výbor Bezpečnostnej rady pre Slovenskú republiku pre kybernetickú bezpečnosť. Predmetný výbor by mal byť zriadený ako stály pracovný orgán Bezpečnostnej rady Slovenskej republiky pre vnútornú koordináciu opatrení kybernetickej bezpečnosti. Bližšie pozri: Návrh zákona, ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z.

[21] V texte Koncepcie sa na viacerých miestach používa pojem „Ústredný štátny orgán“. Z legislatívneho hľadiska, ako aj z hľadiska pojmov, ktoré používa správne právo, by bolo vhodnejšie používať pojem „Ústredný orgán štátnej správy“. Bližšie pozri: VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012, s. 127.

[22] Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Európskej únii.

- Jednotka pre riešenie incidentov (vládny CERT/CSIRT, CERT/CSIRT XY) - osobitné pracovisko ústredného štátneho orgánu - vecne príslušnej autority pre kybernetickú bezpečnosť.[23]
- Formálna platforma pre spoluprácu na národnej úrovni - umožní účasť reprezentantov podnikateľskej a akademickej sféry na príprave a vytváraní vládnych rozhodnutí formou predkladania odporúčaní, alebo názorov na rozvoj a nepretržité zlepšovanie systému zabezpečenia kybernetickej bezpečnosti v Slovenskej republike.[24]

V závere Koncepcia sumarizuje hlavné dôvody prijatia takéhoto koncepčného materiálu pre oblasť kybernetickej bezpečnosti. Týmito dôvodmi sú najmä ochrana národného kybernetického priestoru, plnenie záväzkov Slovenskej republiky ako členskej krajiny Európskej únie a NATO a iných medzinárodných záväzkov, skúsenosti z ostatných členských krajín, optimalizácia spolupráce medzi orgánmi verejnej moci navzájom, ako aj medzi verejnou mocou a súkromnou a akademickou sférou, ako aj odstránenie duplicít.

Na základe prijatých návrhov Koncepcie sa odporúča vypracovať a na rokovanie Bezpečnostnej rady Slovenskej republiky a vlády Slovenskej republiky predložiť: „**Návrh zákona o kybernetickej bezpečnosti“,** ktorý ucelene pokryje oblasť kybernetickej bezpečnosti a **„Návrh Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020“,** ktorý určí vecný, časový a finančný plán realizácie Koncepcie. Okrem vyššie spomenutých dokumentov sa z dôvodu zadefinovania, ustálenia a používania jednotnej terminológie súvisiacej s kybernetickou bezpečnosťou odporúča prerokovať v Medzirezortnej terminologickej komisii Bezpečnostnej rady Slovenskej republiky a následne zverejniť v Terminologickom slovníku krízového riadenia terminológiu, použitú v Koncepcii. Koncepcia taktiež odporúča v primeranom rozsahu formálne stanoviť požiadavky na fyzickú, objektovú, personálnu a administratívnu bezpečnosť, ako aj podmienky bezpečnosti technických a systémových prostriedkov a šifrovej ochrany informácií. Posledné odporúčanie predstavuje vytvorenie formálnej platformy pre systematickú spoluprácu verejnej správy, akademickej obce, vedeckých kruhov a súkromnej sféry na zaistení kybernetickej bezpečnosti v Slovenskej republike.

4 KYBERNETICKÁ BEZPEČNOSŤ V PONÍMANÍ EURÓPSKEJ ÚNIE A NATO

Nakoľko kybernetický priestor nepozná teritoriálne obmedzenie a je de facto bez hraníc, je nutné otázku kybernetickej bezpečnosti riešiť z pohľadu medzinárodného spoločenstva a s ohľadom na záväzky, ktoré vznikajú Slovenskej republike z členstva v NATO a v Európskej únii. Tieto vonkajšie vplyvy vytvárajú tlak na Slovenskú republiku, majúc za cieľ riešenie problematiky ochrany kybernetického priestoru prostredníctvom záväznej právnej regulácie.[25]

Problematika kybernetickej bezpečnosti nie je komplexne riešená medzinárodným právom ani právom Európskej únie. Existuje mnoho medzinárodných dokumentov, ktoré upravujú partikulárne aspekty kybernetickej bezpečnosti (problematika služieb elektronickej komunikácie,

[23] Nepredpokladá sa fyzické zriadenie odvetvových jednotiek v každom odvetví správy. Je však potrebné zabezpečiť realizáciu týchto funkcionalít v rámci jednotlivých odvetví správy. Vládny CERT/CSIRT je jednotka pre riešenie incidentov v pôsobnosti Ministerstva financií SR pre informačné systémy verejnej správy a pre vybrané informačné systémy kritickej infraštruktúry.

[24] Túto platformu má predstavovať Komisia pre kybernetickú bezpečnosť ako stály odborný poradný orgán riaditeľa Národného bezpečnostného úradu pre uplatňovanie štátnej politiky v oblasti kybernetickej bezpečnosti v Slovenskej republike. Vláda Slovenskej republiky vzala na vedomie Návrh Štatútu Komisie pre kybernetickú bezpečnosť. [online]. Dostupné na internete: http://www.rokovanie.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25017

[25] V rámci medzinárodnej spolupráce má Slovenská republika svojich zástupcov v mnohých medzinárodných organizáciách, ako aj v orgánoch Európskej únie a NATO. Aktívne v nich presadzuje svoje záujmy v tejto oblasti. Pravidelne sa zúčastňuje na kybernetických cvičeniach (Cyber Coalition, Locked Shields, Cyber Europe, a iné), ktoré každoročne preverujú schopnosti a reakcie Slovenskej republiky na kybernetické útoky. Úzko spolupracuje najmä s Centrom excelentnosti pre oblasť spoločnej kybernetickej obrany v estónskom Tallinne (NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE), Európskou agentúrou pre sieťovú a informačnú bezpečnosť (European Union Agensy for Network and Information Security Agency, ENISA) a s nedávno vzniknutým Centrom pre boj proti počítačovej kriminalite (European Cybercrime Centre; EC3).

oblasť kritickej infraštruktúry a oblasť ochrany o súkromia v rámci elektronickej komunikácie), avšak komplexný právne záväzný dokument absentuje. [26]

Na účely zaistenia kybernetického priestoru bola na úrovni **Európskej únie** vypracovaná „Stratégia kybernetickej bezpečnosti Európskej únie" (ďalej len „Stratégia EÚ").[27] Tento dokument bol dňa 7.2.2013 predložený Vysokou predstaviteľkou Európskej únie pre zahraničné veci a bezpečnostnú politiku. Podľa Stratégie EÚ možno pod kybernetickou bezpečnosťou rozumieť nasledovné:

„Kybernetická bezpečnosť obyčajne odkazuje na ochranné opatrenia a plány, ktoré môžu byť použité k ochrane kybernetickej domény, a to ako v civilnej, tak aj vo vojenskej oblasti, pred hrozbami, ktoré sú s nimi spojené alebo ktoré by mohli poškodiť jej vzájomne prepojené siete a informačnú infraštruktúru. Kybernetická bezpečnosť usiluje o zachovanie dostupnosti a integrity sietí a infraštruktúry a dôvernosť informácií v nich obsiahnutých."[28]

Cieľom konkrétnych opatrení Stratégie EÚ je zvyšovanie odolnosti informačných systémov voči kybernetickým útokom, znižovanie počítačovej kriminality, ako aj posilňovanie politiky Európskej únie v oblasti medzinárodnej kybernetickej bezpečnosti a kybernetickej obrany. V nadväznosti na uvedený dokument bol schválený „Politický rámec pre kybernetickú obranu" na zasadnutí ministrov obrany v novembri 2014.

Výsledkom zámeru Európskej komisie legislatívne upraviť oblasť kybernetickej bezpečnosti je „**Návrh smernice Európskeho parlamentu a Rady o opatreniach k zaisteniu vysokej spoločnej úrovne bezpečnostných sietí a informácií v Európskej únii"** (ďalej len „Návrh smernice"), ktorá je kľúčovou súčasťou celkovej stratégie kybernetickej bezpečnosti. Návrh smernice okrem vzájomnej spolupráce požaduje, aby každý členský štát prijal národnú stratégiu pre bezpečnosť sietí a informácií, ustanovil vnútroštátny orgán, ktorý by bol zodpovedný za bezpečnosť sietí a informačných systémov a zriadil skupinu pre reakciu na počítačové hrozby, tzv. CERT *(Computer emergency response team)*. Návrh smernice taktiež počíta s ukladaním povinností regulačným subjektom, ktorými budú orgány verejnej správy a tzv. hospodárske subjekty[29] definované v smernici a predpokladá, že orgány verejnej správy a hospodárske subjekty budú povinné oznamovať zodpovednému subjektu incidenty, ktoré budú mať významný dopad na bezpečnosť základných služieb, ktoré poskytujú.[30]

Problematika kybernetickej bezpečnosti je obsahom viacerých dokumentov prijatých **Organizáciou Severoatlantickej zmluvy**. „Strategická koncepcia NATO" *(Strategic Concept for the Defence and Security of the Members of the NATO*), ktorá bola prijatá na summite NATO v Lisabone v roku 2010, uznala kybernetický priestor za kľúčovú súčasť kolektívnej obrany a za novú operačnú doménu. Kybernetické útoky sa vyskytujú čoraz častejšie a môžu dosiahnuť až úroveň, ktorá ohrozí národnú a euroatlantickú prosperitu, bezpečnosť a stabilitu. Zdrojom takýchto útokov môžu byť zahraničné vojenské a spravodajské služby, organizovaní aj individuálni zločinci, teroristické resp. extrémistické skupiny.

---

[26] Úlohy týkajúce sa zabezpečenia potrebnej vysokej úrovne bezpečnosti sietí a prenášaných údajov zabezpečuje Európska agentúra pre bezpečnosť sietí a informácií (ENISA). Bola založená v roku 2004 Nariadením č. 460/2004/ES o zriadení Európskej agentúry pre bezpečnosť sietí a informácií v znení nariadenia č. 1007/2008a sídli v meste Hérakleion na ostrove Kréta. Nariadením č. 460/2004/ES o zriadení Európskej agentúry pre bezpečnosť sietí a informácií v znení nariadenia č. 1007/2008

[27] EURÓPSKA KOMISIA: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: 2013, s. 3. [online].
Dostupné na internete: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[28] Tamtiež s. 3.

[29] Medzi hospodárske subjekty sa pre účely Návrhu smernice rozumejú poskytovatelia služieb informačnej spoločnosti od ktorých závisí poskytovanie ďalších služieb informačnej spoločnosti (ich demonštratívny výpočet je v prílohe Návrhu smernice). alebo prevádzkovateľov kritickej infraštruktúry, ktorá má zásadný význam pre zachovanie životne dôležitých ekonomických a spoločenských činností v oblasti energetiky, dopravy, bankovníctva, obchodovania s cennými papiermi a zdravotníctva (ich demonštratívny výpočet je v prílohe Návrhu smernice).

[30] MAISNER, M., VLACHOVÁ, B.: Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a.s., 2015. s. 55.

Osobitne pre oblasť kybernetickej obrany NATO bola v roku 2011 prijatá „Stratégia kybernetickej obrany NATO“ (*NATO Policy on Cyber Defence*), ktorá vymedzuje úlohy, ciele a aktivity v oblasti kybernetickej obrany, ktoré musí v spolupráci s členskými krajinami vybudovať, zabezpečiť a v budúcnosti rozvíjať. K tejto stratégii bol prijatý „Akčný plán kybernetickej obrany NATO“ (*NATO Cyber Defence Action Plan*). Konkretizuje úlohy a prostriedky na dosiahnutie cieľov kybernetickej obrany.

Stratégia kybernetickej obrany NATO bola v máji 2014 aktualizovaná dokumentom „Posilnená stratégia kybernetickej obrany NATO“ (*Enhanced NATO Policy on Cyber Defence*). Na summite vo Walese v septembri 2014 bol schválený aktualizovaný „Akčný plán kybernetickej obrany NATO“, ktorý stanovuje konkrétne úlohy na naplnenie vyššie uvedenej politiky. Jednou z kľúčových úloh je zosilnenie vzájomnej spolupráce medzi štátnym sektorom, súkromným sektorom a akademickou obcou.

V súvislosti s medzinárodnoprávnou úpravou kybernetického priestoru a vzťahov vznikajúcich v prípade kybernetickej vojny je potrebné spomenúť „Tallinnský manuál medzinárodného práva aplikovateľného na kybernetickú vojnu“ *(Tallinn Manual on the International Law Applicable to Cyber Warfare).* Tento manuál má charakter právne nezáväznej akademickej štúdie, ktorá sa týka aplikácie medzinárodného práva, najmä *ius ad bellum* a medzinárodného humanitárneho práva v kybernetických konfliktoch a v kybernetickej vojne v rámci práva ozbrojených konfliktov. Uvedený dokument bol vydaný v roku 2012 na základe požiadavky Centra výnimočnosti pre oblasť spoločnej kybernetickej obrany v Tallinne, medzinárodnou skupinou expertov.[31] Tallinnský manuál sa skladá z dvoch častí. Časť A sa zaoberá kybernetickou bezpečnosťou a *ius ad bellum*. Časť B sa zaoberá *ius in bello* a právom ozbrojených konfliktov.[32]

Slovenská republika ako člen NATO, a tým pádom súčasť systému kolektívnej obrany a bezpečnosti NATO, musí byť pripravená primerane reagovať aj na kybernetické hrozby, ktoré sa jej priamo netýkajú, ak to vyplýva z medzinárodných zmlúv a dohôd, ktorými je viazaná. Vzhľadom na to, že v súčasných medzinárodných konfliktoch využívajú kybernetické útoky, sa čoraz častejšie spomína aplikácia čl. 5 Severoatlantickej zmluvy, ak by bol kybernetický útok svojou intenzitou, škodami a nepriateľským úmyslom porovnateľný s ozbrojeným útokom vedeným konvenčnými zbraňami.

Jedným z cieľov Koncepcie je zabezpečiť základné princípy kybernetickej bezpečnosti, ktoré odporúča Stratégia kybernetickej bezpečnosti Európskej únie a Stratégia kybernetickej obrany NATO, ako aj spolupracovať s členskými štátmi Európskej únie a NATO, príslušnými orgánmi týchto organizácií a s partnerskými štátmi. Táto spolupráca má docieliť nepretržité monitorovanie, analýzu a vyhodnocovanie bezpečnostnej situácie v kybernetickom priestore, ako aj včasné zisťovanie hrozby vzniku krízovej situácie a koordinovať prijatie preventívnych opatrení na odstránenie spomínanej hrozby. Na základe vyššie uvedených dokumentov je nutné konštatovať, že problematiku ochrany kybernetického priestoru je potrebné riešiť nie len na národnej úrovni, ale najmä na medzinárodnej úrovni.

5 ZÁVER

Otázka kybernetickej bezpečnosti v súčasnosti predstavuje jeden z najvážnejších problémov, ktorému musia čeliť nie len jednotlivé štáty, organizácie, ale aj jednotlivci tvoriaci informačnú spoločnosť, ktorá sa stala závislá od IKT. Táto závislosť so sebou okrem pozitív prináša mnoho hrozieb v podobe kybernetických útokov, ktoré sú čím ďalej sofistikovanejšie a komplikovanejšie. Preto je nevyhnutné, aby štáty na národnej úrovni prijímali záväznú právnu reguláciu týkajúcu sa ochrany národného kybernetického priestoru, ktorá by zabezpečila primeranú úroveň kritickej informačnej a komunikačnej infraštruktúry a základných bezpečnostných oblastí fungovania štátu.

[31] Centrum výnimočnosti pre oblasť spoločnej kybernetickej obrany – NATO CCD CoE predstavuje akreditovanú medzinárodnú vojenskú organizáciu s cieľom posilnenia spolupráce kybernetických obranných schopností členských krajín NATO a zlepšenia interoperability Aliancie v oblasti kooperatívnej kybernetickej obrany. Nie je súčasťou veliteľskej štruktúry NATO, avšak poskytuje expertízu a skúsenosti.

[32] GÁBRIŠ, T.: Cyber Law : textbook. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2014. s.174.

Slovenská republika urobila v oblasti kybernetickej bezpečnosti prvý krok, a to prijatím Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Predmetný dokument znamená posun v diskusii o kybernetickej bezpečnosti Slovenskej republiky a je základným a východiskovým dokumentom pre následnú tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zabezpečeniu kybernetickej bezpečnosti.

Vzhľadom na bezhraničnosť a všadeprítomnosť kybernetických hrozieb je viac ako potrebné vyvíjať medzinárodnú spoluprácu a riešiť otázku kybernetickej bezpečnosti nie len na národnej, ale najmä na medzinárodnej úrovni. V prípade nečinnosti môže dôjsť k materiálnym škodám, k ohrozeniu kritickej infraštruktúry štátu, bezpečného fungovania štátu a v neposlednom rade k nesplneniu medzinárodných záväzkov vyplývajúcich Slovenskej republike či už z členstva v Európskej únii, NATO, alebo inej medzinárodnej organizácii. Želaný stav ochrany národného kybernetického priestoru nemožno dosiahnuť len medzinárodnou spoluprácou, ale jednou z kľúčových úloh pri zabezpečení efektívneho nastavenia právnej úpravy kybernetickej bezpečnosti, je zosilnenie vzájomnej spolupráce medzi štátnym sektorom, súkromným sektorom, akademickou obcou a občianskou spoločnosťou.

Použitá literatúra:

GÁBRIŠ, T.: Cyber Law : textbook. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2014. 249 s. ISBN 978-80-7160-384-9.
MAISNER, M., VLACHOVÁ, B.: Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a.s., 2015. 232 s. ISBN 978-80-7478-817-8.
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
VRABKO, M. a kol.: Správne právo hmotné. Všeobecná časť. 1. vydanie. Bratislava: C. H. Beck, 2012, 480 s. ISBN 978-80-89603-03-9.
VLÁDA SLOVENSKEJ REPUBLIKY: Národná stratégia pre informačnú bezpečnosť Slovenskej republiky. Bratislava 2008. 28 s.
Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Európskej únii.
Návrh zákona, ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z.
EURÓPSKA KOMISIA: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels: 2013.
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Návrh Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020. Bratislava 2015. 21 s.
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY: Návrh Štatútu Komisie pre kybernetickú bezpečnosť. Bratislava 2015. 4 s.
Zákon č. 45/2011 Z.z. o kritickej infraštruktúre.
Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.
Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

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

ZODPOVEDNOSŤ WEBOVÉHO PORTÁLU ZA DISKUSNÉ PRÍSPEVKY

Martin Daňko, Matúš Mesarčík

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The core idea of the paper is assessment of liability of provider of web pages in connection with posts of users (third party) in internet discussions. The aim of the work is to find possible similarities and illustrate key common aspects of pertinent liability during analysis of national and European legislation connected with evaluation of impact of judicial decisions.
Immanent part of the paper is focused on the assessment of newest decision decided by Europena Court of Human Rights – Delfi v Estonia. Final part of the work deals with the theory of port security standing for specific requirements for providers of web portals. Once they are fulfilled the provider does not bear responsibility for the action of third parties.

Abstrakt: Témou predkladaného príspevku je zodpovednosť prevádzkovateľa webového portálu za príspevky užívateľov (tretích osôb) v diskusiách, ktoré sa nachádzajú na webovom priestore prevádzkovateľa. Analýzou ustanovení vnútroštátnych právnych predpisov v korelácii s právnou úpravou obsiahnutou v prameňoch európskeho práva, domácej ale aj zahraničnej judikatúry je ambíciou práce nájsť spoločné menovatele, ktoré by mali viesť k objasneniu limitov a kvality predmetnej zodpovednosti. Osobitnú pozornosť autori venujú najnovšiemu rozhodnutiu Európskeho súdu pre ľudské práva (ďalej len „ESĽP“) – Delfi v Estónsko, ktoré podnietilo obrovskú vlnu diskusií. V závere práce sa nachádza zopár úvah o koncepcii tzv. bezpečnostného prístavu – podmienok, za splnenia, ktorých je poskytovateľ služby chránený a nenesie zodpovednosť.

Key words: Cyberspace, Discussions, Comments, Liability, Provider of web page

Kľúčové slová: internet, diskusia, príspevky, zodpovednosť, prevádzkovateľ webového portálu.

1 ÚVOD

Problematika zodpovednosti webových portálov za príspevky na diskusných fórach je v slovenskom právnom poriadku pomerne málo sledovanou. Aj napriek skutočnosti, že 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. 284/2004 Z. z. (ďalej len „zákon o elektronickom obchode“ alebo „ZoEO“)[1] je súčasťou nášho právneho poriadku viac ako desať rokov, stále jeho výklad nemožno považovať za ustálený, čo samozrejme spôsobuje aplikačné problémy. Zodpovednostné vzťahy, ktoré môžu vzniknúť medzi poskytovateľom služieb informačnej spoločnosti (definovaný v § 2 písm. b) ZoEO) a príjemcom týchto služieb (def, v § 2 písm. c) ZEO), v aplikačnej praxi nemusia byť vzhľadom na absenciu ustálenej judikatúry dostatočne jasné. Ťažiskovým je tak hľadanie hmotnoprávneho základu zodpovednostného vzťahu prevádzkovateľa diskusného fóra, ktorý je nepochybne v právnom postavení poskytovateľa služieb informačnej spoločnosti na jednej strane a na druhej strane osobou, ktorá v postavení prijímateľa služieb, bola obsahom uloženým na internetových stránkach prevádzkovateľa diskusného fóra poškodená – bolo zasiahnuté do jej práv a právom

[1] Prijatím zákona o elektronickom obchode sa do právneho poriadku Slovenskej republiky implementovala Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode – smernica o elektronickom obchode, (Ú. v. ES L 178, 17. 7. 2000 upravujúca mimo iného aj problematiku zodpovednostných vzťahov medzi poskytovateľmi služieb informačnej spoločnosti a ich prijímateľmi v práve Európskej Únie.

chránených záujmov. V tomto smere je potrebné hneď v úvode spomenúť doktora Husovca, ktorý sa ako jeden z mála a možno jediný na Slovensku venuje problematike zodpovednosti na internete. Doktor Husovec vo svojich dielach analyzuje problematiku zodpovednosti na internete a ponúka riešenia a závery, s ktorými sa autori tohto článku zhodujú a vo svojej ďalšej právnej analýze z nich aj vychádzajú[2].

2 JUDIKATÚRA

Problematika zodpovednosti webového portálu za diskusné príspevky tretích osôb (užívateľov) bola ústrednou témou viacerých súdnych rozhodnutí, či už sa jednalo o rozhodovaciu činnosť súdov v Slovenskej republike, Českej republike alebo v rámci judikátov Európskeho súdu pre ľudské práva. Zodpovednosť webového portálu v relácii k diskusným príspevkom môže mať v zásade dvojakú podobu. Jednak môže ísť o diskusné príspevky užívateľov zasahujúce do práva na ochranu osobnosti zväčša prostredníctvom hanlivých resp. vulgárnych výrazov na adresu konkrétnych osôb (tzv. difamačné príspevky) alebo sa môže jednať o príspevky užívateľov prostredníctvom ktorých prispievajú k šíreniu nelegálneho materiálu prostredníctvom internetovej siete.[3] Rozhodnutia, ktoré sú predmetom analýzy tejto časti práce sú výlučne založené na skutkovom základe uvedeného v prvej kategórii vyššie spomenutej diferenciácie.

2.1. Prvé rozhodnutie v ére samostatnosti Slovenskej republiky zaoberajúce sa predmetnou zodpovednosťou je rozhodnutie Krajského súdu Trenčín pod spisovou značkou 19Co/35/2012. Skutkový stav prípadu spočíva v tom, že na webovom sídle občianskeho združenia, ktoré verejnosť oboznamovalo s regionálnymi novinkami boli v diskusii pod určitými článkami publikované príspevky, ktorými užívatelia pod rúškom anonymity častovali žalobcu výrazmi „zlodej“ a „podvodník“. Žalobca sa rozhodol brániť na súde a žiadal od poskytovateľa webového portálu/diskusného fóra odstránenie pikantných príspevkov, ospravedlnenie a náhradu nemajetkovej ujmy v peniazoch. Prvostupňový súd všetkým nárokom vyhovel. Žalovaný sa ale odvolal a Krajský súd v Trenčíne rozhodol, že žalovaný je povinný vymazať niektoré výrazy z diskusie a vo zvyšnej časti rozhodnutia návrh navrhovateľa zamietol. Vo všeobecnosti ale možno konštatovať, že v zmysle predmetného rozhodnutia prevádzkovateľ webového portálu nenesie zodpovednosť za anonymné príspevky tretích strán. Súd svoj postup odôvodnil hlavne nedostatkom v intenciách pasívnej a aktívnej legitimácie. V zmysle odôvodnenia tohto rozhodnutia je predpokladom úspešného uplatnenia práva na ochranu osobnosti neoprávnený zásah, ktorý je zároveň spôsobilý privodiť ujmu na chránených osobnostných právach. Nositeľom oprávnenia domáhať sa svojej právnej ochrany je fyzická osoba, do osobnostných práv ktorej bolo zasiahnuté. V tomto prípade možno kvitovať, že predmetné výrazy v diskusii prvostupňoví a súčasne aj odvolací súd vyhodnotili ako spôsobilé zasiahnuť do osobnostných práv nakoľko ich hlavným cieľom bolo zneuctenie a poníženie žalobcu.

Na strane druhej je ale potrebné vymedziť účastníka predmetného právneho vzťahu, ktorý je nositeľom povinnosti upustiť od neoprávnených zásahov do práva na ochranu osobnosti alebo odstrániť ich následky resp. poskytnúť primerané zadosťučinenie. Touto osobou je vždy tá osoba, ktorá sa dopustila určitého konania, neoprávnene zasahujúceho do chránených osobnostných práv. Vzhľadom na skutkové okolnosti prejednávaného prípadu možno zhodnotiť, že pasívne legitimovaným účastníkom je anonymný diskutér/anonymný diskutéri. Súd judikuje, že žalovaný ako prevádzkovateľ webového portálu nie je tou osobou, ktorá zasahuje do osobnostných práv navrhovateľa a protiprávneho úkonu sa nedopustil ani v prípade, že je registrátorom a prevádzkovateľom webového portálu, ktorý umožňuje tretím osobám uverejňovať svoje myšlienky a názory. Deliktu by sa ale dopustil v prípade, ak aj po právoplatnom rozhodnutí súdu napadnuté výrazy v diskusii ponechal. V tomto prípade by ale išlo o iný a samostatný delikt.[4]

---

[2] HUSOVEC, M.: Zodpovednosť na internete podľa českého a slovenského práva. Praha: CZ.NIC, 2014, 230 s., ISBN: 978-80-904248-8-3

[3] V tomto prípade sa môže jednať napr. o detskú pornografiu, propagáciu psychotropných látok alebo odkazy na bezplatné stiahnutie autorského diela.

[4] HUSOVEC, M. : Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osôb In *Revue pro právo a technologie Vol. 6/2012*, http://revue.law.muni.cz/dokumenty/21141 (dostupné 1.10.2015)

Predmetnú zodpovednosť ale nemožno v tomto prípade chápať absolútne. Podľa Husovca Krajsky súd Trenčín v tomto prípade pristúpil k príliš úzkemu výkladu § 13 Občianskeho zákonníka v súvislosti s otázkou pasívnej legitimácie, podľa ktorého má fyzická osoba najmä právo domáhať sa, aby sa upustilo od neoprávnených zásahov do práva na ochranu jej osobnosti, aby sa odstránili následky predmetných zásahov a aby bolo dané primárne zadosťučinenie. V zmysle autorovej interpretácie tak pasívne legitimovaný môže byť ktokoľvek, kto hoci len umožňuje páchanie deliktu tretiemu bez toho, aby ho sám páchal.[5] Za určitých okolností sa s týmto názorom možno stotožniť, nemožno ale takto postupovať vo všetkých prípadoch rovnako. Prevádzkovateľ blogu pod vlastným doménovým menom by bol v takomto prípade zodpovedný za komentáre pod svojimi článkami. Európska súdna prax ale precizovala v prípade L´oreal v eBay[6] určité hranice extenzívneho vnímania takejto legitimácie spočívajúce v účinnosti, primeranosti a zákazu vytvárať bariéry legitímnemu obchodu v spoločnosti. Z tohto hľadiska následne možno posúdiť ďalšie faktory ovplyvňujúce predmetnú „možnosť" spáchania deliktu ako napr. intenzita zásahu, dostupnosť a reálna možnosť verejnosti so zásahom prísť do styku a pod.

Krajský súd v Trenčíne tak povinnosť odstrániť určité výrazy z diskusie založil na aplikácii ustanovení zákona č. 22/2004 o elektronickom obchode.[7] Otázne ale je, že súd nariadil odstránenie iba špecifických výrazov a nie celého príspevku resp. kompletného diskusného vlákna. Z objektívneho hľadiska by sa možno zdalo vhodnejšie odstránenie celého príspevku/vlákna, keďže komentár typu „X. je..." alebo „všetci dobre vieme, aký je Y..." už majú ambíciu evokovať určité emócie a podozrenia, aj keď v tomto prípade by bolo veľmi náročné dokázať potencialitu zásahu do osobnostných práv resp. samotnú ujmu.[8]

2.2. Druhým rozhodnutím zo stredoeurópskeho priestoru, na ktoré sme upriamili pozornosť je rozhodnutie Vrchného súdu v Prahe 3 Cmo 197/2010. Skutková podstata sporu spočívala v tom, že žalobca (spoločnosť Prolux Consulting) zistil, že na stránke žalovaného subjektu (webový portál Internet Info) sa v diskusii pod článkom na tomto webovom portál nachádzajú príspevky, ktoré poškodzujú dobré meno žalobcu.[9] Spoločnosť Prolux Consulting následne vyzvala žalovaného, aby predmetné príspevky z diskusie odstránila. Webový portál ale túto žiadosť odmietol s poukazom na to, že nemá preukázanú nepravdivosť predmetných príspevkov. Prolux Consluting sa tak obrátila na súd a domáhala sa odstránenia príspevkov a finančnú náhradu nemajetkovej ujmy. Prvostupňový súd nariadil odstrániť celé diskusné vlákno bez nároku na finančnú satisfakciu.

Odvolací súd sa vo svojom odôvodnení venoval viacerým aspektom poskytovania služieb informačnej spoločnosti. V prvom rade sa zaoberal obsahom diskusných príspevkov a ich samotnou protiprávnosťou. Vrchný súd v Prahe judikoval, že konkréte výrazy diskutujúcich neobsahujú žiadnu informáciu, ktorú by bolo možné považovať za protiprávne, nepravdivé a dehonestujúce a sú len opisom skúsenosti diskutujúcich so službami žalobcu. Webový portál zároveň nemá povinnosť skúmať mieru pravdivosti jednotlivých skúseností s vyššie uvedenými službami žalobcu. Na strane druhej je ale prevádzkovateľ webového portálu povinný udržiavať určitú úroveň diskusie.

Nemenej dôležitým aspektom ale bola úvaha súdu nad samotnou zodpovednosťou za príspevky tretích osôb v rámci diskusii na webovom portály. Český súd v tomto prípade interpretoval ustanovenia zákona č. 480/2004 Sb. o niektorých službách informačnej spoločnosti a súčasne vymedzil dve podmienky na vyvodenie takejto zodpovednosti podľa § 5 ods. 1 spomínaného

[5] Tamže
[6] C-324/09, § 144
[7] Konkrétne §6 ods. 4
[8] V tejto súvislosti možno túto situáciu porovnať s rozhodnutím SDEÚ vo veci Google Spain týkajúce sa práva byť zabudnutý, kde bola prevádzkovateľovi vyhľadávača uložená povinnosť zmazať indexy, ktoré sa objavujú po zadaní mena určitej osoby na jej žiadosť z dôvodu neaktuálnosti a pod. Spoločnosť Google síce index zmaže ale v dolnej časti stránky, ktoré indexuje samotné výsledky sa objaví notifikácia, ktorá upozorňuje, že niektoré výsledky mohli byť odstránené na základe právnych predpisov Európskej únie o ochrane osobných údajov. V tomto prípade tak možno konštatovať, že samotné „zabudnutie" nie je až také efektívne ako by sa na prvý pohľad mohlo zdať.
[9] Konkrétne sa jednalo o výrazy „lže jako svině" a pokusy o likvidáciu žalobcu.

predpisu.[10] V prvom rade sa musí jednať o informácie, ktoré sú v rozpore s platným právom alebo o protiprávnom konaní užívateľa. Zároveň ale za predmetný obsah prevádzkovateľ zodpovedá iba v prípade, ak nenaplní liberačný dôvod, ktorý spočíva v dokázaní faktu, že o protiprávnosti informácie nemohol vedieť. V tomto prípade bol dubiózny práve konkrétny aspekt, vzhľadom na to, že bolo náročne dokázať skutočné poškodenie dobrého mena právnickej osoby.

Analýza vyššie spomenutých rozhodnutí ukázala určité tendencie v smerovaní pri posudzovaní problematiky zodpovednosti prevádzkovateľa webového portálu za príspevky tretích osôb v diskusiách. Styčným bodom v oboch sporoch bolo, že sa jednalo o veľmi podobné príspevky (ne)zasahujúce do osobnostných práv fyzickej osoby resp. dobrého mena právnickej osoby. Možno konštatovať, že v ani jednom prípade súd explicitne neinterpretoval právne predpisy v zmysle, že prevádzkovateľ je povinný kontrolovať obsah diskusných príspevkov bez vonkajšieho podnetu. Situácia sa ale mení v prípade, že na takýto príspevok bol upozornený alebo mal vedomosť o tom, že fórum obsahuje informácie zasahujúce do práv fyzických resp. právnických osôb.

2.3. Búrlivú diskusiu v ostatnom období vzhľadom na predmet predkladaného príspevku podnietilo rozhodnutie Európskeho súdu pre ľudské práva vo veci Delfi v Estónsko. Zo skutkového hľadiska sa predmetný judikát zaoberá situáciu, keď spoločnosť Delfi (estónska spoločnosť, ktorá vlastní najväčšie spravodajské portály v štáte) zverejnila článok o trajektovej spoločnosti o zmene trás trajektov v dôsledku čoho spoločnosť prerazila v určitých úsekoch ľad, ktorý slúžil ako alternatívna magistrála pre cestnú dopravu na ostrovy. Spravodajský portál ponúkal užívateľom možnosť komentovať článok v diskusii. Akási kontrola vhodnosti komentárov fungovala na dvoch princípoch: (i) tzv. *notice-and-take-down* systém, v ktorom každý užívateľ portálu mohol určitý komentár označiť ako nevhodný resp. obsahujúci hanlivé výrazy a ten bol po preskúmaní následné odstránený z diskusie a (ii) automatickej kontrole určitých slov a slovných spojení, ktoré automaticky neboli zverejňované. Estónska spoločnosť bola následne notifikovaná a nevhodností komentárov, ale tie vymazala až po šiestich týždňoch od ich zverejnenia. Estónsky súd prvého aj druhého stupňa zhodne uznali zodpovednosť spoločnosti Delfi za komentáre tretích osôb v diskusiách pod článkom na spravodajskom portály. Následne spor pokračoval pred Európskym súdom pre ľudské práva, ktorý po prvýkrát riešil predmetnú problematiku vo svojej rozhodovacej činnosti. Spravodajský portál ako reakciu na vyvodenie zodpovednosti urobil opatrenia v podobe zostavenia tímu moderátorov, ktorý mali na starosti kontrolu notifikovaných komentárov a súlad s novozavedenými pravidlami pridávania diskusných príspevkov.

V úvode samotného rozhodnutia súd pragmaticky hodnotí, že práva a povinnosti v kyberpriestore sa do určitej miery môžu a v niektorých prípadoch musia odlišovať od interpretácie záväzných pravidiel správania sa v reálnom svete.[11] Zároveň ale poukazuje na fakt, že táto platforma ponúka prakticky neobmedzený priestor na vyjadrovanie svojich názorov, ktoré v predmetnom prípade nabrali veľmi vulgárny a dehonestujúci ráz. Súčasne stanovuje, že prevádzkovateľ spravodajského portálu na základe interpretácie právnych predpisov a stálej judikatúry môže byť v zásade zodpovedný za zverejňovanie protiprávnych komentárov na svojom webovom sídle. Spoločnosť tak bola v pozícii, keď mohla odhadnúť svoje postavenie a povinnosti a predvídať určité aktivity svojich užívateľov.

Predmetný judikát zároveň stanovuje aj akúsi negatívnu enumeráciu subjektov na internete, ktorí za prejavy tretích osôb nezodpovedajú. Konkrétne sa jedná o diskusné fóra vo forme tzv. vývesiek, kde niet osoby, ktorá by diskusiu moderovala a takisto je zodpovednosti zbavený

[10] (1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen
a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

[11] § 113 predmetného rozhodnutia

prevádzkovateľ blogu alebo webstránky pre svoju súkromnú potrebu. Podobné by sa malo postupovať aj v prípade sociálnych sietí. [12]

Európsky súd pre ľudské práva svoje rozhodnutie postavil na hodnotení štyroch kľúčových aspektov: (i) kontexte komentárov, (ii) opatrení prijatých spoločnosťou v súvislosti s odstraňovaním difamačných príspevkov, (iii) alternatívy v podobe zodpovednosti samotných autorov predmetných príspevkov, (iv) následky rozhodnutia vnútroštátnych súdov pre prevádzkovateľ webového portálu.

V prípade kontextu komentárov súd posudzoval z viacerých hľadísk. V prvom rade konštatoval, že pozícia profesionálne vedeného spravodajského portálu je do určitej miery závislá aj od komerčných aktivít, ktoré priamo súvisia s počtom prístupov na danú webstránku a v konečnom dôsledku aj s komentovaním článkov. Osobitne by sme na tomto mieste chceli zvýrazniť, že prevádzkovateľ webového portálu nedal jednotlivým užívateľom možnosť upraviť alebo vymazať ich príspevky po ich publikácii. Fungoval iba vyššie spomenutý tzv. *notice-and-take-down system*. Na tomto podklade tak súd konštatoval že Delfi bolo v určitej miere povinné vykonávať kontrolu komentárov od užívateľov.

Zodpovednosť autorov komentárov je súdom analyzovaná z hľadiska anonymity, ktorú internet svojim užívateľom vo všeobecnosti poskytuje. Anonymitu možno podľa názoru súdu zadeliť do dvoch kategórii podľa možnosti identifikácie. V prvom prípade je užívateľ síce chránený a verejnosti neznámy pod svojou internetovou identitou, ale na druhej strane prevádzkovateľ služby informačnej spoločnosti disponuje určitým údajmi, na základe ktorých ho možno identifikovať (či už podľa poskytnutých osobných údajov pri registrácii, previazanosť užívateľského konta s profilom na sociálnej sieti a pod.). Naopak v niektorých prípadoch ale nie je založenie užívateľského konta podmienkou prispievania do diskusie a jediným možným spôsobom identifikácie je prístupový bod na internet tzv. IP adresa, ktorú definujeme ako logický identifikátor daného uzla (najčastejšie počítača) v sieti, ktorý komunikuje s inými uzlami prostredníctvom protokolu IP (internet).[13] Laicky povedané ide o unikátne označenie počítača používateľa pripojeného na internet. Každý, kto vstúpi do tohto špecifického prostredia tak automaticky získava svoju virtuálnu identitu. Tento fakt ale môže značne skomplikovať identifikáciu užívateľa. Na jednej strane môže jeden užívateľ používať viacero zariadení s prístupom na internet (doma, v internetovej kaviarni, v práci a pod.) a získať tak viac ako jednu identitu. Naopak ale môže nastať aj situácia, že jedno zariadenia používa viacero fyzických osôb a tie súborne reprezentuje jedna identita, aj keď sa jedná o väčší počet subjektov. Špecifickou stránkou IP adries je aj jej statická alebo dynamická forma. O statických IP adresách hovoríme vtedy, ak sa pri pripojení na internet ostáva rovnaká a nemenná. Naproti tomu dynamické IP adresy sú charakteristické tým, že pri viacerých pripojeniach do siete sa tento identifikátor môže meniť. Jedno zariadenie tak v konečnom dôsledku získava viacero označení. V praxi tak môžu nastať značné problémy s identifikáciou konkrétnych užívateľov, ktorý na webstránku pridali príspevky s nevhodným alebo protiprávnym obsahom. Podľa názoru Európskeho súdu pre ľudské práva tak žalobca správne určil žalovaného ako prevádzkovateľa webového portálu a nie konkrétnych užívateľov. Zaujímavá situácia by ale nastala, ak by pre pridanie príspevku do diskusie bola potrebná registrácia. Prevádzkovateľ by tak mal prístup k určitým dátam, ktoré by mohli mať relevanciu v súvislosti s identifikovaním. Na tomto mieste je ale potrebné dodať, že internet je platforma, ktorá poskytuje prakticky neobmedzený priestor pre možné zavádzanie týkajúce sa informácii o virtuálnej identite. O pasívnej legitimácie tretích osôb v rámci potenciálnej žaloby by tak mohli nastať značné pochybnosti.

Súd ako ďalšie kvalifikačné kritérium hodnotil mechanizmy prevádzkovateľa pri kontrole diskusných príspevkov. Súčasne zdôrazňuje, že citlivé príspevky boli vymazané až po šiestich týždňov od upozornenia. V tejto súvislosti sa ale ponúkajú dve roviny zodpovednosti. Prvá možnosť súvisí s *ex ante* fázou, na základe ktorej si spravodajský portál neplnil povinnosť monitorovať diskusné príspevky na svojom webovom sídle. Druhá rovina je už samotná zodpovednosť za nevymazanie komentára po jeho zverejnení na základe vlastnej iniciatívy. ESĽP konštatuje, že v tomto prípade by liberačným dôvodom bolo, ak by spravodajský portál bez meškania napadnuté diskusné príspevky z diskusie odstránil.[14] Svoje odôvodnenie oprel o analýzu technických možností prevádzkovateľa potrebných pre predmetný úkon. Ten mal k dispozícii automatický filter, ktorý

[12] § 116 predmetného rozhodnutia
[13] Adresa IP, http://sk.wikipedia.org/wiki/Adresa_IP (dostupné 2.10. 2015)
[14] § 153 predmetného rozhodnutia

mechanicky cenzuroval určité slová a slovné výrazy a už spomínaný *notice-take-down system* a skupinu moderátorov diskusii. Tieto mechanizmy v analyzovanom prípade ale zjavne zlyhali a osobitne zvýrazňuje, že možnosti súkromnej osoby ako obete prejavov nenávisti na internete v relácii k monitorovaniu obsahu siete sú v mnohých smeroch limitovanejšie ako možnosti prevádzkovateľa spravodajského portálu zabrániť alebo promptne citlivé príspevky odstrániť.

Na základe vyššie uvedených kritérií tak Európsky súd pre ľudské práva judikoval, že na predmetnom skutkovom základe je prevádzkovateľ webového portálu zodpovedný za príspevky tretích osôb v diskusiách na internete. Rozhodnutie spustilo lavínu nevôle hlavne zo strany prevádzkovateľov spravodajských portálov a niektoré dokonca odňali užívateľom možnosť pridávať komentáre k článkom a celé diskusné vlákna vymazali resp. znepristupnili. Na tomto mieste je ale potrebné poukázať na určité špecifiká daného prípadu, ktoré možno povedať zjemňujú kvalitu a imperatív celého rozhodnutia. (subjekt, lehota na odstránenie, mechanizmy)

Jeden zo základných aspektov, ktorý zohral rolu pri analýze prípadu zo strany ESĽP je nepochybne samotný subjekt, ktorý konanie na európskom súde inicioval. Jednalo sa o veľmi populárny spravodajský portál s obrovským vplyvom na trhu a ekonomickými aktivitami, ktoré súviseli so značným množstvom prístupov na webstránku počas dennej prevádzky. Na ilustrovanie dôležitosti tohto aspektu ponúkame porovnanie podobného príkladu z reality. Predstavme si, že na úradnú vývesku v centre mesta niekto vyvesí oznam, ktorým vulgárnym a dehonestujúcim spôsobom zasiahne do práva na ochranu osobnosti miestneho podnikateľa. Je predpoklad, že okolo daného miesta prejdú cez deň stovky ba až tisíce ľudí. Rozdielna situácia by ale nastala, ak by takýto oznam visel povedzme v bytovom dome alebo v miestnom klube, ktorý má výrazne nižšiu návštevnosť ako centrum mesta. V korelácii s virtuálnym priestorom by sa tak mohlo jednať napr. o blogy – pragmaticky rozhodnutím vylúčené negatívnou enumeráciou subjektov neaplikovateľnosti predmetného rozhodnutia. Teda možno povedať, že v prípade oznamu na úradnej výveske v centre mesta je úplne legitímne očakávať akúsi kvázi vyššiu *due dilligence* od osôb zodpovedných za jej obsah vzhľadom na potenciálne zásahy do práv a právom chránených záujmov ostatných.

Ďalším aspektom, ktorý si zasluhuje pozornosť je aj lehota v ktorej spravodajský portál napadnuté príspevky odstránil. Komentáre ponechal na stránke po dobu šiestich týždňov. Vzhľadom na veľmi jednoduchú možnosť odstránenia príspevkov možno konštatovať, že táto doba je neprimerane dlhá. V našom príklade s úradnou výveskou by pravdepodobne takéto neskoré odobratie oznamu spôsobilo výraznú ujmu do práv na ochranu osobnosti podnikateľa. Z tohto dôvodu je veľmi dôležité v každom prípade posudzovať aj časové kritérium, či už v ponechaní príspevku na webovom portály bez upozornenia resp. analyzovať dobu, po ktorú bol diskusný komentár zverejnený po upozornení na jeho nevhodnosť alebo protiprávnosť. Kameň úrazu tvorí predovšetkým primárne časové kritérium, ktoré je ale závislé od kvality kontroly diskusie v jednotlivých diskusných vláknach a v neposlednom rade aj od aktivity ostatných užívateľov a ich možnosti difamačné príspevky nahlásiť administrátorovi resp. moderátorom diskusie.

Nakoniec je potrebné vziať do úvahy aj technické možnosti prevádzkovateľa a mechanizmy súvisiace s odstraňovaním príspevkov. Podľa názoru súdu dosť závažným faktorom v predmetnom prípade bolo, že samotní užívatelia nemali možnosť svoje príspevky upravovať resp. mazať po ich zverejnení. Toto privilégium mal výhradne prevádzkovateľ diskusie, ktorý tak na svoje plecia vzal určitý podiel zodpovednosti za jej obsah. V ilustrovanom príklade by tak v prípade absencie možnosti kontroly obsahu úradnej vývesky bolo zrejmé legitímne očakávať určitý rozsah zodpovednosti od osôb na to poverených. Na druhej strane ale ťažko žiadať, aby každý populárnejší internetový portál si po tomto rozhodnutí zriadil armádu moderátorov, ktorí budú hliadkovať nad úrovňou komentárov. Takýto krok by bol minimálne finančne náročným, nehovoriac o tom, že by sa mohla narušiť už tak dosť krehká hranica medzi slobodou prejavu a právom na rešpektovanie súkromného života.

V súvislosti s predmetným judikátom Európskeho súdu pre ľudské práva je tak možno až príliš odvážne tvrdiť, že zakotvuje absolútnu zodpovednosť prevádzkovateľa webového portálu za diskusné príspevky tretích osôb. Z vyššie uvedenej analýzy vyplývajú viaceré špecifické okolnosti, ktoré je potrebné brať do úvahy pri posudzovaní tejto otázky. To ale neznamená, že toto rozhodnutie nemôže slúžiť ako memento zodpovedným subjektom pri podobných prípadoch. Mantinely manévrovania prevádzkovateľov sa tak do určitej miery zúžili.

3 ZÁVER

Ak by sa prípad obdobný, aký bol v Estónsku, riešil na Slovensku, predpokladáme, že zodpovednostné vzťahy by boli riešenie obdobne, ako tomu bolo vo veci spis. zn.19Co/35/2012 na Krajskom súde v Trenčíne. Ustanovenie § 6 ods. 4 ZoEO upravujúcj zodpovednosť poskytovateľa služieb informačnej spoločnosti za protiprávny obsah jednoznačne stanovuje povinnosť prevádzkovateľa internetového diskusného fóra ako poskytovateľa služieb odstrániť protiprávny obsah bez zbytočného odkladu, inak v opačnom prípade sa zodpovednosť za protiprávny obsah rozširuje aj na samotného poskytovateľa. Po notifikácií protiprávneho príspevku osobou dotknutou na svojich právach a právom chránených záujmoch musí prevádzkovateľ internetovej diskusie spraviť všetko preto, aby protiprávny obsah bol z jeho internetovej diskusie odstránený.

Otázkou je či samotný poskytovateľ služby dokáže posúdiť a vyhodnotiť protiprávnosť napadnutého obsahu. V tomto prípade ho ZoEO stavia do role „sudcu aj kata“. Poskytovateľ služieb sa musí rozhodnúť, či zoberie na seba túto rolu a odstráni príspevok, a na tak riskuje, že jeho konanie je v rozpore so slobodou prejavu autora tohto príspevku, alebo rozhodne, že príspevok nemá protiprávny obsah a v diskusií ho ponechá. Ponechaním riskuje možné právne následky v podobe zodpovednostných vzťahov podľa § 6 ZoEO, kde nemožno vylúčiť ani posudzovanie jeho konania, ako konania v rozpore s § 415 Občianskeho zákonníka, tzn. porušenie všeobecnej prevenčnej povinnosti. Použitie § 415 Občianskeho zákonníka sa môže zdať veľmi neistým a odvážnym spôsobom, ako sa domáhať (s následnou aplikáciou § 420 Občianskeho zákonníka) škody, ale pokiaľ by na svojich právach dotknutá osoba preukázala porušenie všeobecnej prevenčnej povinnosti u poskytovateľa služieb a v príčinnej súvislosti s porušením tejto povinnosti aj vznik škody (predovšetkým v prípadoch, kedy by bolo protiprávnosť obsahu možné takmer až objektívne predpokladať), nemožno túto aplikáciu vylúčiť.

Podľa nášho názoru obavy poskytovateľov internetových diskusií vyplývajúce z ich povinnosti kontrolovať obsah diskusných fór sú zbytočné. Máme zato, že prípadom Delfi sa len vytvoril spoločenský tlak na dôsledné uplatňovanie smernice o elektronickom obchode, a to v prípadoch, keď diskusné príspevky fungujú na spomínanom notice-and-take- down systéme.

V kontexte uvedeného je však dôležité poukázať na iný a nemenej dôležitý problém, ktorý v sebe problematika zodpovednosti za protiprávny obsah zverejnený v internetovej diskusií poskytovateľa služieb informačnej spoločnosti nesie. Je spravodlivé od prevádzkovateľa diskusie požadovať, aby bol v roly sudcu a kata a výlučne pomerne v krátkom čase (v našom zákone o elektronickom obsahu je použité spojenie „bez zbytočného odkladu“) rozhodol, či pridaný príspevok možno považovať za informáciu, ktorá má protiprávny obsah? V záujem poskytnutia istého riešenia uvedenej polemiky sme názoru, že by bolo možné dať možnosť poskytovateľovi služieb informačnej spoločnosti nie len odstrániť informácie s protiprávnym obsahom, ale aj právo umožniť zmazať tieto informácie osobami, ktoré sa ich protiprávneho obsahu domáhajú. Týmto spôsobom by sa preniesla rovina posudzovania protiprávnosti obsahu na dotknuté osoby a prevádzkovateľ diskusného fóra by bol zbavený tiaže zo zodpovednosti za protiprávny obsah - ako osoby v už spomínanej roly sudcu a kata práva slobody prejavu. Je zrejmé, že takáto možnosť by pre prevádzkovateľa internetových diskusií znamenala potreby technických zmien, ktoré by umožnili dotknutej osobe zmazať z jej pohľadu protiprávny príspevok, ale náklady môžu byť v súvislosti s možnosťou prenesenia zodpovednosti na iný subjekt považované za zanedbateľné. Skutočnou hrozbou uvedeného riešenia by bola jedine obava, že diskusné fóra by už nemuseli byť priestorom pre realizácie slobody prejavu a zmenili by sa na „polia vymazaných príspevkov“. No aj diskusné fórum má svoje „trhové pravidlá“, kde zárukou záujmu je kvalita prispievateľov a ich príspevkov, a preto uvedené riešenie by mohlo priniesť aj zodpovednejšie konanie samotných prispievateľov – príjemcov služieb informačnej spoločnosti.

Použitá literatúra:

GÁBRIŠ, T.: Cyber Law – 1.vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2014, 249 s., ISBN: 978-80-7160-384-9

HUSOVEC, M.: Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osôb. In *Revue pro právo a technologie Vol. 6/2012*,

HUSOVEC, M.: Zodpovednosť na internete podľa českého a slovenského práva. Praha: CZ.NIC, 2014, 230 s., ISBN: 978-80-904248-8-3

MAISNER, M. a kol.: Základy práva informačních technológií. Bratislava: Iura Edition, 2013. 317 s., ISBN: 978-80-8078-594-9

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

UBERIZÁCIA SLUŽIEB Z HĽADISKA PRÁVA SLOVENSKEJ REPUBLIKY

Tomáš Gábriš, Jakub Jošt

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The paper concentrates on the so-called uberization of services under the law of the Slovak Republic, mainly from the point of view of labour law, competition law, civil law (tort law) and administrative law.

Abstrakt: Príspevok skúma tzv. uberizáciu služieb v podmienkach právneho poriadku Slovenskej republiky, najmä z hľadiska pracovného práva, súťažného práva, občianskeho práva (zodpovednosti za škodu) a správneho práva.

Key words: Uber, cyberspace, Slovak Republic

Kľúčové slová: Uber, kyberpriestor, Slovenská republika

1 ÚVOD

Fenomén spoločnosti Uber a koncept jej fungovania je v súčasnosti už celosvetovo všeobecne známy. Uber je spoločnosť, ktorá prostredníctvom mobilnej aplikácie poskytuje možnosť stretu ponuky a dopytu vodičov automobilov a potenciálnych záujemcov o prepravu osôb (zákazníkov). Formálne možno túto službu vnímať ako delenie nákladov (*sharing economy*) na pohonné hmoty medzi vodiča a prepravovanú osobu. Fakticky však v niektorých prípadoch vodiči túto činnosť vedome a účelovo vykonávajú ako zárobkovú činnosť. Všetky platby pritom prebiehajú online. Zákazník zadá číslo platobnej karty, z ktorej mu Uber po ukončení jazdy odpočíta sumu za zvezenie. Vodič získa od Uberu raz do týždňa vyplatených 80 percent toho, čo zaplatili jeho zákazníci.[1] Takúto službu však veľmi negatívne vnímajú doterajšie taxislužby, ktorých poskytovanie obdobných služieb je limitované viacerými administratívnymi požiadavkami na úrovni zákona, ako aj všeobecne záväzných predpisov miest a obcí. Regulačné orgány zatiaľ k tejto problematike pristupujú s opatrnosťou, a ich prístupy sa v jednotlivých štátoch líšia[2] – osobitne v prípade USA sa uprednostňuje myšlienka nebrzdenia nových foriem podnikania a poskytovania služieb.[3]

[1] Pozri http://www.etrend.sk/financie/vyzera-to-ako-taxik-ale-taxik-to-nie-je-co-je-to-uber.html (navštívené dňa 7. 10. 2015); na výber sa ponúka päť úrovní – lacný UberX, klasický taxík UberTaxi, limuzína UberBlack, veľké UberSUV, či luxusné UberLux. V mnohých mestách je však stále v ponuke iba najnižšia UberX, zvaná aj UberPop. Pozri: http://ekonomika.sme.sk/c/7442829/aplikacia-uber-v-bratislave-vnikne-do-reviru-mestu-aj-taxisluzbam.html#ixzz3nsIKgKRf (navštívené dňa 7. 10. 2015).

[2] Pozri http://ekonomika.sme.sk/c/8011677/o-buducnosti-uberu-vo-francuzsku-rozhodoval-ustavny-sud.html?ref=trz (navštívené dňa 7. 10. 2015).

[3] DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1097 a nasl., s. 1105-1106. Odkazuje na: CHAPMAN, S.: The Flimsy Case for Regulating Uber. In: Chicago Tribune, 2. januára 2015. Dostupné na internete: http://www.chicagotribune.com/news/opinion/chapman/ct-uber-regulation-background-pricing-sexual-assault-perspec-0104-20150102-column.html, a na: http://perma.cc/RB4L-TF4N (navštívené dňa 7. 10. 2015) a WEBER, H.: As Uber Battles 13 Law-suits, Cabbies & State Agencies Are Out for Blood (Update). In: Venturebeat, 8. mája 2014. Dostupné na internete: http://venturebeat.com/2014/05/08/as-uber-battles-13-lawsuits-cabbies-state-agencies-are-out-for-blood/, a na: http://perma.cc/A2ZR-8BXB (navštívené dňa 7. 10. 2015).

Uber sa tak stal synonymom pre poskytovateľov služieb postavených na koncepte tzv. zdieľanej ekonomiky,[4] ktorého prejavy a realizácia sú niekedy vnímané ako na hrane zákona. Uber totiž spochybňuje tradičné poskytovanie služieb, ktoré si v mnohých prípadoch vyžaduje osobitné povolenia, a namiesto toho ponúka širokú možnosť poskytovať rovnaké služby v rámci zdieľanej ekonomiky komukoľvek. Koncept, ktorý využíva Uber, je totiž možné aplikovať aj na iné služby, než je poskytovanie služieb osobnej cestnej dopravy. Existuje viacero iných oblastí, ktoré sa „uberizujú“;[5] hovorí sa dokonca o uberizácii medicíny (napr. keď nemocnice zdieľajú lekárov),[6] či advokácie.[7] Takýto spôsob uberizácie – zdieľania profesionálov – pritom nemusí predstavovať závažnejší problém. Problém vyvstáva osobitne v prípadoch, keď ide o poskytovanie služieb osobami bez formálnych oprávnení na poskytovanú činnosť[8] - práve takéto obchádzanie povolení (koncesií) spôsobuje, že uberizácia služieb je médiami a tiež doterajšou konkurenciou v poskytovaní daných služieb vnímaná negatívne.[9]

Predmetom nášho príspevku bude však práve „uberizácia“ osobnej cestnej dopravy, čo je v súčasnosti v Slovenskej republike najvypuklejší problém.[10] V tejto súvislosti sa zameriame na právne výzvy, ktorým aplikácia spoločnosti Uber a jej užívatelia čelia z hľadiska vybraných právnych odvetví slovenského právneho poriadku.[11] Osobitne významnou právnou otázkou je pritom už základná otázka statusu spoločnosti Uber, totiž či Uber predstavuje dopravnú spoločnosť, alebo iba poskytovateľa služieb informačnej spoločnosti[12] ako tzv. TNC (Transportation network company). To je otázka, ktorú má aktuálne riešiť Súdny dvor Európskej únie,[13] čím sa reaguje na nejednotný prístup členských štátov EÚ vo vzťahu k Uberu, keď napr. Nemecko podstatne regulačne obmedzilo

---

[4] Pozri http://hn.hnonline.sk/slovensko-119/o-uber-na-slovensku-sa-uz-zaujima-aj-brusel-913034 (navštívené dňa 7. 10. 2015).

[5] MANJOO, F.: Uber, a Rising Business Model That Could Change How You Work. In: New York Times, 28. januára 2015. Dostupné na internete: http://www.nytimes.com/2015/01/29/technology/personaltech/uber-a-rising-business-model.html, a na: http://perma.cc/GJ8L-7V5V (navštívené dňa 7. 10. 2015); v oblasti stravovania ide napr. o službu Uber Eats: https://newsroom.uber.com/2015/04/ubereats-now-serving-chicago-nyc/ (navštívené dňa 7. 10. 2015). Tiež: http://style.hnonline.sk/digital-132/kontroverzna-taxisluzba-uber-vam-teraz-prinesie-domov-aj-oblubene-jedlo-743968 (navštívené dňa 7. 10. 2015).

[6] KHAN, F.: The “uberization” of healthcare: the forthcoming legal storm over mobile health technology’s impact on the medical profession. Dostupné na internete: http://works.bepress.com/fazal_khan/7/ (navštívené dňa 7. 10. 2015). Hovorí aj o osobitnom spôsobe uberizácie zdravotníctva – s. 4: „*if a mobile health evaluation indicates that a patient’s condition is serious enough to require professional attention, a health care plan could send out a “physician extender” (e.g., physician assistant, nurse practitioner, home health aide, etc.) to your home, workplace, or long-term care facility with portable diagnostic equipment and even a mobile pharmaceutical dispensary that wirelessly interfaces with your secure electronic medical records (EMR).*“ Ide vlastne o druh telemedicíny (e-Health).

[7] HALTOM, B.: Your Uber Attorney Is 2 Minutes Away. In: Tennessee Bar Journal, august 2015, s. 34-35.

[8] Pozri http://ekonomika.sme.sk/c/7991880/daniari-vodici-uberu-musia-mat-zivnost-aj-pokladnicu.html?ref=avizocl (navštívené dňa 7. 10. 2015).

[9] http://spravy.pravda.sk/ekonomika/clanok/367992-bratislavu-ochromi-strajk-taxikarov/ (navštívené dňa 7. 10. 2015).

[10] http://ekonomika.sme.sk/c/8004542/taxikari-zablokuju-bratislavu-chystaju-protest-proti-uberu.html?ref=trz (navštívené dňa 7. 10. 2015)

[11] Obdobne na problémy z hľadiska viacerých právnych odvetví z pohľadu práva USA upozornila DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1097 a nasl.

[12] T.j. v podstate sprostredkovanie dopravy, alebo dispečerské služby: Takto funguje aj dosiaľ fungujúca aplikácia Hopin. Cez ňu si zákazník, podobne ako pri Uberi, objedná vozidlo, no s tým podstatným rozdielom, že príde licencovaný taxikár. Pozri: http://www.etrend.sk/financie/vyzera-to-ako-taxik-ale-taxik-to-nie-je-co-je-to-uber.html

[13] http://www.euractiv.sk/lisabonska-strategia/clanok/aplikaciu-uber-preskuma-sudny-dvor-eu-023952

činnosť Uberu[14] (hoci Uber podala na Európskej komisii sťažnosť,[15] že nemecká regulácia taxislužieb a súťažné právo porušujú právo EÚ[16]), podobne ako Francúzsko.[17] V Španielsku je činnosť Uberu dokonca zakázaná,[18] a práve španielsky sudca sa obrátil na SD EÚ s otázkou ohľadom povahy spoločnosti Uber a služieb ňou poskytovaných.[19] Uber však stále funguje v Spojenom kráľovstve, Taliansku, Švajčiarsku a Írsku. Od augusta 2015 pritom pôsobí aj na Slovensku, a to zatiaľ bez väčších prekážok.[20]

2 PRACOVNÉ PRÁVO

Prvou otázkou, ktorej v súvislosti so službou poskytovanou spoločnosťou Uber budeme venovať pozornosť, je otázka statusu tejto spoločnosti a jednotlivých vodičov, ktorí ponúkajú možnosť zvezenia druhých osôb svojím automobilom, a to z hľadiska pracovného práva. Osobitne

[14] V Nemecku sa vyžaduje, aby vodiči mali rovnaké povolenia ako taxikári, a tiež sa im zakazuje akceptovať nových zákazníkov predtým, ako vysadia aktuálneho zákazníka, čím sa služba stáva menej atraktívnou, nakoľko vodiči musia dlhšie čakať na ďalšieho zákazníka. Pozri http://techcrunch.com/2015/07/15/following-uber-plea-european-commission-investigates-germanys-restrictions/ (navštívené dňa 7. 10. 2015).

[15] Európska komisia v tejto súvislosti spustí čoskoro celoeurópsku štúdiu v tejto súvislosti. Pozri https://www.theparliamentmagazine.eu/articles/news/eu-commission-launches-study-uber (navštívené dňa 7. 10. 2015).

[16] Obdobne sa Uber na Komisii sťažuje na Francúzsko a Španielsko. Pozri http://tech.eu/brief/judge-uber-european-court-of-justice/ (navštívené dňa 7. 10. 2015).

[17] Tzv. zákon Thevenoud vyžaduje, aby sa vodiči medzi jazdami vracali na stanovište, obmedzuje používanie lokalizačných softvérov za účelom hľadania klientov, a zakazuje nelicencované poskytovanie služby. Tento zákon Uber napadol pred francúzskymi súdmi aj pred Európskou komisiou. Pozri http://www.reuters.com/article/2015/03/31/us-france-uber-idUSKBN0MR0SQ20150331 (navštívené dňa 7. 10. 2015). Pozri tiež http://hn.hnonline.sk/svet-120/kauza-uber-vrcholi-zatkli-dvoch-manazerov-taxisluzby-822197 (navštívené dňa 7. 10. 2015). Napokon, francúzsky ústavný súd zakázal poskytovanie služieb spoločnosti Uber , pokiaľ vodiči nebudú spĺňať podmienky, ktoré musia spĺňať aj taxislužby: http://openiazoch.zoznam.sk/cl/160151/Francuzsky-sud-potvrdil-rozhodnutie-proti-sluzbe-Uber (navštívené dňa 7. 10. 2015).

[18] Pozri: http://skift.com/2015/04/30/why-ubers-one-size-fits-all-approach-didnt-work-in-spain/ (navštívené dňa 7. 10. 2015): „*UberPop was really popular in cities like Madrid and Barcelona. It's the low-cost version of UberX in the U.S. and allows any person with very few background-checks to drive people around the city in their own cars without a taxi license and also lets people split the fare with multiple passengers. This model is illegal in Spain and many European countries*."

[19] Pozri: http://tech.eu/brief/judge-uber-european-court-of-justice/ (navštívené dňa 7. 10. 2015): „*The specific questions the CJEU has been asked to rule on by the judge are:*

1) whether Uber provides a "mere transport activity" or "an electronic intermediation or information society service" in Europe

2) if partially an "information society" service , whether the American company should benefit from the principle of freedom to provide services guaranteed by Article 56 TFEU and Directive 2006/123/EC and Directive 2000/31/EC

3) whether Spanish unfair competition law as applied to "information society" services is contrary to European law, specifically Article 9 of the Services Directive, which states that an authorization, licensing or permits regime cannot be restrictive or disproportionate, and cannot unreasonably hinder the principle of freedom of establishment

4) whether the restrictions Spain is currently imposing on Uber (which is incorporated in the Netherlands), including court-ordered bans, are allowed if the service is able to benefit from the principle of freedom to provide services guaranteed by the aforementioned Article 56 TFEU and Directive 2006/123/EC and Directive 2000/31/EC."

[20] Pozri: http://www.etrend.sk/podnikanie/uberisti-to-su-ti-co-sa-musia-stat-platcami-dph.html (navštívené dňa 7. 10. 2015); tiež: http://www.cas.sk/clanok/328905/bratislavskym-vodicom-uberu-chce-mesto-klepnut-po-prstoch-za-chybajucu-licenciu-mastna-pokuta.html (navštívené dňa 7. 10. 2015).

v zahraničí sa totiž otvára otázka, či v prípade Uberu ide o zamestnávateľa, a či v prípade vodičov ide o samostatne zárobkovo činné osoby, alebo o zamestnancov.[21]

Z pohľadu slovenského Zákonníka práce v § 1 ods. 2 definuje závislú prácu (ktorá sa má vykonávať primárne v pracovnom pomere podľa Zákonníka práce) nasledovne:

(2) Závislá práca je práca vykonávaná vo vzťahu ***nadriadenosti zamestnávateľa a podriadenosti zamestnanca, osobne zamestnancom pre zamestnávateľa, podľa pokynov zamestnávateľa, v jeho mene, v pracovnom čase určenom zamestnávateľom***.

Ak by teda vodiči mali vo vzťahu k spoločnosti Uber (alebo teoreticky k jednotlivým zákazníkom) predstavovať zamestnancov, museli by títo vodiči byť k Uberu (alebo zákazníkom) vo vzťahu podriadenosti, prácu vykonávať osobne pre zamestnávateľa, podľa jeho pokynov, v jeho mene, a v pracovnom čase určenom zamestnávateľom. Znaky závislej práce pritom musia byť naplnené kumulatívne.

Pokiaľ ide o prvú čiastkovú otázku podriadenosti, máme za nepochybné, že vodiči nie sú (resp. nemali by byť) Uberu a ani zákazníkom podriadení v takom zmysle, aby od nich boli závislí a teoreticky môžu rovnaké služby poskytovať aj bez spoločnosti Uber a jej aplikácie. Navyše, v spojení s druhým znakom závislého postavenia – výkonom „pre zamestnávateľa" platí, že vodiči svoje služby poskytujú primárne zákazníkom, nie Uberu; Uber tu vystupuje nanajvýš ako sprostredkovateľ. Ohľadom konania „podľa pokynov zamestnávateľa" platí, že Uber nemôže žiadnemu vodičovi prikázať akceptovať ktoréhokoľvek zákazníka. Uber iba oznamuje vodičovi, kto má záujem o jeho služby – samotné rozhodnutie o akceptovaní tejto ponuky zostáva na vodičovi. Vodiči tiež striktne vzaté nevykonávajú činnosť „v mene" spoločnosti Uber (hoci „branding" spoločnosti Uber pritom hrá podstatnú rolu) – každému zákazníkovi by totiž malo byť zrejmé, že vo veci realizácie osobnej dopravy nevstupuje do vzťahu so spoločnosťou Uber, ale priamo s vodičom. Uber iba umožňuje zákazníkovi nájsť vodiča ochotného ho odviezť na ním požadovanej trase. Napokon, ani „pracovný čas" vodičom neurčuje Uber, nakoľko je plne na vôli vodiča, do akej miery a v akom rozsahu bude zákazníkom poskytovať svoje služby.

Záverom teda môžeme konštatovať, že medzi vodičom a spoločnosťou Uber podľa nášho názoru nedochádza k vzniku pracovnoprávneho pomeru. Inou by zrejme bola situácia, ak by vzťah medzi vodičom a spoločnosťou bol taký, že vodič by bol povinný akceptovať zákazníkov, ktorých mu určí Uber, a to v čase, ktorých mu určí spoločnosť Uber.

Obdobne možno konštatovať, že ani vo vzťahu vodiča a zákazníka tiež nejde o pracovnoprávny vzťah, nakoľko ide o zväčša jednorazový alebo ojedinelý, nepravidelný vzťah, v ktorom vodič nie je povinný zákazníka akceptovať, poskytnúť mu svoje služby, nie je od neho závislý, nie je zákazníkovi podriadený, ani nevykonáva prácu vodiča v mene zákazníka (hoci je pravda, že ju vykonáva zásadne podľa jeho pokynov a v čase ním určenom).

3 OCHRANA SPOTREBITEĽA

Ďalšou právnou otázkou, ktorú možno v súvislosti s využívaním aplikácie spoločnosti Uber otvoriť, je otázka, či vodiči predstavujú obchodných partnerov Uberu, t.j. podnikateľov (dodávateľov), alebo ide o spotrebiteľov produktu – služieb – spoločnosti Uber.[22] Postavenie samotnej spoločnosti Uber je pritom nepochybne postavením podnikateľa (dodávateľa), a postavenie koncových zákazníkov je zase nepochybne zväčša postavením spotrebiteľa.

[21] DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1105-1106. Odkazuje na EPSTEIN, Richard: Uber and Lyft in California: How to Use Employment Law to Wreck an Industry. In: Forbes, 16. marca 2015. Dostupné na internete: http://www.forbes.com/sites/richardepstein/2015/03/16/uber-and-lyft-in-california-how-to-use-employment-law-to-wreck-an-industry/, a na: http://perma.cc/FGV9-XQJT (navštívené dňa 7. 10. 2015); HUET, E.: What Happens to Uber Drivers and Other Sharing Economy Workers Injured on the Job? In: *Forbes*, 6. januára 2015. Dostupné na internete: http://www.forbes.com/sites/ellenhuet/2015/01/06/workers-compensation-uber-drivers-sharing-economy/, a na: http://perma.cc/9JUJ-ZS2Y (navštívené dňa 7. 10. 2015).

[22] DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1130.

Použité pojmy – dodávateľ a spotrebiteľ – nám v slovenskom právnom poriadku definuje všeobecný predpis – Občiansky zákonník. Podľa § 52 ods. 3 Občianskeho zákonníka, „*dodávateľ je osoba, ktorá pri uzatváraní a plnení spotrebiteľskej zmluvy koná v rámci predmetu svojej obchodnej alebo inej podnikateľskej činnosti*.“ Podľa ods. 4, „*spotrebiteľ je fyzická osoba, ktorá pri uzatváraní a plnení spotrebiteľskej zmluvy nekoná v rámci predmetu svojej obchodnej činnosti alebo inej podnikateľskej činnosti*.“ Je teda nepochybné, že služby spoločnosti Uber sú poskytované v rámci obchodnej alebo inej podnikateľskej činnosti. Obdobne je zrejmé, že samotní zákazníci, využívajúci služby Uberu a vodičov, väčšinou nekonajú v rámci predmetu svojej obchodnej činnosti alebo inej podnikateľskej činnosti. Otáznym je však status vodičov. Ak by šlo o zamestnancov spoločnosti Uber, čo sme vyššie popreli, šlo by o pracovnoprávny vzťah, nie o spotrebiteľský vzťah. Ak však nejde o zamestnancov, mohlo by tiež ísť o osoby konajúce v rámci predmetu svojej obchodnej činnosti alebo inej podnikateľskej činnosti. Dôležité je teda posúdiť, či v prípade vodičov ide o výkon obchodnej alebo podnikateľskej činnosti. Aktuálny postoj slovenských správnych a osobitne finančných orgánov je pritom ten, že ide o podnikanie, ktoré si vyžaduje splnenie podmienok zákona č. 56/2012 Z.z. o cestnej doprave, a to za rovnakých podmienok, aké musia plniť najmä taxikári. Inak ide o neprávnené podnikanie.[23] Otáznym sa pritom javí, či ide skutočne o podnikateľov aj v prípadoch, ak nejde o pravidelnú činnosť, a činnosť je teda v podstate napr. iba jednorazová. V takomto prípade by totiž nemusela byť naplnená definičná požiadavka podnikania podľa živnostenského zákona,[24] Obchodného zákonníka,[25] ani iného osobitného zákona.[26]

4 SÚŤAŽNÉ PRÁVO

Bez ohľadu na to, či samotný vodič je podnikateľom (dodávateľom) alebo nie, a teda či ide o spotrebiteľský alebo obchodný vzťah s Uberom, status Uberu môžeme v súlade s jeho vyššie

[23] Pozri: https://www.podnikajte.sk/start-podnikania/c/1031/category/registracne-povinnosti/article/neopravnene-podnikanie.xhtml#sthash.nXiorSRM.dpuf (navštívené dňa 7. 10. 2015).

[24] § 2 zákona č. 455/1991 Zb. o živnostenskom podnikaní: „*Živnosťou je sústavná činnosť prevádzkovaná samostatne, vo vlastnom mene, na vlastnú zodpovednosť, za účelom dosiahnutia zisku a za podmienok ustanovených týmto zákonom*.“

[25] § 2 ods. 1 Obchodného zákonníka č. 513/1991 Zb.: „*Podnikaním sa rozumie sústavná činnosť vykonávaná samostatne podnikateľom vo vlastnom mene a na vlastnú zodpovednosť za účelom dosiahnutia zisku*.“

[26] Činnosť je vykonávaná sústavne, ak je vykonávaná opakovane alebo so zámerom jej opakovaného vykonávania. Živnosťou nie je činnosť, ktorá je vykonávaná jednorazovo alebo sporadicky, resp. občas. Porovnaj: https://www.podnikajte.sk/start-podnikania/c/1031/category/registracne-povinnosti/article/neopravnene-podnikanie.xhtml#sthash.nXiorSRM.dpuf (navštívené dňa 7. 10. 2015).V tejto súvislosti možno poukázať aj na službu AirBnB, ktorá spočíva tiež na princípe zdieľanej ekonomiky – konkrétne ide o krátkodobé prenájmy nehnuteľností (bytov a bytových priestorov). „*V zmysle živnostenského zákona nie je v prípade prenájmu nehnuteľností, bytových a nebytových priestorov potrebné ohlásiť živnosť, ak sú v súvislosti s prenájmom poskytované len základné služby. Pojem základné služby nie je v živnostenskom zákone definovaný, preto je potrebné vychádzať zo zvyklostí (praxe). Podľa zoznamu odporúčaných označení voľných živností a ich bližšieho vymedzenia, ktorý je dostupný na internetovej stránke Ministerstva vnútra SR, k základným službám patria napríklad: dodávka tepla a teplej úžitkovej vody, elektrickej energie, plynu, odvoz tuhého komunálneho odpadu, odvod odpadovej vody alebo odvod splaškov, kominárske služby, upratovanie spoločných priestorov a pod. Aj v tomto prípade je vhodné informovať sa na živnostenskom úrade ešte pred začiatkom prenájmu*.“ Citované podľa: https://www.podnikajte.sk/start-podnikania/c/1031/category/registracne-povinnosti/article/neopravnene-podnikanie.xhtml#sthash.nXiorSRM.dpuf (navštívené dňa 7. 10. 2015).

„*Príklad: Ak by súčasťou nájomnej zmluvy bolo poskytovanie upratovacích prác priestorov pre ubytovaných, ide o službu nad rámec základných služieb. V tomto prípade by sa prenajímateľ dopustil neoprávneného podnikania, ak by neohlásil prevádzkovanie živnosti.*“ Tamže. Ak prenájom nehnuteľností zahŕňa aj doplnkové služby, možno týmto spôsobom podnikať len na základe živnostenského oprávnenia.

podanou charakeristikou vnímať ako status sprostredkovateľa – či už podľa Občianskeho alebo Obchodného zákonníka.

Podľa § 774 Občianskeho zákonníka, „*sprostredkovateľskou zmluvou sa sprostredkovateľ zaväzuje obstarať záujemcovi za odmenu uzavretie zmluvy a záujemca sa zaväzuje sprostredkovateľovi poskytnúť odmenu vtedy, ak bol výsledok dosiahnutý pričinením sprostredkovateľa*.“ Obdobne, podľa § 642 Obchodného zákonníka, „*zmluvou o sprostredkovaní sa sprostredkovateľ zaväzuje, že bude vyvíjať činnosť smerujúcu k tomu, aby záujemca mal príležitosť uzavrieť určitú zmluvu s treťou osobou, a záujemca sa zaväzuje zaplatiť sprostredkovateľovi odplatu (províziu)*.“

Ak by sme mali za to, že vodiči vykonávajú svoju činnosť ako podnikanie, teoreticky by do úvahy prichádzala aj možnosť, že Uber by pôsobil ako obchodný zástupca vodičov v zmysle § 652 Obchodného zákonníka: „*zmluvou o obchodnom zastúpení sa obchodný zástupca ako podnikateľ zaväzuje pre zastúpeného vyvíjať činnosť smerujúcu k uzatvoreniu určitého druhu zmlúv (ďalej len „obchody“) alebo dojednávať a uzatvárať obchody v mene zastúpeného a na jeho účet a zastúpený sa zaväzuje zaplatiť obchodnému zástupcovi províziu*.“

Samozrejme, v praxi ide v skutočnosti o inominátny zmluvný vzťah, ktorý zrejme vykazuje znaky oboch uvedených zmluvných typov.

Ak by sme pritom akceptovali možnosť, že vodiči sú obchodnými partnermi spoločnosti Uber, a nie sú spotrebiteľmi, môžeme plynulo prejsť k otázke, či v tomto obchodnom vzťahu Uber nezneužíva svoje postavenie na trhu vo vzťahu k svojim obchodným partnerom a ku konkurencii (osobitne taxislužbám) v zmysle nedovoleného obmedzovania hospodárskej súťaže alebo nekalej súťaže (§ 42 Obchodného zákonníka). V USA tak napríklad vodiči a taxislužby žalovali Uber z dôvodu, že núti vodičov požadovať za poskytnutie služby zákazníkovi odplatu (ktorú nazýva ako „gratuity“, t.j. akési „sprepitné“), z ktorej núti vodičov odovzdávať podiel spoločnosti Uber (pričom suma „gratuity“ prekračuje výšku odmien určenú všeobecne záväzným predpisom pre taxislužby), príp. núti vodičov poskytovať zákazníkom zľavy,[27] aké určí Uber. Osobitne z dôvopdu označovania poplatku ako „gratuity“ sa ozývajú aj tvrdenia, že Uber postupuje nekalo aj voči zákazníkom (ktorí sú zväčša spotrebiteľmi), ktorým poskytuje nepravdivé informácie o svojej službe,[28] prípadne že zavádza aj o poistení vodičov.[29] Nepochybne by pritom bolo zaujímavé z hľadiska ochrany spotrebiteľa a neprijateľných zmluvných podmienok preskúmať aj všeobecné obchodné podmienky poskytovania služby Uber, na to však na tomto mieste nemáme priestor.

5 ZODPOVEDNOSTNÉ VZŤAHY

Osobitným právnym problémom, ktorý sa v súvislosti so spoločnosťou Uber často pertraktuje, je otázka právnej zodpovednosti. V prvom rade sa spoločnosti Uber vytýka, že vodičov nevyberá dostatočne dôkladne, resp. že ich nevyberá na základe dostatočných výberových kritérií.[30] V druhom rade sa kritizuje, že vodiči nie sú dostatočne poistení.[31] V tejto súvislosti však treba

[27] Pozri: http://finweb.hnonline.sk/spravy-zo-sveta-financii-126/kontroverzna-taxisluzba-zaziva-dalsi-protest-vo-vlastnych-radoch-633680 (navštívené dňa 7. 10. 2015).

[28] WARD, S. F.: ‘App‘ Me a Ride: Internet car companies offer convenience, but lawyers see caution signs. In: ABA Journal, január 2014.

[29] DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1105-1106.

[30] Pozri napr. LOPEZ, A.: Prices Slashed for UberX as Opposition Raise Questions Over Safety. In: *NBC Los Angeles*. Dostupné na internete: http://www.nbclosangeles.com/news/local/UberX-Cuts-Prices-as-Opposition-Raises-Questions-Over-Safety-264278051.html, a na: http://perma.cc/W2ZY-VHB3 (navštívené dňa 7. 10. 2015).

[31] Pozri FRIEDHOFF, S.: Insurance Could Make Road Bumpy for Uber and Lyft. In: BOSton GLOBE, 7. januára 2015. Dostupné na internete: http://www.bostonglobe.com/business/2015/01/07/insurance-questions-latest-bump-road-for-ride-share-companies/wegXpHUBpZHwtUXNHJSf6H/.html, a na: http://perma.cc/MRF4-YK5T (navštívené dňa 7. 10. 2015). Od 1. júla 2015 Kalifornia vyžaduje, aby vodiči mali poistenie už od okamihu nalogovania do aplikácie, bez ohľadu na to, či vezú pasažiera – k nehode totiž môže dôjsť aj v procese preberania zákazky, pred tým, ako zákazník do automobilu nastúpi. Pozri DAVIS, J.:

konbštatovať, že táto kritika by bola opodstatnenou, pokiaľ by Uber mal byť považovaný za dopravnú spoločnosť, kde vodiči vystupujú v mene spoločnosti. Spoločnosť Uber však odmieta, že by v prípade vodičov šlo o jej zamestnancov – vyberá ich teda zrejme nie primárne z toho dôvodu, aby zabezpečila kvalitné poskytovanie dopravných služieb, ale skôr preto, aby zabezpečila dôveryhodnosť samotnej aplikácie Uber. Je však otázne, či tým spoločnosť Uber neprekračuje hranice "bezpečného prístavu" poskytovateľa služieb informačnej spoločnosti, ktorý zásadne, pokiaľ aktívne nezasahuje do obsahu poskytovanej služby a nevyberá príjemcu informácií (služieb), nezodpovedá za obsah poskytovanej služby.[32] Nárokmi kladenými na vodičov a ich vozidlá sa však javí, akoby Uber preberal zodpovednosť za výber vodičov a za kvalitu nimi poskytovaných služieb. Ak by takto postupoval akýkovek poskytovateľ služieb informačnej spoločnosti (napr. v prípade prevádzkovateľov internetových portálov), zrejme by takýmto konaním prekračoval bezpečný prístav „nevedomého poskytovateľa", a prechádzal by do pozície poskytovateľa, ktorý vykonáva kontrolu nad obsahom poskytovaných služieb a obsahom komunikácie jeho zmluvných partnerov či zákazníkov. Je preto iba otázkou času, kedy sa obdobne ako v prípade poskytovateľov služieb informačnej spoločnosti objaví aj v súvislosti so sprostredkovaním služieb zdieľanej ekonomiky úvaha o zodpovednosti za obsah, resp. kvalitu zdieľanej služby, a prvé prelomové súdne rozhodnutie v tejto súvislosti.[33]

6 ZODPOVEDNOSTNÉ VZŤAHY

Podstatná časť kritiky „uberizácie" služieb sa zameriava na skutočnosť, že niekedy ide o poskytovanie služieb obdobných alebo rovnakých ako sú služby, ktorých poskytovanie si inak vyžaduje osobitné povolenia, či koncesie. Príkladom môže byť konkurencia aplikácie Uber taxislužbám, ktoré musia spĺňať osobitné nároky a podmienky zákona o cestnej doprave č. 56/2012 Z.z. Kritici túto situáciu porovnávajú s poskytovaním lekárnických, či zdravotníckych služieb bez potrebného povolenia.[34]

Zákon o cestnej doprave č. 56/2012 Z.z. pritom v Slovenskej republike upravuje:

a) prístup k výkonu povolania prevádzkovateľa cestnej dopravy,
b) pravidlá podnikania v cestnej doprave,
c) zabezpečovanie dopravnej obslužnosti územia v pravidelnej doprave,
d) práva a povinnosti dopravcov a cestujúcich v autobusovej doprave a v taxislužbe,

---

Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015, s. 1112.

[32] Pozri § 6 ods. 1 zákona č. 22/2004 Z.z. o elektronickom obchode: „*Poskytovateľ služieb nezodpovedá za prenášané informácie, ak služby informačnej spoločnosti pozostávajú výlučne z prenosu informácií v elektronickej komunikačnej sieti alebo z poskytnutia prístupu do elektronickej komunikačnej siete, a poskytovateľ služieb*
a) nedal podnet na prenos informácií,
b) nevybral príjemcu informácií,
c) nezostavil ani neupravil informácie."
Ide o ustanovenie prevzaté z čl. 12 smernice 2000/31/ES o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode).

[33] Napríklad v prípade obdobnej služby ako poskytuje spoločnosť Uber, konkrétne v prípade spoločnosti Lyft, jej právny zástupca výslovne konštatuje, že Lyft sa považuje za poskytovateľa služieb informačnej spoločnosti v zmysle čl. 230 zákona Communication Decency Act z roku 1996, podľa ktorého poskytovateľ interaktívnej počítačovej služby nemôže byť považovaný za vydavateľa alebo pôvodcu informácií poskytovaných iným poskytovateľom informácií: „*no provider or user of an interactive computer service can be treated as the publisher or speaker of information provided by another "information content provider."*" Pozri WARD, Stephanie Francis: 'App' Me a Ride: Internet car companies offer convenience, but lawyers see caution signs. In: *ABA Journal*, január 2014. Na druhej strane sa však ozývajú hlasy, že ak spoločnosť vodičov vybavuje GPS zariadeniami, označuje ich svojou značkou, prekračuje hranice čl. 230 zákona. Tamže.

[34] WARD, S. F.: 'App' Me a Ride: Internet car companies offer convenience, but lawyers see caution signs. In: ABA Journal, január 2014.

Otáznym tu je, či spoločnosť Uber a jednotliví vodiči vykonávajú povolanie prevádzkovateľa cestnej dopravy, podnikajú v cestnej doprave, resp. či sú dopravcami v taxislužbe. Dôležitým môže byť v tejto súvislosti ustanovenie, poda ktorého sa tento zákon nevzťahuje na „cestnú dopravu pre vlastnú potrebu". Vlastná potreba je pritom definovaná odkazom na čl. 2 ods. 5 nariadenia Európskeho parlamentu a Rady (ES) č. 1073/2009 tak, že ide o poskytovanie dopravných služieb vlastným automobilom, pričom nejde o primárnu činnosť dopravcu, a doprava je poskytovaná na nekomerčné účely.[35] Ak by teda služby sprostredkúvané Uberom a obdobnými spoločnosťami boli skutočnou „zdieľanou ekonomikou" v úzkom zmysle, teda v zmysle zdieľania nákladov na spoločnú prepravu osôb jedným automobilom, a pre vodiča by nešlo o zárobkovú činnosť, ale len o vedľajšiu aktivitu bez komerčného (obchodného) cieľa, zrejme by služby vodičov nespadali pod ustanovenia zákona o cestnej doprave a nevyžadovali by sa pre nich ani povolenia, aké sa vyžadujú v prípade taxislužby**.**

Na taxislužby sa totiž vzťahuje osobitný § 26 citovaného zákona, podľa ktorého taxislužba je prevádzkovanie osobnej dopravy vozidlami taxislužby ako prepravy jednotlivých cestujúcich alebo skupiny cestujúcich do cieľového miesta podľa zmluvy o preprave osôb. Dopravca môže ponúkať poskytovanie dopravných služieb zverejnením základných podmienok ich poskytovania na stanovišti taxislužby, na svojom webovom sídle, na vozidlách taxislužby, formou reklamy alebo zriadením dispečingu a propagáciou objednávkovej služby. Obec môže navyše všeobecne záväzným nariadením ustanoviť podrobnosti o výkone taxislužby na území obce a vydať prevádzkový poriadok stanovišťa taxislužby.

Dopravca môže uzavrieť zmluvu o preprave osôb s cestujúcim:

a) prostredníctvom vodiča vozidla taxislužby na stanovišti taxislužby alebo kdekoľvek na území určenom v koncesii, kde sa počas jazdy bez cestujúceho nachádza s vozidlom taxislužby,

b) vo svojom sídle, na inom vopred zverejnenom mieste alebo na obvyklej zastávke vozidla taxislužby na pravidelnej trase, ktorá však nesmie byť súbežná s trasou autobusovej linky, alebo

c) prostredníctvom dispečingu.

Podmienky prevádzkovania taxislužby upravuje § 27 zákona: prevádzkovať taxislužbu môže len držiteľ koncesie podľa tohto zákona.

Práve tieto normy pritom spôsobujú, že úprava podmienok pre prevádzkovateľov taxislužieb, resp. dopravcov v rámci taxislužieb sa javí ako podstatne zväzujúcejšia v porovnaní so službami poskytovanými vodičmi prostredníctvom aplikácie Uber. Preto prevádzkovatelia taxislužieb spoločnosť Uber a jej model zdieľanej ekonomiky vehementne odmietajú.

S rovnakým problémom sa pritom aplikácia spoločnosti Uber stretáva na celom svete – rozdielny je však prístup autorít k riešeniu tejto situácie – napríklad zodpovedné kalifornské autority túto situáciu nateraz vyriešili tak, že vytvorili vo svojich predpisoch osobitnú kategóriu TNC – „transportation network company", ktoré musia požiadať o licenciu a zároveň preverovať register trestov vodičov, poskytnúť vodičom tréning, úplne vylúčiť tolerovanie drog a alkoholu u vodičov, a zabezpečiť poistné krytie vo výške aspoň 1 milióna dolárov.[36] Ide teda o osobitnú úpravu poskytovania služieb cestnej dopravy obdobných taxislužbám, ale s voľnejším režimom. Zároveň však tiež ide o úpravu, ktorá sa javí byť osobitnou aj vo vzťahu k poskytovaniu služieb informačnej spoločnosti, a zavádzajúcou osobitné podmienky pre poskytovanie takých služieb informačnej

---

[35] „*5.* ***'own-account transport operations'*** *means operations carried out for non-commercial and non-profit-making purposes by a natural or legal person, whereby:*

— *the transport activity is only an ancillary activity for that natural or legal person, and*

— *the vehicles used are the property of that natural or legal person or have been obtained by that person on deferred terms or have been the subject of a long-term leasing contract and are driven by a member of the staff of the natural or legal person or by the natural person himself or by personnel employed by, or put at the disposal of, the undertaking under a contractual obligation;...*"

Ods. 4 daného článku nariadenia pritom pozná aj definíciu občasnej dopravy – „*4.* ***'occasional services'*** *means services which do not fall within the definition of regular services, including special regular services, and the main characteristic of which is the carriage of groups of passengers constituted on the initiative of the customer or the carrier himself; ...*"

[36] WARD, S. F.: 'App' Me a Ride: Internet car companies offer convenience, but lawyers see caution signs. In: ABA Journal, január 2014. Spoločnosť Lyft napríklad vyžaduje, aby vodiči nepoužívali autá staršie ako vyrobené v roku 2000.

spoločnosti, kde poskytovateľ koná nad rámec poskytovania služieb informačnej spoločnosti – tým, že sa spolupodieľa aj na výbere adresátov (príjemcov) služieb, a vykonáva nad nimi istý dohľad. Toto riešenie pritom môže slúžiť ako inšpirácia aj pre prípadnú úpravu v členských štátoch EÚ.

7 ZÁVER

V príspevku sme podrobili aplikáciu spoločnosti Uber právnej analýze z hľadiska vybraných aspektov slovenského právneho poriadku.

Z hľadiska pracovného práva pritom podľa nás medzi vodičom a spoločnosťou Uber nedochádza k vzniku pracovnoprávneho pomeru. Ani vo vzťahu vodiča a zákazníka tiež v žiadnom prípade nejde o pracovnoprávny vzťah. V oboch prípadoch absentuje naplnenie znakov závislej práce – podriadenosť zamestnanca, výkon práce pre zamestnávateľa, podľa jeho pokynov, v jeho mene a v pracovnom čase určenom zamestnávateľom.

Z hľadiska ochrany spotrebiteľa sme dospeli k záveru, že spoločnosť Uber predstavuje dodávateľa (podnikateľa, konajúceho na základe inominátnej zmluvy obdobnej sprostredkovateľskej zmluve alebo zmluve o obchodnom zastúpení), a zákazník zásadne predstavuje spotrebiteľa, nekonajúceho v predmete svojej podnikateľskej činnosti. V prípade vodičov prevažuje v súčasnosti v SR u orgánov finančnej správy mienka, že ide o výkon podnikateľskej činnosti obdobný poskytovaniu taxislužby. My sa však domnievame, že odpoveď na túto otázku závisí od rozsahu, v akom vodič službu poskytuje – definičným znakom podnikania je totiž to, že je to sústavná činnosť vykonávaná podnikateľom vo vlastnom mene a na vlastnú zodpovednosť za účelom dosiahnutia zisku, čo nemusí v prípade vodičov využívajúcich aplikáciu spoločnosti Uber vždy bezvýhradne platiť. Je teoreticky možné, že aj sám vodič teda bude spotrebiteľom služieb spoločnosti Uber, a nie jej obchodným partnerom. Z hľadiska spotrebiteľského práva môže byť tiež otáznym, či Uber vo svojich zmluvných podmienkach neobsahuje vo vzťahu k spotrebiteľom (vodičom, zákazníkom vodičov) neprijateľné zmluvné podmienky – tejto problematike sme sa však v tomto príspevku bližšie nevenovali.

Z hľadiska súťažného práva sa ďalej Uberu vyčíta napríklad klamlivá reklama (tým, že poskytuje nepravdivé informácie o povahe svojich služieb a ich obsahu – napr. že vodiči majú koncesie poskytovateľov taxislužieb a pod.) a zneužívanie postavenia na trhu (nanucovanie poskytovania zliav koncovým zákazníkom podľa pokynov spoločnosti Uber).

V otázke zodpovednostných vzťahov sme upozornili na skutočnosť, že pokiaľ Uber vyberá a preveruje vodičov, ktorí využívajú aplikáciu Uber, prekračuje tým podľa nášho názoru „bezpečný prístav“ spoločnosti poskytujúcej služby informačnej spoločnosti (t.j. iba služby komunikácie medzi vodičom a zákazníkom, ako to inak o sebe tvrdí Uber, ale aj obdobná spoločnosť Lyft), a potenciálne na seba preberá zodpovednosť za kvalitu a obsah služieb poskytnutých vodičmi.

Napokon, v otázke povinnosti vodičov využívajúcich aplikáciu spoločnosti Uber dodržiavať podmienky kladené na taxislužby zákonom o cestnej doprave máme za to, že povinnosť získať koncesiu a spravovať sa pravidlami platnými pre taxislužby sa nevzťahuje na prípady, ak ide o cestnú dopravu pre vlastnú potrebu v zmysle nariadenia č. 1073/2009 – teda ak vodič svojím vlastným automobilom zvezie inú osobu iba ako svoju vedľajšiu činnosť, a nekoná tak za účelom zisku, resp. za účelom výkonu podnikania, ale iba napr. za účelom zdieľania nákladov na konkrétnu jazdu – čo mohol byť zrejme pôvodný zámer spoločnosti Uber. To však samozrejme neplatí, ak u vodiča ide v skutočnosti o sústavný výkon podnikateľskej činnosti za účelom zisku.

Záverom ešte musíme upozorniť na skutočnosť, že viaceré z naznačených otázok môžu v blízkej budúcnosti rýchlo stratiť relevanciu, resp. objavia sa nové právne otázky, ktoré sme v tomto príspevku neriešili – a to najmä v súvislosti s aktuálnym testovaním automobilov bez vodičov, ktoré by mohli nahradiť doterajšie zdieľanie jazdy a skôr sa priblížiť k poskytovaniu osobitného druhu taxislužby bez vodičov, čo si zrejme opäť vyžiada osobitnú právnu úpravu.[37]

[37] KHAN, F.: The “uberization” of healthcare: the forthcoming legal storm over mobile health technology’s impact on the medical profession, s. 8. Dostupné na internete: http://works.bepress.com/fazal_khan/7/ (navštívené dňa 7. 10. 2015).

Použitá literatúra:

DAVIS, J.: Drive at your own risk: Uber violates unfair competition laws by misleading UberX drivers about their insurance coverage. In: Boston College Law Review, Vol. 56, 2015.
HALTOM, B.: Your Uber Attorney Is 2 Minutes Away. In: Tennessee Bar Journal, august 2015.
FRIEDHOFF, S.: Insurance Could Make Road Bumpy for Uber and Lyft. In: BOSton GLOBE, 7. januára 2015. Dostupné na internete: http://www.bostonglobe.com/business/2015/01/07/insurance-questions-latest-bump-road-for-ride-share-companies/wegXpHUBpZHwtUXNHJSf6H/.html, a na: http://perma.cc/MRF4-YK5T (navštívené dňa 7. 10. 2015).
HUET, E.: What Happens to Uber Drivers and Other Sharing Economy Workers Injured on the Job? In: *Forbes*, 6. januára 2015. Dostupné na internete: http://www.forbes.com/sites/ellenhuet/2015/01/06/workers-compensation-uber-drivers-sharing-economy/ (navštívené dňa 7. 10. 2015).
KHAN, F.: The "uberization" of healthcare: the forthcoming legal storm over mobile health technology's impact on the medical profession. Dostupné na internete: http://works.bepress.com/fazal_khan/7/ (navštívené dňa 7. 10. 2015).
LOPEZ, A.: Prices Slashed for UberX as Opposition Raise Questions Over Safety. In: *NBC Los Angeles*. Dostupné na internete: http://www.nbclosangeles.com/news/local/UberX-Cuts-Prices-as-Opposition-Raises-Questions-Over-Safety-264278051.html, a na: http://perma.cc/W2ZY-VHB3 (navštívené dňa 7. 10. 2015).
MANJOO, F.: Uber, a Rising Business Model That Could Change How You Work. In: New York Times, 28. januára 2015. Dostupné na internete: http://www.nytimes.com/2015/01/29/technology/personaltech/uber-a-rising-business-model.html, a na: http://perma.cc/GJ8L-7V5V (navštívené dňa 7. 10. 2015).
WARD, S. F.: 'App' Me a Ride: Internet car companies offer convenience, but lawyers see caution signs. In: ABA Journal, január 2014.

Kontaktné údaje:

doc. JUDr. PhDr. Tomáš Gábriš, PhD., LL.M., MA
tomas.gabris@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovenská republika

Mgr. Ing. Jakub Jošt
jakub.jost@gmail.com
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovenská republika

REFORMA PRAVIDIEL OCHRANY ÚDAJOV V EURÓPSKEJ ÚNII

Daniela Ježová

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The three main EU institutions, the European Parliament, the Council and the European Commission, started on 24 June 2015 negotiations under the co-decision procedure on the proposed general regulation on data protection, which is known as the informal "trialogue". The basis for this trialogue is the Commission proposal of January 2012, legislative resolution of 12 March 2014 and the Council's general approach adopted on 15 June 2015. The three institutions are committed to deal with Regulation GDPR within a broader reform package on data protection, which includes a proposed Directive on police and judicial activities. This process should be completed by the end of 2015 and under him by the formal adoption of the two instruments could occur early in 2016, after which should be followed by a two-year transitional period.

Abstrakt: 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“. 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 . Tieto tri inštitúcie sa zaviazali zaoberať sa nariadením GDPR v rámci širšieho reformného balíka pre ochranu údajov, ktorý zahŕňa navrhovanú smernicu o policajných a justičných činnostiach. Tento proces by mal byť ukončený koncom roka 2015 a na základe neho by k formálnemu prijatiu oboch nástrojov mohlo dôjsť začiatkom roku 2016, po ktorom by malo nasledovať dvojročné prechodné obdobie.

Key words: protection of personal data, Europe 2020, general directive on data protection, general regulation on data protection.

Kľúčové slová: Ochrana osobných údajov, reforma 2015, Europa 2020, všeobecné nariadenia o ochrane osobných údajov, smernica o všeobecnej ochrane údajov.

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 (ďalej len „nariadenie GDPR“), 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 nariadením GDPR v rámci širšieho reformného balíka pre ochranu údajov, ktorý zahŕňa navrhovanú smernicu o policajných a justičných činnostiach. Tento proces by mal byť ukončený koncom roka 2015 a na základe neho by k formálnemu prijatiu oboch nástrojov mohlo dôjsť začiatkom roku 2016, po ktorom by malo nasledovať dvojročné prechodné obdobie.

[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.

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[3] sa stratégiou Európa 2020[4] 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.

V predstavách Komisie má reforma znamenať väčšiu kontrolu občanov nad osobnými údajmi. Posilniť by sa malo právo byť zabudnutý aj upozornenia o zneužití dát. Jednotná legislatíva prinesie úspory, menej byrokracie a zároveň prísnejšie tresty za priestupky.

Osobné údaje sú všetky údaje týkajúce sa jednotlivca, jeho osobného, pracovného alebo verejného života. Môže ísť o akékoľvek informácie – meno, fotografiu, emailovú adresu, bankové spojenie, príspevky na sociálnych sieťach, zdravotné informácie alebo IP adresu počítača. V digitálnom veku má zhromažďovanie a uchovávanie osobných údajov veľký význam. Údaje používajú všetky podniky – od poisťovní a bánk až po sociálne médiá a vyhľadávače. V globalizovanom svete sa prenos údajov do tretích krajín stal dôležitým faktorom každodenného života. V online prostredí neexistujú hranice a „cloud computing“ zmenil pohľad na miesto uchovávania údajov. Preto zhromažďovanie, analýza, výmena a zneužívanie údajov a riziko „profilovania“ podnietené technickým vývojom dosiahli nebývalé rozmery a vyžadujú prísne pravidlá na ochranu údajov, ako sú rozhodné právo a vymedzenie zodpovedností všetkých zainteresovaných strán, pokiaľ ide o vykonávanie právnych predpisov EÚ v oblasti ochrany údajov.

Nový právny základ stanovený v článku 16 ZFEÚ a skutočnosť, že v článku 8 Charty základných práv[5], 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.

Európska rada vyzvala Komisiu, aby zhodnotila fungovanie nástrojov EÚ v oblasti ochrany údajov a v prípade potreby predstavila ďalšie legislatívne a nelegislatívne iniciatívy[6]. Európsky

[3] 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“.

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

[5] „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.

[6] „Štokholmský program — otvorená a bezpečná Európa, ktorá slúži občanom a chráni ich“, Ú. v. EÚ C 115, 4.5.2010, s. 1.

parlament vo svojej rezolúcii[7] o Štokholmskom programe uvítal komplexný systém ochrany údajov v EÚ a okrem iného vyzval k revízii rámcového rozhodnutia. Komisia vo svojom akčnom pláne na implementáciu Štokholmského programu[8] zdôraznila potrebu zabezpečiť, aby sa základné právo na ochranu osobných údajov uplatňovalo v kontexte politík EÚ konzistentne. Vo svojom oznámení „Komplexný prístup k ochrane osobných údajov v Európskej únii“[9] Komisia dospela k záveru, že EÚ potrebuje komplexnejšiu a konzistentnú politiku, pokiaľ ide o základné právo na ochranu osobných údajov. Podľa tohto oznámenia, Komisia predniesla návrh na reformu ochrany údajov v januári 2012. Európsky parlament prijal v júli 2012 uznesenie[10] týkajúce sa tejto reformy.

2 SÚČASNÁ PRÁVNA ÚPRAVA OCHRANY OSOBNÝCH ÚDAJOV

V súčasnosti pôsobia v Európe dva právne systémy – právne nástroje prijaté na pôde Rady Európy (ďalej len „RE“) – Dohovor č. 108 a na pôde Európskej únie – aktuálne platná Smernica Európskeho parlamentu a Rady 95/46/EC z 24.10.1995 (ďalej len „Smernica z roku 1995“). Je potrebné si uvedomiť, že všetky členské štáty EÚ sú viazané oboma právnymi reguláciami, keď vezmeme do úvahy skutočnosť, že Rada Európy má ku dnešnému dňu 47 členských štátov a z nich 28 sú členovia EÚ. Rovnako esenciálna je aj judikatúra najvyšších orgánov oboch právnych systémov – Európskeho súdu pre ľudské práva (ďalej len „ESĽP“) a Súdneho dvora EÚ (ďalej len „SDEÚ“). V nasledujúcej časti priblížime najvýznamnejšie prvky oboch právnych úprav.[11]

Hlavný právny predpis EÚ týkajúci sa ochrany osobných údajov, smernica 95/46/ES3, bol prijatý v roku 1995 a jeho úlohou bolo dosiahnuť dva ciele – chrániť základné právo na ochranu údajov a zaručiť voľný tok osobných údajov medzi členskými štátmi. Smernicu doplnilo rámcové rozhodnutie 2008/977/SVV ako všeobecný nástroj na úrovni Únie určený na ochranu osobných údajov v oblastiach policajnej a justičnej spolupráce v trestných veciach[12].

Územné uplatňovanie smernice prekračuje hranice členských štátov EÚ a zahŕňa aj štáty, ktoré nie sú členskými štátmi EÚ, ale patria do Európskeho hospodárskeho priestoru, a to Island, Lichtenštajnsko a Nórsko. Dôležitou výnimkou z uplatňovania smernice o ochrane údajov je tzv. výnimka pre domáce činnosti, konkrétne pre spracúvanie osobných údajov súkromnými osobami na výlučne osobné účely alebo účely domácnosti[13].

Keďže smernica o ochrane údajov je určená len pre členské štáty EÚ, bolo potrebné prijať ďalší právny nástroj s cieľom stanoviť ochranu údajov pri spracovaní osobných údajov inštitúciami a orgánmi EÚ.[14] Nariadenie č. 45/2001 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov stanovuje rovnaké pravidlá a obmedzenia na úrovni inštitúcií EÚ a orgánov. Tiež zakladá úrad Európskeho dozorného úradníka pre ochranu údajov, nezávislý orgán dohľadu s úlohou zabezpečenia dodržiavania Smernice.[15]

Ďalším špecifickým právnym nástrojom je Smernica 2002/58/EC týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a

---

[7] Uznesenie Európskeho parlamentu o oznámení Komisie Európskemu parlamentu a Rade – Priestor slobody, bezpečnosti a spravodlivosti pre občanov – Štokholmský program, ktoré bolo prijaté 25. novembra 2009 (P7_TA(2009)0090).

[8] KOM(2010) 171 v konečnom znení

[9] KOM(2010) 609 v konečnom znení

[10] Uznesenie Európskeho parlamentu zo 6. júla 2011 o komplexnom prístupe k ochrane osobných údajov v Európskej únii (2011/2025(INI))

[11] Agentúra Európskej únie pre základné práva, Európsky súd pre ľudské práva – Rada Európy: Príručka o európskom práve v oblasti ochrany údajov. 2014. ISBN: ISBN 978-92-871-9937-9 (Rada Európy)ISBN 978-92-9239-340-3 (FRA), str.: 15.

[12] Rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach, Ú. v. EÚ L 350, 30.12.2008, s. 60 (rámcové rozhodnutie

[13] Smernica o ochrane údajov, článok 3 ods. 2 druhá zarážka.

[14] Agentúra Európskej únie pre základné práva, Európsky súd pre ľudské práva – Rada Európy: Príručka o európskom práve v oblasti ochrany údajov. 2014. ISBN: ISBN 978-92-871-9937-9 (Rada Európy)ISBN 978-92-9239-340-3 (FRA), str.: 19.

[15] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2

elektronických komunikáciách). Upravuje spracovávanie osobných údajov a ochranu súkromia v oblasti elektronických komunikácií a reguluje oblasti ako súkromie, fakturačné a prevádzkové údaje, pravidlá pre nevyžiadanú poštu, atď.

Rámcové rozhodnutie Rady 2008/977/SVV o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach je prvým všeobecným právnym rámcom pre ochranu údajov v „treťom pilieri" EÚ. Jeho obsah je taktiež založený na Dohovore č. 108, ale od Smernice z roku 1995 sa odlišuje v mnohých aspektoch, ktoré súvisia so špecifickou povahou subjektov.[16]

3 REFORMNÝ BALÍK

„Pred 17 rokmi používalo internet menej ako 1% Európanov. Dnes sa drvivá väčšina osobných údajov prenáša a vymieňa v rámci kontinentov a vôbec po svete v zlomku sekundy. Ochrana osobných údajov je základným právom všetkých Európanov. Nie vždy však občania majú pocit, že majú úplnú kontrolu nad svojimi údajmi. Moje návrhy pomôžu vybudovať dôveru v online služby, pretože ľudia budú lepšie informovaní o svojich právach a budú mať väčšiu kontrolu nad svojimi informáciami. Reforma pomôže dosiahnuť tento cieľ a súčasne uľahčí situáciu podnikov a zníži ich náklady. Silný, jasný a jednotný právny rámec na úrovni EÚ pomôže uvoľniť potenciál jednotného trhu s digitálnym obsahom a podporiť hospodársky rast, inovácie a tvorbu pracovných miest."[17] Takto sa dňa 25. januára 2012 vyjadrila podpredsedníčka Komisie a komisárka EÚ pre spravodlivosť Viviane Redingová, keď Európska komisia predložila návrh komplexnej reformy pravidiel ochrany údajov v EÚ v roku 1995 s cieľom posilniť právo na súkromie v online prostredí a podporiť digitálnu ekonomiku Európy.

Reforma zahŕňa dva legislatívne návrhy: 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**) a návrh 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 (**smernica o všeobecnej ochrane údajov**).

Hlavné prvky reformy sú: – ochrana údajov ako základné právo; – pokrytie všetkých typov situácií a odvetví, – technicky neutrálny právny rámec, ktorý zahŕňa rôzne postupy spracúvania údajov, – predchádzanie fragmentácii a poskytnutie právnej istoty jednotlivcom, podnikom a verejným subjektom, – zaistenie harmonizácie spracúvania osobných údajov zo strany orgánov presadzovania práva a výmena týchto údajov medzi nimi, – zaistenie ochrany jednotlivcov z EÚ v prípade, že sú osobné údaje zasielané do tretích krajín, a poskytnutie bezpečných a flexibilných nástrojov pre medzinárodný tok údajov.[18]

3.1 Všeobecné nariadenie o ochrane údajov

Jadrom balíka Komisie je všeobecné nariadenie o ochrane údajov. Tento návrh nariadenia[19] aktualizuje a modernizuje princípy smernice o ochrane údajov z roku 1995. Zakladá práva jednotlivcov a stanovuje povinnosti osôb spracúvajúcich a zodpovedných za spracúvanie údajov. Zároveň zavádza metódy pre zabezpečenie dodržiavania ako aj rozsah sankcií za porušenie pravidiel.

Návrh sa opiera o článok 16 ZFEÚ, ktorý je novým právnym základom pre prijatie pravidiel ochrany údajov zavedeným Lisabonskou zmluvou. Toto ustanovenie umožňuje prijať pravidlá týkajúce sa ochrany fyzických osôb, pokiaľ ide o spracúvanie osobných údajov zo strany členských štátov pri výkone činností, ktoré patria do rozsahu pôsobnosti práva Únie. Umožňuje aj prijatie pravidiel týkajúcich sa voľného pohybu osobných údajov vrátane osobných údajov spracovávaných členskými štátmi alebo súkromnými subjektmi. Nariadenie sa považuje za najvhodnejší právny

[16] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2

[17] Tlačová správa Európskej komisie z 25.01.2012 dostupná na http://europa.eu/rapid/press-release_IP-12-46_sk.htm (07.10.2015)

[18] Pozri pracovný dokument EP zo 6. júla 2012 o všeobecnom nariadení o ochrane údajov a smernici o spracúvaní osobných údajov príslušnými orgánmi za účelom prevencie, vyšetrovania, odhaľovania či stíhania trestných činov (PE491.322v01).

[19] COM(2012) 11 final

nástroj na vymedzenie rámca ochrany osobných údajov v Únii najmä vďaka priamemu uplatňovaniu nariadenia v súlade s článkom 288 ZFEÚ, čo zníži rozdielnosť právnych úprav.

Smernica prijatá v roku 1995 vytvorila pre EÚ plošne konzistentný súbor národných zákonov na ochranu údajov. Smernica síce stanovila hlavné zásady, ale v členských štátoch sa pri jej aplikácií uplatňujú rôzne prístupy. Explozívny nárast využívania sociálnych sietí a veľkých analýz údajov (okrem iného) stále viac evidentne preukazuje, že potreba nového prístupu k ochrane údajov je odôvodnená.

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. Napriek tomu to však stále ostávajú oblasti, v ktorých budú naďalej pretrvávať rozdiely medzi jednotlivými členskými štátmi. [20]

Právo na ochranu osobných údajov je stanovené v článku 8 charty, v článku 16 ZFEÚ a v článku 8 Európskeho dohovoru o základných právach. Ako zdôraznil Súdny dvor EÚ[21], právo na ochranu osobných údajov sa nejaví ako absolútne právo, ale musí sa zohľadniť so zreteľom na jeho funkciu v spoločnosti[22]. Ochrana údajov úzko súvisí s rešpektovaním súkromného a rodinného života, ktoré sú chránené článkom 7 charty.

Návrh nariadenia vychádza zo súčasne platnej smernice 95/46/ES ale zakotvuje aj nové prvky ako zásady transparentnosti (povinnosť pre prevádzkovateľov poskytnúť transparentné a ľahko dostupné a pochopiteľné informácie, pričom sa vychádza najmä z Madridskej rezolúcie o medzinárodných štandardoch o ochrane osobných údajov a súkromia[23]), spresnenie zásady obmedzenia spracovania údajov na nevyhnutné minimum a zavedenie komplexnej zodpovednosti a povinnosti pre prevádzkovateľa. Zásada transparentnosti si vyžaduje, aby všetky informácie určené verejnosti alebo dotknutej osobe boli ľahko prístupné a ľahko pochopiteľné a napísané jasne a jednoducho. Týka sa to najmä situácií, ako je online reklama, v ktorých veľký počet účastníkov a technologická komplexnosť sťažujú dotknutej osobe zistiť a pochopiť, či osobné údaje, ktoré sa jej týkajú, boli zhromaždené, kým a na aké účely. Keďže deťom prislúcha osobitná ochrana, všetky informácie a každá komunikácia, pri ktorej sa spracovanie zameriava osobitne na dieťa, by mali byť napísané jasne a jednoducho, aby ich dieťa mohlo jednoducho pochopiť.

Cieľom návrhu nariadenia je posilniť práva a poskytnúť jednotlivcom efektívne a funkčné prostriedky, ktoré zaistia, že budú plne informovaní o tom, čo sa s ich osobnými údajmi deje, a ktoré im umožnia účinnejší výkon ich práv. Pozitívum predstavuje aj posilnenie zodpovednosti tých, ktorí osobné údaje spracúvajú. Prevádzkovatelia tak budú musieť vykonávať operácie s osobnými údajmi dôslednejšie rešpektujúc právo fyzických osôb na súkromie.

---

[20] 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 (25.10.2015)

[21] Súdny dvor EÚ, rozsudok z 9.11.2010, spojené veci C-92/09 a C-93/09 Volker und Markus Schecke a Eifert, Zb. 2010, s. I-0000

[22] V súlade s článkom 52 ods. 1 charty je možné obmedziť výkon práva na ochranu údajov, ak je takéto obmedzenie ustanovené zákonom, rešpektuje podstatu práv a slobôd a za predpokladu dodržiavania zásady proporcionality je takéto obmedzenie nevyhnutné a skutočne zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných

[23] Rezolúcia bola prijatá na medzinárodnej konferencii komisárov pre ochranu údajov a súkromia, ktorá sa konala 5. novembra 2009. Pozri aj článok 13 ods. 3 návrhu nariadenia o spoločnom európskom kúpnom práve [KOM(2011) 635 v konečnom znení]

Zavádza právo dotknutej osoby na prenosnosť údajov, t. j. na prenesenie údajov z jedného systému elektronického spracovania do iného bez toho, aby jej v tom prevádzkovateľ bránil. Ako predpoklad uplatnenia tohto práva a s cieľom zlepšiť prístup fyzických osôb k ich osobným údajom sa tu stanovuje právo získať od prevádzkovateľa tieto údaje v štruktúrovanej forme a v bežne používanom elektronickom formáte.[24] Zjednoduší sa prenos údajov medzi jednotlivými prevádzkovateľmi. Budú stanovené spôsoby, ktoré dotknutej osobe uľahčia uplatnenie jej práv stanovených v tomto nariadení, vrátane mechanizmov pre vyžiadanie si bezplatného prístupu k údajom, ich opravu, výmaz a na uplatnenie práva namietať. Prevádzkovateľ by mal byť povinný odpovedať na žiadosť dotknutej osoby v stanovenej lehote a uviesť dôvody v prípade, že nemôže vyhovieť žiadosti dotknutej osoby. Rovnako ustanovuje povinnosť pre prevádzkovateľov poskytnúť transparentnú a ľahko dostupnú informáciu subjektom údajov o ich spracúvaných údajoch.

Základnými princípmi v pravidlách ochrany údajov EÚ sa stanú aj „Ochrana údajov by design" a „Ochrana údajov by default" – znamená to, že ochranné záruky majú byť začlenené do produktov a služieb od najzákladnejších stupňov vývoja a základné nastavenia rešpektujúce súkromie majú byť štandardom – napr. na sociálnych sieťach alebo v mobilných aplikáciách.[25]

V článku 22 sa zohľadňuje diskusia o „zásade zodpovednosti" a podrobne sa tu opisuje zodpovednosť a povinnosť prevádzkovateľa dodržiavať ustanovenia tohto nariadenia a preukázať dosiahnutie súladu, a to aj prostredníctvom prijatia interných pravidiel a mechanizmov na zabezpečenie takéhoto súladu.

Zavádza sa povinnosť pre prevádzkovateľov a sprostredkovateľov vykonávať posúdenie vplyvu na ochranu údajov pred vykonávaním operácií spracovania spojených s rizikami. Ďalej sa zavádza povinnosť určiť úradníka pre ochranu údajov pre verejný sektor a v prípade súkromného sektora pre veľké podniky, alebo ak hlavné činnosti prevádzkovateľa alebo sprostredkovateľa pozostávajú z operácií spracovania, ktoré si vyžadujú pravidelné a systematické monitorovanie.[26]

Návrh potvrdzuje už existujúcu povinnosť členských štátov zriadiť nezávislý orgán dohľadu na národnej úrovni. Zároveň sa snaží o zavedenie mechanizmu pre vytvorenie jednotnosti v aplikácii práva ochrany údajov v EÚ. Komisia obzvlášť navrhuje v prípade, že sa spracovanie osobných údajov vykonáva vo viac ako jednom členskom štáte, ustanoviť jeden kompetentný dohľadný orgán pre kontrolu všetkých týchto činností. Tento princíp, známy ako one-stop-shop, znamená, že v každom prípade bude príslušným orgánom orgán členského štátu, v ktorom má prevádzkovateľ alebo sprostredkovateľ miesto hlavnej činnosti.

Zároveň návrh Komisie zahŕňa zriadenie Európskeho výboru pre ochranu údajov. Tento bude pozostávať z vedúcich predstaviteľov dozorných orgánov z jednotlivých členských štátov členského štátu a európskeho dozorného úradníka pre ochranu údajov. pozostávať zo zástupcov všetkých 28 nezávislých dozorných orgánov a nahradí pracovnú skupinu pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov, ustanovenú článkom 29 smernice 95/46/ES.

„Ochrana údajov bude tak významná, ako protimonopolizácia v intenciách compliance rizika. Podľa Nariadenia ochrana údajov už nebude oblasťou, kde by si podniky mohli dovoliť neuvážene riskovať."[27]

Pri pohybe osobných údajov za hranice sa môže zvýšiť riziko z hľadiska možnosti fyzických osôb uplatniť práva ochrany údajov, a to najmä pokiaľ ide o ich schopnosť chrániť sa pred nezákonným využitím alebo zverejnením týchto informácií. Návrh tiež zahŕňa úpravu prenosu osobných údajov do tretích krajín a medzinárodných organizácií. V tejto oblasti dostáva Komisia oprávnenia hodnotiť úroveň ochrany poskytovanú územným alebo sprostredkujúcim sektorom v tretej krajine. V prípadoch, kde Komisia neprijala rozhodnutie o primeranosti územia alebo sektora, môže sa prenos osobných údajov uskutočniť v určitých prípadoch alebo keď sú poskytnuté

[24] Čl. 18 a nasl. Návrhu nariadenia

[25] European Commission Facts sheet. Memo/15/5170

[26] Tento článok vychádza z článku 18 ods. 2 smernice 95/46/ES, v ktorom bola stanovená možnosť pre členské štáty zaviesť takúto požiadavku namiesto všeobecnej oznamovacej povinnosti.

[27] 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 (25.10.2015)

náležité záruky (štandardné ustanovenia o ochrane údajov, záväzné korporátne pravidlá, zmluvné doložky).

Návrh priznáva právo dotknutých osôb podať žalobu dozornému orgánu ako aj ich právo na súdny prostriedok nápravy, odškodnenie a vyvodenie zodpovednosti. Zavádza veľmi prísne sankcie pre prevádzkovateľov a sprostredkovateľov, ktorí porušia pravidlá ochrany údajov.[28]

3.2 Aktuálny stav nariadenia

O Nariadení naďalej prebiehajú rokovania. Stále ostáva iba vo forme návrhu a rokujú legislatívne orgány EÚ a členských štátov. Aktuálne hlavné návrhy sú:

- Znenie Komisie: Komisia zverejnila prvý návrh Nariadenia 25. januára 2012
- Znenie Parlamentu: Dňa 12. marca 2014 prijal Parlament súbor navrhovaných dodatkov k návrhu Komisie
- Znenie Rady: Rada zverejnila kompromisný návrh spolu s návrhmi ďalších kapitol Nariadenia. Konečné znenie Rady sa očakáva v roku 2015.

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“. Základ pre trialóg predstavuje návrh Komisie z 25. januára 2012, legislatívne uznesenie Parlamentu z 12. marca 2014 a všeobecný prístup Rady prijatý 15. júna 2015. Zavŕšenie procesu rokovania sa predpokladá koncom roka 2015 a na jeho základe by k formálnemu prijatiu oboch nástrojov mohlo dôjsť začiatkom roku 2016, nasledované prechodným obdobím dvoch rokov.[29]

3.3 Smernica o ochrane osobných údajov spracúvaných za účelom vymáhania práva

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. Navrhovaná smernica sa zameriava na ochranu práv jednotlivcov na ochranu ich osobných údajov za súčasnej garancie vysokej úrovne verejnej bezpečnosti. Tento návrh sa aplikuje na cezhraničné i národné spracúvanie údajov kompetentnými orgánmi členských štátov za účelom vymáhania práva. Nepokrýva činnosti vykonávané inštitúciami, orgánmi, úradmi alebo agentúrami EÚ, rovnako ako ani činnosti spadajúce mimo rámca únijného práva.[30]

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.[31]

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.[32]

Medzi princípmi návrh smernice stanovuje, že členské štáty musia zabezpečiť, aby osobné údaje boli spracúvané zákonne, zhromažďované na určité, presne vymedzené a legitímne účely, a nesmú prekračovať hranice účelu, na ktorý sú spracúvané. Aj keď zahŕňa povinnosti členských

[28] Dostupné na: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/. (10.09.2015).

[29] European Data Protection Supervisor: Stanovisko 3/2015. Str. 2.

[30] Dostupné na: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/. (10.09.2015) .

[31] 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.

[32] 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.

štátov poskytnúť zrozumiteľnú informáciu a zabezpečiť jednotlivcovo právo na prístup, taktiež stanovuje obmedzenia, ktoré umožňujú členským štátom prijať právne opatrenia obmedzujúce právo na prístup.

Popisuje zodpovednosť kontrolóra, vrátane prvkov zo všeobecného nariadenia o ochrane údajov ako napr. poskytnúť oznámenie o porušení a vymenovanie úradníka pre ochranu údajov (data protection officer). Prenos do tretej krajiny sa môže uskutočniť, iba ak je to potrebné na účely vymáhania práva a ak Komisia prijala rozhodnutie o vhodnosti úrovne ochrany, ktorú poskytuje táto krajina. Pokiaľ neexistuje rozhodnutie o vhodnosti, prenos údajov sa môže uskutočniť na základe dostatočných záruk. Navyše je k týmto možnostiam predpokladané ustanovenie pre osobitné účely. Dohliadajúce orgány môžu byť tie isté, ako tie zriadené podľa nariadenia o ochrane údajov.

Zavádza pravidlá o povinnej vzájomnej pomoci a všeobecnú povinnosť spolupracovať. Zároveň stanovuje, že Európska poradná rada pre ochranu údajov (the European Data Protection Advisory Board) môže tiež plniť svoje úlohy pre vykonávanie činností zahrnutých v tejto smernici.[33]

Diskusie o návrhu smernice sa uskutočňujú v Pracovnej skupine pre výmenu informácií a ochranu údajov (DAPIX).

4 OCHRANA OSOBNÝCH ÚDAJOV MEDZI EÚ A USA VO SVETLE NAJNOVŠIEHO ROZHONDUTIA SD EÚ

Dňa 6.10.2015 Súdny dvor EÚ rozhodol v právnej veci C-362/14 Maximillian Schrems proti Data Protection Commissioner (komisár pre ochranu údajov). Návrh na začatie prejudiciálneho konania sa týka výkladu článku 25 ods. 6 a článku 28 smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov z hľadiska článkov 7, 8 a 47 Charty základných práv Európskej únie ako aj v podstate platnosti rozhodnutia Komisie 2000/520/ES[34] z 26. júla 2000 v súlade so smernicou 95/46 o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA. Išlo o vec jeho odmietnutia vyšetriť sťažnosť podanú pánom Schremsom z dôvodu, že Facebook Ireland Ltd zasiela do Spojených štátov osobné údaje svojich používateľov a uchováva ich na serveroch umiestnených v tejto krajine. Pán Schrems v tejto súvislosti odkazoval na odhalenia pána Edwarda Snowdena týkajúce sa činností informačných služieb Spojených štátov, najmä National Security Agency (ďalej len „NSA“).

Súdny dvor vyhlásil rozhodnutie Komisie 2000/520/ES[35], ktoré konštatuje, že Spojené štáty zaisťujú preneseným osobným údajom primeranú úroveň ochrany, za neplatné. Otázka Vyššieho súdu Írska smeruje k tomu, či rozhodnutie Komisie 2000/520/ES bráni tomu, aby vnútroštátny dozorný orgán preskúmal sťažnosť, v ktorej sa uvádza, že tretia krajina nezaisťuje primeranú úroveň ochrany, a prípadne zastavil spochybnený prenos údajov. Súdny dvor konštatuje, že existencia rozhodnutia Komisie, ktoré konštatuje, že tretia krajina zaisťuje preneseným osobným údajom primeranú úroveň ochrany, nemôže vylúčiť ani obmedziť právomoci, ktorými disponujú vnútroštátne dozorné orgány podľa Charty základných práv Európskej únie a smernice. žiadne ustanovenie smernice nebráni vnútroštátnym orgánom kontrolovať prenosy osobných údajov do tretích krajín, ktoré boli predmetom rozhodnutia Komisie. Takto aj v prípade existencie rozhodnutia Komisie vnútroštátne dozorné orgány, na ktoré sa podala žiadosť, musia mať možnosť nezávisle preskúmať, či prenos údajov osoby do tretej krajiny spĺňa požiadavky stanovené smernicou. Zatiaľ čo Súdny dvor má jediný právomoc vyhlásiť neplatnosť aktu Únie, vnútroštátne dozorné orgány, na ktoré bola podaná žiadosť, môžu aj pri existencii rozhodnutia Komisie, ktoré konštatuje, že tretia krajina poskytuje primeranú úroveň ochrany osobných údajov, preskúmať, či prenos údajov osoby do tejto krajiny dodržiava požiadavky právnej úpravy Únie týkajúcej sa ochrany týchto údajov, ako aj obrátiť sa na vnútroštátne súdy z rovnakého titulu ako dotknutá osoba, aby tieto súdy podali návrh na začatie prejudiciálneho konania s cieľom preskúmať platnosť tohto rozhodnutia.[36]

[33] Dostupné na: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/. Navštívené: 2015-09-14.

[34] Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou 95/46 o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA (Ú. v. ES L 215, s. 7; Mim. vyd. 16/001, s. 119).

[35] Rozhodnutie 2000/520 prijala Komisia na základe článku 25 ods. 6 smernice 95/46

[36] Tlačové komuniké SD EÚ č. 117/15

Komisia mala povinnosť konštatovať, že Spojené štáty skutočne zaisťujú z dôvodu svojho vnútroštátneho práva alebo medzinárodných dohôd, ktoré podpísali, úroveň ochrany základných práv, ktorá je v podstate rovnocenná úrovni zaručenej v rámci Únie podľa smernice v spojení s Chartou, pričom Komisia takéto konštatovanie nevykonala, ale preskúmala len režim bezpečného prístavu. Režim sa uplatňuje iba na americké podniky, ktoré k nemu pristúpia, pričom samotné orgány verejnej moci Spojených štátov mu nepodliehajú. Požiadavky týkajúce sa národnej bezpečnosti, verejného záujmu alebo vymáhania práva Spojených štátov majú prednosť pred režimom bezpečného prístavu a americké podniky sú povinné bez akéhokoľvek obmedzenia neuplatniť pravidlá ochrany stanovené týmto režimom, ak sú v rozpore s takýmito požiadavkami. Americký režim bezpečného prístavu tak umožňuje zásahy zo strany amerických orgánov verejnej moci do základných práv osôb, pričom rozhodnutie Komisie neobsahuje nijaké ustanovenie, čo sa týka existencie pravidiel, ktorých cieľom by bolo obmedzenie týchto prípadných zásahov, v Spojených štátoch alebo existencie účinnej právnej ochrany proti týmto zásahom.

Existujú dve oznámenia Komisie[37], z ktorých možno vyvodiť, že orgány Spojených štátov mali prístup k osobným údajom preneseným z členských štátov do tejto krajiny a mohli ich spracovať spôsobom nezlučiteľným najmä s účelom ich prenosu a nad rámec toho, čo bolo prísne nevyhnutné a primerané vzhľadom na národnú bezpečnosť. Rovnako Komisia konštatovala, že pre dotknuté osoby neexistovali správne alebo súdne prostriedky nápravy umožňujúce najmä prístup k údajom, ktoré sa ich týkajú, a prípadne dosiahnuť ich opravu alebo ich vymazanie. [38]

Súdny dvor rovnako uvádza, že právna úprava, ktorá neupravuje nijakú možnosť osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov, zasahuje podstatu obsahu základného práva na účinnú súdnu ochranu, pričom takáto možnosť je súčasťou existencie právneho štátu.

Tento rozsudok má za následok, že írsky dozorný orgán je povinný preskúmať sťažnosť pána Schremsa so všetkou náležitou starostlivosťou, ktorá sa vyžaduje, a že je jeho úlohou po skončení svojho vyšetrovania rozhodnúť, či je podľa smernice potrebné zastaviť prenos údajov európskych používateľov Facebooku do Spojených štátov z dôvodu, že táto krajina nezaisťuje primeranú úroveň ochrany osobných údajov.

Safe Harbour predstavoval najjednoduchšiu cestu pre americké spoločnosti, ako legálne importovať osobné údaje z EÚ, ale nikdy sa nejednalo o jedinú cestou. Čo sa stane teraz, je, že tieto spoločnosti budú musieť použiť iné mechanizmy na prenos osobných údajov. Jedným z možných spôsobov sú známe "vzorové zmluvy doložiek" alebo štandardizované obchodné podmienky. Uvedené rozhodnutie prišlo v čase prípravy reforiem nového režimu Safe Harbour, Umbrella Agreement a reformného balíka týkajúceho sa ochrany údajov v EÚ.

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 navrhovanej legislatívy EÚ, ktorý bude v dohľadnej dobe prijatý, nie je ani zďaleka konečným cieľom. Predpokladaným prínosom reformy by malo byť najmä zharmonizovanie pravidiel a vytvorenie konzistentnej a efektívnej cesty k zakotveniu pevných štandardov ochrany údajov v Európe. Ako uznávajú inštitúcie EÚ, dôvera občanov je dôležitou podmienkou pre nové produkty a služby, ktoré sú spojené so spracúvaním osobných údajov. V dnešnej dobe je táto dôvera ľudí značne narušená, ako to potvrdili aj výsledky nedávneho prieskumu Eurobarometer[39], na základe

[37] Oznámenie Komisie Európskemu parlamentu a Rade nazvané „Obnovenie dôvery v toky údajov medzi EÚ a USA“ [COM(2013) 846 final, 27. november 2013] a oznámenie Komisie Európskemu parlamentu a Rade o fungovaní systému bezpečného prístavu z pohľadu občanov EÚ a spoločností usadených v EÚ [COM(2013) 847 final, 27. november 2013].

[38] Tlačové komuniké SD EÚ č. 117/15

[39] http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm zhliadnuté 07.10.2015

ktorého 8 z 10 opýtaných potvrdilo, že nemajú pocit úplnej kontroly nad svojimi údajmi. Ostáva teda veriť, že reforma prinesie očakávané výsledky a odstráni tento stav neistoty.

Použitá literatúra:

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).
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),
Európa 2020 – Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu (COM(2010)2020)
Štokholmský program — otvorená a bezpečná Európa, ktorá slúži občanom a chráni ich“, Ú. v. EÚ C 115, 4.5.2010, s. 1
Uznesenie Európskeho parlamentu o oznámení Komisie Európskemu parlamentu a Rade – Priestor slobody, bezpečnosti a spravodlivosti pre občanov – Štokholmský program, ktoré bolo prijaté 25. novembra 2009 (P7_TA(2009)0090).
COM(2010) 171 v konečnom znení
COM(2010) 609 v konečnom znení
Uznesenie Európskeho parlamentu zo 6. júla 2011 o komplexnom prístupe k ochrane osobných údajov v Európskej únii (2011/2025(INI))
Agentúra Európskej únie pre základné práva, Európsky súd pre ľudské práva – Rada Európy: Príručka o európskom práve v oblasti ochrany údajov. 2014. ISBN: ISBN 978-92-871-9937-9 (Rada Európy)ISBN 978-92-9239-340-3 (FRA), str.: 15.
Rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach, Ú. v. EÚ L 350, 30.12.2008, s. 60 (rámcové rozhodnutie
COM(2012) 11 final
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
Súdny dvor EÚ, rozsudok z 9.11.2010, spojené veci C-92/09 a C-93/09 Volker und Markus Schecke a Eifert, Zb. 2010, s. I-0000
European Commission Facts sheet. Memo/15/5170
Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou 95/46 o primeranosti ochrany poskytovanej zásadami bezpečného prístavu a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA (Ú. v. ES L 215, s. 7; Mim. vyd. 16/001, s. 119).
Rozhodnutie 2000/520 prijala Komisia na základe článku 25 ods. 6 smernice 95/46
Tlačové komuniké SD EÚ č. 117/15
Oznámenie Komisie Európskemu parlamentu a Rade nazvané „Obnovenie dôvery v toky údajov medzi EÚ a USA“ [COM(2013) 846 final, 27. november 2013] a oznámenie Komisie Európskemu parlamentu a Rade o fungovaní systému bezpečného prístavu z pohľadu občanov EÚ a spoločností usadených v EÚ [COM(2013) 847 final, 27. november 2013].
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.

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

EŠTE RAZ K ROZHODNUTIU ESĽP VO VECI DELFI

Jakub Jošt, Tomáš Gábriš

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: In the contribution the authors will first pay attention to the interpretation of the Delfi award of the ECtHR by the media after the decision was announced, then they will address the award itself, and finally they will sum up their own interpretation of the importance of the award for news servers and for their liability for comments made by their readers.

Abstrakt: V príspevku najprv poukážeme na interpretáciu, ktorú ponúkli médiá bezprostredne po zverejnení rozhodnutia ESĽP vo veci Delfi, potom objasníme obsah vlastného rozhodnutia, a napokon zosumarizujeme naše vlastné závery k vplyvu alebo naopak irelevantnosti tohto rozhodnutia vo vzťahu k činnosti spravodajských serverov a ich zodpovednosti za komentáre čitateľov v diskusiách.

Key words: Delfi, liability, information society services, Internet

Kľúčové slová: Delfi, zodpovednosť, služby informačnej spoločnosti, internet

1 ÚVOD

Rozhodnutie Európskeho súdu pre ľudské práva (ďalej len „ESĽP“) vo veci Delfi vyvolalo mediálnu búrku nielen na Slovensku, ale v celej Európe. Závery, ku ktorým dospievali prvotné komentáre vykresľovali toto rozhodnutie ako koniec slobody prejavu v Európe, a predpovedali zánik internetových diskusií na spravodajských portáloch. Tieto vyjadrenia sme už v čase prvotných komentátorov považovali za prehnané, a rozhodnutie vo veci Delfi sme krátko po jeho zverejnení považovali za rozhodnutie vychádzajúce z osobitného právneho stavu platného v Estónsku, ako domovskom štáte tohto prípadu. V tomto príspevku zosumarizujeme naše postrehy k uvedenému rozhodnutiu, poukážeme na pozadie estónskeho právneho poriadku, ktoré považujeme pre konečné rozhodnutie za kľúčové, a tiež sa vyjadríme k možnému (a osobitne k želateľnému) dopadu, resp. významu tohto rozhodnutia pre poskytovanie služieb informačnej spoločnosti v Európe.

2 ROZHODNUTIE ESĽP VO VECI DELFI

Spoločnosť Delfi AS je akciová spoločnosť registrovaná v Estónsku. Je prevádzkovateľkou jedného z najväčších internetových spravodajských portálov v krajine, na ktorého webových stránkach v januári 2006 publikovala článok o prepravnej spoločnosti, ktorá zmenila trasu pre jej trajekty dopravujúce ľudí na niektoré ostrovy, následkom čoho sa lámal ľad tam, kde pod vplyvom mrazu mohli vzniknúť ľadové cesty, predstavujúce lacnejšie a rýchlejšie spojenie s ostrovmi v porovnaní s lodnou prepravou. Čitatelia mali pod týmto článkom možnosť príspevok voľne komentovať, k čomu ich aj portál priamo vyzýval. Mnoho čitateľov pridalo do diskusie urážlivé alebo výhražné príspevky na adresu prevádzkovateľa lodnej prepravy a majiteľa prepravnej spoločnosti.

Majiteľ trajektovej spoločnosti v apríli 2006 Delfi AS zažaloval. V júni 2008 estónske súdy rozhodli v jeho prospech, nakoľko mali za to, že komentáre boli urážlivé, a že Delfi AS za ne bola zodpovedná, nakoľko predstavuje obdobu vydavateľa printovej tlače a sama čitateľov vyzývala ku komentovaniu článkov na spravodajskom portáli. Majiteľovi prepravnej spoločnosti súd priznal 5 000 EEK (približne 320,- EUR) ako náhradu škody. Odvolanie spoločnosti Delfi AS v júni 2009 najvyšší súd zamietol. Delfi AS sa následne obrátila na ESĽP, s námietkou, že rozhodnutie estónskych súdov predstavuje porušenie práva na slobodu prejavu.

ESĽP však prostredníctvom svojej komory rozhodol, že to, že spoločnosť Delfi AS bola považovaná za zodpovednú za komentáre, bolo opodstatneným a primeraným zásahom do jej práva na slobodu prejavu, a nedošlo pritom k porušeniu čl. 10 Dohovoru Rady Európy o základných právach a ľudských slobodách z roku 1950. V zmysle čl. 43 a čl. 44 Dohovoru pritom nebol tento

rozsudok Komory ESĽP z 10. októbra 2013 ihneď právoplatný, nakoľko v lehote troch mesiacov odo dňa vynesenia rozsudku mohla ktorákoľvek zo strán požiadať o predloženie veci Veľkej komore ESĽP. Porota piatich sudcov pritom mala za to, že spoločnosťou Delfi AS podané odvolanie v tejto veci si vyžaduje ďalšie preskúmanie, a tak Veľká komora ESĽP prijala vec na ďalšie prerokovanie. [1]

Rozhodnutie Veľkej komory ESĽP zo 16. júna 2015 napokon potvrdilo rozhodnutie komory z 10. októbra 2013. To viedlo k početným reakciám ako právnikov, tak aj neprávnikov, najmä žurnalistov, a spravodajských portálov, ktorí vospolok toto rozhodnutie prezentovali ako útok na slobodu slova a na všetky spravodajské portály.

3 REAKCIE NA ROZHODNUTIE VEĽKEJ KOMORY

Rozhodnutie vo veci Delfi už po rozhodnutí komory z roku 2013 vyvolalo reakciu primárne u samotnej spoločnosti Delfi, vo vzťahu k ňou prevádzkovanému portálu. Delfi zamestnala tím administrátorov, ktorí dostali za úlohu prejsť všetkými anonymnými aj pseudonymnými komentármi. Iné estónske diskusné fóra, ktoré si nemohli dovoliť zamestnať administrátorov diskusií, jednoducho zrušili možnosť pridávať anonymné komentáre, čo sa prezentovalo ako koniec anonymného vyjadrovania názorov.[2]

Podobné nálady – o konci slobody prejavu – a o postihu diskusných fór a portálov poskytujúcich priestor pre diskusie, sa začali vzápätí po zverejnení rozhodnutia Veľkej komory z roku 2015 šíriť aj v slovenskom mediálnom priestore.

Problematickým z tohto pohľadu bol napríklad komentár v DenníkuN zo 16.6.2015, hoci odkazoval na blog v anglickom jazyku, v ktorom bolo rozhodnutie zhodnotené vyváženejšie:[3] „*Na Slovensku bola doposiaľ zaužívaná prax, že majitelia webov nenesú zodpovednosť za príspevky v diskusiách, kým na ne neboli upozornení. Ak ale dostali upozornenie a problematické komentáre neodstránili, mohli byť voči nim podstúpené právne kroky. Rozhodnutie súdu v Štrasburgu môže ale znamenať, že nesú zodpovednosť za všetky príspevky, aj za tie, o ktorých nevedia. Respektíve, že ak sa chcú vyhnúť právnym problémom, mali by nájsť kapacity na skontrolovanie každého príspevku, ktorý čitatelia pod článkami napíšu*.“[4]

Aj v tlačovej správe TASR zo 17. 6. 2015 v úvode agentúrnej správy nájdeme síce isté prehnané zovšeobecnenie, ktoré máme za nesprávne, nasledujúci odsek však túto správu uviedol na pravú mieru: „*Za urážlivé komentáre pod článkom na internetovej stránke je zodpovedný jej prevádzkovateľ, ktorý ich musí vymazať aj bez upozornenia dotknutej strany, ak obsahujú poburovanie a priame hrozby fyzickým útokom. Rozhodol o tom v utorok Európsky súd pre ľudské práva (ESĽP) v Štrasburgu, informovala agentúra DPA. Rozhodnutie ESĽP sa vzťahuje na konkrétny prípad a preto nemusí byť uvedeným spôsobom aplikované v krajinách s odlišnou legislatívou. Súd však tiež konštatoval, že sloboda prejavu nebude obmedzená, ak členské štáty*

[1] Sumarizácia prípadu podľa MAJERNÍK, T.: Rozsudok Komory z 10. októbra 2013 vo veci: Delfi AS proti Estónsku sťažnosť č. 64569/09. Dostupné na internete: portal.concourt.sk/download/attachments/17269496/ESLP25.pdf (navštívené dňa 7. 10. 2015). Celý text rozhodnutia je dostupný na internete: http://hudoc.echr.coe.int/eng?i=001-155105 (navštívené dňa 7. 10. 2015).

[2] MALCOLM, J.: European Web Host Ruled Liable for Users' Comments—Even Though It Didn't Read Them. Dostupné na internete: https://www.eff.org/deeplinks/2015/06/european-web-hosts-ruled-liable-users-comments-even-if-they-didnt-read-them (navštívené dňa 7. 10. 2015).

[3] WOODS, L.: The Delfi AS vs Estonia judgement explained. Dostupné na internete: http://blogs.lse.ac.uk/mediapolicyproject/2015/06/16/the-delfi-as-vs-estonia-judgement-explained/ (navštívené dňa 7. 10. 2015).

[4] Za urážky v internetových diskusiách sú zodpovední majitelia webov, rozhodol súd v Štrasburgu. Dostupné na internete: https://dennikn.sk/161792/za-urazky-v-internetovych-diskusiach-su-zodpovedni-majitelia-webov-rozhodol-sud-v-strasburgu/ (navštívené dňa 7. 10. 2015). Podobne: http://alianciazanedelu.sk/?p=5819 (navštívené dňa 7. 10. 2015) alebo http://www.omediach.com/internet/item/6887-za-urazlive-komentare-diskuterov-ma-niest-zodpovednost-web (navštívené dňa 7. 10. 2015).

Rady Európy budú od prevádzkovateľov internetových stránok vyžadovať odstránenie zjavne protiprávnych komentárov.“[5]

Napokon, veľmi triezvo k rozhodnutiu a jeho dopadu pristúpil portál „medialne“ v príspevku z 10.7.2015: „*Slovenské weby nie sú zodpovedné za urážky v diskusiách, kým ich na ne niekto neupozorní. Nič na tom zatiaľ nemení ani nedávny verdikt súdu v Štrasburgu, ktorý vydal odlišné stanovisko. Zhodujú sa právnici, ktorí sa špecializujú na právo informačných technológií a na médiá*.“[6] Zároveň citoval názor, podľa ktorého je poľutovaniahodné, že ESĽP akceptoval, že vnútroštátny právny poriadok môže zaviesť „*prípustnosť striktnej zodpovednosti medzičlánkov, respektíve prostredníkov spoločenskej diskusie, akým je aj jej novinársky iniciátor...*“.[7]

4 ROZHODNUTIE VEĽKEJ KOMORY A JEHO ODÔVODNENIE

Na tomto mieste sa pokúsime bližšie rozanalyzovať rozhodnutie Veľkej komory ESĽP a zaujať v rámci vyššie uvedeného diapazónu názorov a hodnotení tohto rozhodnutia vlastné stanovisko. Ako sme pritom už avizovali, zastávame skôr posledné citované stanovisko, ktoré je však až produktom istého časového odstupu od samotného rozhodnutia. Vo všeobecnosti totiž s rastúcim časovým odstupom od rozhodnutia jednotlivé stanoviská vykazujú triezvejší pohľad na vec. V našom príspevku nám je pritom dopriata výhoda až niekoľkých mesiacov odstupu, a preto aj naše stanoviská budú viac zdržanlivé a menej unáhlené ako mohli byť prvotné závery a reakcie.

V prvom rade máme za opomínané, že rozhodnutie Veľkej komory ESĽP zo 16. júna 2015[8] v odôvodnení poukázalo na to, že estónsky právny poriadok a judikatúra už od roku 2005 (pozri alineu 31 rozhodnutia Veľkej komory) vykladali definíciu zverejňovateľa, resp. vydavateľa ako osobu, ktorá zverejňuje informácie tretím osobám. Judikatúra pritom opakovane potvrdzovala, že vydavateľom je rovnako osoba, ktorá informáciu médiu poskytla na publikovanie, ako aj médium, ktoré informáciu zverejnilo. Elektronické médium je pritom podľa estónskej judikatúry považované za vydavateľa rovnako ako printové médium, a dokonca sa naň vzťahuje úprava platná pre printových vydavateľov, vrátane zodpovednosti vydavateľov – to primárne z dôvodu, že aj elektronické médium má rovnako ako printové médium ekonomický záujem na publikovaní čitateľských komentárov. Pokiaľ pritom takýto komentár obsahuje hanlivé informácie o tretej osobe, vydavateľom je ten, kto takýto komentár sprístupnil verejnosti, a to bez ohľadu na to, či šlo o elektronické alebo printové médium.

Estónske súdy teda odmietli Delfi (a obdobné spoločnosti prevádzkujúce elektronické spravodajské portály) podradiť pod právnu úpravu estónskeho zákona o službách informačnej spoločnosti a pod režim smernice o elektronickom obchode, a namiesto toho aplikovali ustanovenia estónskeho občianskeho zákonníka a zákona o záväzkovom práve. Preto súdy neuplatnili na Delfi podmienky tzv. bezpečného prístavu (*safe harbor*) podľa Smernice o elektronickom obchode, ktoré sa inak vzťahujú na poskytovateľov služieb informačnej spoločnosti v zmysle, že ak je poskytovateľ služby prevažne pasívnym a nemá vedomosť o protiprávnosti obsahu, za protipávnosť nezodpovedá.

Podľa aliney 42 rozhodnutia Veľkej komory, v Estónsku bolo v minulosti pred súdmi prejednaných viacero prípadov, kedy bola podaná žaloba na ochranu osobnostných práv proti autorovi článku, ako aj proti vydavateľovi média (novín), alebo len proti mediálnemu vydavateľovi. Podľa aliney 43 dokonca nižšie súdy vo viacerých prípadoch rozhodli o tom, že vydavateľ (prevádzkovateľ portálu) zodpovedá za komentáre k online článkom, čo potvrdili aj odvolacie súdy s tým, že im bolo zjavné, že prevádzkovateľ v týchto prípadoch nebol pasívnym poskytovateľom služby, a bol poskytovateľom obsahu (*content provider*). Súdy pritom poukazovali na to, že podľa

[5] Tlačová správa TASR. Prevratné rozhodnutie súdu: Za urážky pod článkom môže portál. Dostupné na internete: http://www.pluska.sk/spravy/zo-zahranicia/prevratne-rozhodnutie-sudu-za-urazky-pod-clankom-moze-portal.html (navštívené dňa 7. 10. 2015).

[6] PETKOVÁ, Z.: Ako môže kontroverzné rozhodnutie zlikvidovať (vulgárne) diskusie na webe. Dostupné na internete: http://medialne.etrend.sk/internet/ako-moze-kontroverzne-rozhodnutie-zlikvidovat-vulgarne-diskusie-na-webe.html (navštívené dňa 7. 10. 2015).

[7] Tamže.

[8] Dostupné na internete: http://hudoc.echr.coe.int/eng?i=001-155105 (navštívené dňa 7. 10. 2015).

rozhodnutia SD EÚ (*C-236/08 až C-238/08 Google France and Google*[9]) posúdenie, či poskytovateľ služby je aktívnym alebo pasívnym, je v rukách národných súdov.

Podľa aliney 53, v rozhodnutí *C-324/09 L'Oréal and Others*[10] síce SD EÚ potvrdil, že zodpovednosť poskytovateľa je vylúčená, ak nie je aktívnym do takej miery, ktorá mu umožňuje kontrolovať alebo dozvedieť sa o obsahu prenášaných alebo uložených informácií, jeho zodpovednosť však nie je vylúčená, ak nepostupoval tak, ako by mal opatrný poskytovateľ postupovať. Alinea 54 a 55 však pritom dodáva, že to neznamená, že je opodstatnené vyžadovať od poskytovateľov plošné preventívne filtrovanie obsahu prenášaných alebo ukladaných informácií (to konštatoval SD EÚ vo veci *C-360/10 SABAM*[11]).

Zásadne teda bola právna situácia v Estónsku taká, že veľkí vydavatelia, hoci šlo o elektronické portály, spadali pod všeobecnú úpravu zodpovednosti za porušenie osobnostných práv (príp. za inú škodu alebo ujmu) podľa občianskeho práva. Ak by sa však aj malo postupovať podľa smernice o elektronickom obchode, resp. podľa jej transpozície v osobitnom estónskom zákone, súdy v Estónsku judikovali, že takéto spoločnosti by boli zväčša aktívnymi poskytovateľmi, prípadne poskytovateľmi obsahu – nakoľko vyzývajú užívateľov, aby tento obsah sami tvorili. Ani v prípade ich podradenia pod služby informačnej spoločnosti teda estónske súdy nepripúšťali ich zbavenie sa zodpovednosti v zmysle ustanovení o bezpečnom prístave v smernici o elektronickom obchode.

Súd navyše v alinee 115 skonštatoval, že v tomto prípade šlo o veľký, profesionálne manažovaný portál, ktorý fungoval na komerčnej báze, a vyslovene vyzýval čitateľov, aby komentovali jednotlivé zverejnené články. Podľa aliney 116 pritom výslovne platí, že tento prípad sa nevzťahuje na iné internetové fóra, kde sa užívatelia vyjadrujú bez toho, aby ich k tomu prevádzkovateľ vyzýval, ani na diskusie v sociálnych médiách, kde samotné médium neposkytuje žiadny obsah, ktorý by mal byť komentovaný, a poskytovateľom obsahu (*content provider*) môže byť osoba, ktorá spravuje stránku alebo blog ako svoje hobby. Domáce právo teda rozlišuje medzi spravodajskými portálmi, ktoré sú aktívne a žijú z toho, že ľudia komentujú ich články, a inými prevádzkovateľmi, ktorí iba pasívne poskytujú priestor na diskusie tretích osôb.

Komora sa vysporiadala aj s argumentáciou právnych zástupcov spoločnosti Delfi, a v alinee 62 tak napríklad Komora odmietla tvrdenie spoločnosti Delfi AS, resp. jej právnych zástupcov, podľa ktorého obmedzenie slobody prejavu vydavateľov nebolo dané v Estónsku zákonom, ako sa to vyžaduje na legitímne a legálne obmedzenie základných práv. Podľa Komory však na splnenie podmienky zákonného obmedzenia základných práv postačuje, že národné súdy v Estónsku nepovažovali poskytovateľov za spadajúcich pod výnimku zo zodpovednosti v zmysle smernice EÚ o elektronickom obchode a príslušného estónskeho Zákona o službách informačnej spoločnosti. Komora odmietla posúdiť, resp. preskúmať príslušnú judikatúru národných súdov v tejto súvislosti, nakoľko táto úloha Komore neprísluší – uspokojila sa s tým, že národným súdom bolo zjavne zrejmé, že vydavateľ (médium) je zodpovedné za urážlivé výroky, ktoré publikovalo, a že spadá pod ustanovenia občianskeho zákonníka a zákona o záväzkoch.

5 KONFRONTÁCIA S PRÁVNOU ÚPRAVOU EÚ A JUDIKATÚROU SD EÚ

Ako už skonštatovala aj Komora v rozhodnutí Delfi, jej závery rovnako ako ani závery estónskych súdov nie sú protichodné so súvisiacou judikatúrou SD EÚ. Vo vzťahu k judikatúre SD EÚ pritom síce treba uviesť, že podľa niektorých názorov rozhodnutie ESĽP nabúrava princípy, na ktorých je postavená zodpovednosť poskytovateľov služieb informačnej spoločnosti – poskytovatelia by totiž mali byť vyňatí zo zodpovednosti, pokiaľ neovplyvňujú obsah, a zároveň v prípade upozornenia na protiprávny obsah tento bez zbytočného odkladu odstránia, komentátori však v tomto prípade správne upozorňujú na to, že smernica o elektronickom obchode nebráni tomu, aby estónsky právny poriadok zaviedol zodpovednosť poskytovateľov aj za protiprávny obsah, ktorý bol poskytovateľom po upozornení na jeho protiprávnosť následne odstránený.[12]

[9] http://curia.europa.eu/juris/liste.jsf?num=C-236/08 (navštívené dňa 7. 10. 2015).
[10] http://curia.europa.eu/juris/liste.jsf?num=C-324/09 (navštívené dňa 7. 10. 2015).
[11] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-360/10 (navštívené dňa 7. 10. 2015).
[12] MALCOLM, J.: European Web Host Ruled Liable for Users' Comments—Even Though It Didn't Read Them. Dostupné na internete: https://www.eff.org/deeplinks/2015/06/european-web-hosts-ruled-liable-users-comments-even-if-they-didnt-read-them (navštívené dňa 7. 10. 2015).

Veľká komora však upozornila na to, že estónske súdy vôbec nepokladali Delfi za poskytovateľa služieb informačnej spoločnosti, ale pokladali ho za tradičného vydavateľa. Veľká komora pritom bola ochotná akceptovať túto klasifikáciu spoločnosti Delfi AS, a to s poukazom na ekonomický záujem vydavateľa a na možnosti kontroly nad komentármi a ich obsahom. Táto kontrola sa prejavovala napríklad tým, že Delfi zakazovala komentáre s protiprávnym obsahom a mala možnosť znemožniť komentovanie tým komentátorom, ktorí porušili pravidlá komentovania. Delfi dokonca využívala filtrovací mechanizmus, hoci nie najdokonalejší.

Aj preto sa môže javiť, že Delfi AS by mohla byť rovnako postihnutá aj v zmysle čl. 14 smernice o elektronickom obchode (teda nie na základe všeobecnej úpravy o zodpovednosti vydavateľov), a to z dôvodu, že u nej predsa len bolo možné predpokladať istý stupeň vedomosti o protiprávnych komentároch, resp. istý stupeň vlastnej aktivity – ako to naznačuje aj samotné rozhodnutie komory s odkazmi na judikatúru SD EÚ. Hoci by totiž aj Delfi nemala vedomosť o protiprávnom obsahu, konala vraj tak, že bolo možné očakávať, že takúto vedomosť má.[13]

Podobne argumentuje aj Lorna Woods – už v prípade L'Oreal (C-324/09 z 12. júla 2011[14]) totiž SD EÚ konštatoval, že čl. 14 smernice nemá poskytovať ochranu v prípadoch, kedy poskytovateľ hrá „aktívnu rolu" pri prezentovaní a poskytovaní informácií, pričom táto aktívna rola mu dáva možnosť kontolovať alebo získať vedomosť o obsahu informácií. V tomto prípade pritom Delfi disponovala moderátomi (administrátormi) diskusií a tiež filtrovacím systémom. Pritom síce platí, že povinnosť monitorovať obsah diskusií, resp. služieb informačnej spoločnosti nemožno poskytovateľom ukladať (podľa čl. 15 smernice), nakoľko však národné súdy nepovažovali Delfi za poskytovateľa podľa tejto smernice, nevzťahovala sa na Delfi ani ochrana pred uložením monitorovacej povinnosti.

Uvedené estónske národné riešenie pritom podľa komentátorov nie je priamo v rozpore so smernicou. Otvára to však otázky, či rôznorodé národné prístupy k definovaniu poskytovateľa služieb informačnej spoločnosti v EÚ nebude vhodné zjednotiť, a to práve preto, aby sa predišlo uvedeným nejasnostiam a rozporom vo výklade tohto pojmu a aplikácie smernice na úrovni členských štátov EÚ.[15]

6 VÝZNAM ROZHODNUTIA PRE ZODPOVEDNOSŤ PREVÁDZKOVATEĽOV SLUŽIEB INFORMAČNEJ SPOLOČNOSTI V EÚ

Rozhodnutie Veľkej komory ESĽP vo svojej podstate potvrdilo, že vnútroštátny právny poriadok (v tomto prípade estónsky) má možnosť stanoviť si zákonom vlastné hranice základných práv. Tieto hranice boli estónskymi zákonmi a súdnym výkladom zákonov stanovené tak, že v ustálenej judikatúre boli online spravodajské portály považované za vydavateľov rovnocenných s papierovou tlačou, a nepodliehali výnimkám priznávaným poskytovateľom služieb informačnej spoločnosti. V takomto definovaní vydavateľov nevidel ESĽP rozpor s Dohovorom, ani so základnými právami.

Negatívne hodnotenie tohto záveru ESĽP sa pritom opiera o to, že takýto prístup k možnostiam vnútroštátnej úpravy a výkladu pojmu vydavateľa (a iných prípadne súvisiacich otázok) teoreticky umožňuje národnú úpravu, ktorá zavádza objektívnu zodpovednosť vydavateľov – ako to s obavami vyjadril aj disentujúci sudca ESĽP Sajó.[16]

V podstate tu však ani tak nejde o otázku objektívnej zodpovednosti vydavateľov, ako skôr o otázku definície a rozlíšenia vydavateľa papierovej tlače a vydavateľa v podmienkach služieb informačnej spoločnosti – totiž otáznym môže byť, do akej miery by sa malo pripustiť, aby si

[13] KUCZERAWY, A. – OMBELET, P-J.: Not so different after all? Reconciling Delfi vs. Estonia with EU rules on intermediary liability. Dostupné na internete: http://blogs.lse.ac.uk/mediapolicyproject/2015/07/01/not-so-different-after-all-reconciling-delfi-vs-estonia-with-eu-rules-on-intermediary-liability/ (navštívené dňa 7. 10. 2015).

[14] http://curia.europa.eu/juris/liste.jsf?num=C-324/09 (navštívené dňa 7. 10. 2015).

[15] WOODS, L.: Delfi v Estonia: Curtailing online freedom of expression? Dostupné na internete: http://eulawanalysis.blogspot.be/2015/06/delfi-v-estonia-curtailing-online.html (navštívené dňa 7. 10. 2015).

[16] HUSOVEC, M.: ECtHR: Imposing Strict Liability for User Comments is Compatible with Freedom of Expression. Dostupné na internete: http://www.husovec.eu/2015/06/ecthr-imposing-strict-liability-for.html (navštívené dňa 7. 10. 2015).

jednotlivé členské štáty EÚ vlastnou právnou úpravou a judikatúrou rozhodli, že vydavateľ elektronickej tlače bude podliehať rovnakej úprave ako vydavatelia papierovej tlače a nebude požívať výhody „bezpečného prístavu“ poskytovateľa služieb informačnej spoločnosti.

Ak by sa pritom aj EÚ (v judikatúre SD EÚ alebo v novej výslovnej právnej úprave) v budúcnosti ujednotila na tom, že všetci vydavatelia elektronickej tlače podliehajú pod smernicu o elektronickom obchode, máme za to, že stále zostane otvorená druhá naznačená otázka – ako rozhodnúť, či poskytovateľ spadá pod bezpečný prístav pasívneho a nevedomého poskytovateľa. Javí sa teda zároveň ako potrebné určiť aj bližšie kritériá „aktívneho“ poskytovateľa (napr. tým, že vyzýva na využívanie služieb informačnej spoločnosti v zmysle prenosu alebo ukladania informácií užívateľmi, alebo tým, že využíva filtrovací systém a pod.), resp. poskytovateľa obsahu (*content provider*).

Napokon, uvažovať možno aj o presnom vymedzení hraníc zodpovednosti vydavateľa (poskytovateľa). Riešením by tu obdobne ako v prípade navrhovaného nového nariadenia EÚ o ochrane osobných údajov mohlo byť nahradenie smernice o elektronickom obchode novým nariadením o elektronickom obchode (prípadne pod vhodnejším názvom – ako je napr. nariadenie o službách informačnej spoločnosti), ktoré by jednotne a presne upravilo podmienky zodpovednosti poskytovateľov služieb informačnej spoločnosti. Aj podľa názoru Electronic Frontier Foundation (EFF) totiž aktuálne rozhodnutie ESĽP vo veci Delfi dáva zelenú možnostiam sprísnenia zodpovednostných pravidiel vo vzťahu k poskytovateľom služieb informačnej spoločnosti, čo v konečnom dôsledku môže skutočne viesť k obmedzeniam slobody prejavu.[17]

7 ZÁVER

V predloženom príspevku sme sa pokúsili o vlastnú analýzu rozhodnutia Veľkej komory ESĽP vo veci Delfi. Na rozdiel od prvotných prehnaných reakcií interpretujúcich toto rozhodnutie ako koniec slobody prejavu a koniec internetových diskusií zaujímame v tomto príspevku zdržanlivejší postoj. Poukazujeme na to, že ESĽP v prípade Delfi posudzoval domáce estónske právo a jeho zákonné obmedzenie slobody slova tým, že podľa estónskeho práva vydavatelia elektronických médií požívajú rovnaký právny status z hľadiska zodpovednostných vzťahov ako vydavatelia printových médií. Rozhodnutie miestneho súdu vo veci Delfi bolo pritom podľa ESĽP v súlade s domácim právnym poriadkom, bolo predvídateľné, sledovalo legitímny cieľ, a bolo aj nevyhnutné (čo však môže byť otázne – naznačili to aj disentujúci sudcovia ESĽP Sajó a Tsotsoria: podľa nich totiž absolútna objektívna zodpovednosť vydavateľa podľa domáceho právneho poriadku nie je nevyhnutnou). Ani Dohovor Rady Európy o ochrane základných práv a ľudských slobôd, ani právo EÚ v podobe smernice o elektronickom obchode pritom takúto vnútroštátnu úpravu a výklad neznemožňujú; naopak, ESĽP svojím rozhodnutím vo veci Delfi takúto úpravu rešpektuje.

Ak by sme však aj mali za to, že spoločnosť Delfi mala byť posudzovaná ako poskytovateľ služieb informačnej spoločnosti (čo v súčasnosti smernica EÚ nezaručuje), bolo by potrebné vysporiadať sa s tým, či Delfi predstavovala pasívneho poskytovateľa služieb, alebo poskytovateľa aktívneho. Na rozhodnutie tejto otázky, ktorú považuje za dôležitú aj SD EÚ napr. v rozhodnutí L'Oreal, nám pritom smernica o elektronickom obchode tiež nedáva dostatočnú odpoveď – práve preto sa tiež môže potenciálne vyskytovať v rôznych členských štátoch EÚ rôzne hodnotenie „aktivity“. Napokon, rôzne môžu byť aj štandardy objektívnej zodpovednosti a odchýlky od tzv. bezpečného prístavu poskytovateľov služieb informačnej spoločnosti.

Všetky naznačené nejednoznačnosti by sa pritom do budúcnosti dali odstrániť buď judikatúrou SD EÚ, alebo spresnením úpravy v smernici o elektronickom obchode, alebo napokon podrobnou úpravou spojenou s povýšením úpravy služieb informačnej spoločnosti zo smernice o elektronickom obchode na úroveň nariadenia o službách informačnej spoločnosti.

[17] MALCOLM, J.: European Web Host Ruled Liable for Users' Comments—Even Though It Didn't Read Them. Dostupné na internete: https://www.eff.org/deeplinks/2015/06/european-web-hosts-ruled-liable-users-comments-even-if-they-didnt-read-them (navštívené dňa 7. 10. 2015).

Použitá literatúra:

HUSOVEC, M.: ECtHR: Imposing Strict Liability for User Comments is Compatible with Freedom of Expression. Dostupné na internete: http://www.husovec.eu/2015/06/ecthr-imposing-strict-liability-for.html (navštívené dňa 7. 10. 2015).
KUCZERAWY, A. – OMBELET, P-J.: Not so different after all? Reconciling Delfi vs. Estonia with EU rules on intermediary liability. Dostupné na internete: http://blogs.lse.ac.uk/mediapolicyproject/2015/07/01/not-so-different-after-all-reconciling-delfi-vs-estonia-with-eu-rules-on-intermediary-liability/ (navštívené dňa 7. 10. 2015).
MAJERNÍK, T.: Rozsudok Komory z 10. októbra 2013 vo veci: Delfi AS proti Estónsku sťažnosť č. 64569/09. Dostupné na internete: portal.concourt.sk/download/attachments/17269496/ESLP25.pdf (navštívené dňa 7. 10. 2015).
MALCOLM, J.: European Web Host Ruled Liable for Users' Comments—Even Though It Didn't Read Them. Dostupné na internete: https://www.eff.org/deeplinks/2015/06/european-web-hosts-ruled-liable-users-comments-even-if-they-didnt-read-them (navštívené dňa 7. 10. 2015).
PETKOVÁ, Z.: Ako môže kontroverzné rozhodnutie zlikvidovať (vulgárne) diskusie na webe. Dostupné na internete: http://medialne.etrend.sk/internet/ako-moze-kontroverzne-rozhodnutie-zlikvidovat-vulgarne-diskusie-na-webe.html (navštívené dňa 7. 10. 2015).
WOODS, L.*:* Delfi v Estonia: Curtailing online freedom of expression? Dostupné na internete: http://eulawanalysis.blogspot.be/2015/06/delfi-v-estonia-curtailing-online.html (navštívené dňa 7. 10. 2015).
WOODS, L.: The Delfi AS vs Estonia judgement explained. Dostupné na internete: http://blogs.lse.ac.uk/mediapolicyproject/2015/06/16/the-delfi-as-vs-estonia-judgement-explained/ (navštívené dňa 7. 10. 2015).

Kontaktné údaje:

doc. PhDr. JUDr. Tomáš Gábriš, PhD., LL.M.
tomas.gabris@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovenská republika

Mgr. Ing. Jakub Jošt
jakub.jost@gmail.com
Univerzita Komenského v Bratislave, Právnická fakulta
Šafárikovo nám. č. 6
P.O.BOX 313
810 00 Bratislava
Slovenská republika

INTERNETOVÉ VYHĽADÁVAČE V KONTEXTE VYBRANÝCH SÚŤAŽNOPRÁVNYCH ASPEKTOV

Rastislav Luby

Európska komisia

Abstract: The internet phenomenon has opened a new digital space as for the global communication, as well not least for the new digital economy, market, advertising and commerce. Search engines accumulate data and use sophisticated algorithms for being able to generate relevant information out of this data for user as a potential customer, who is in the same time in position of an addressee of digital advertising, whether targeted or untargeted. The way the search results are displayed has become a subject of global attention over the last years. The digital space indeed introduces opportunities to promote a competitive environment, but in the same time it also introduces a challenge for competition authorities to verify if there is no distortion of fair competition in that space. The aim of this paper is to analyse, from the subjective viewpoint of the author, selected competition law interpretation aspects mainly at the stage of defining the relevant market and identifying a position of dominance on it. It is however not the aim of this paper to provide a final view on the question whether it is possible, or not, to identify an abuse of a dominant position in specific real cases.

Abstrakt: Fenomén internetu otvoril nový digitálny priestor, ako pre globálnu komunikáciu, tak aj v neposlednom rade pre novú digitálnu ekonomiku, trh, reklamu a obchod. Vyhľadávače akumulujú dáta a využívajú sofistikované algoritmy na to, aby z týchto dát vedeli generovať relevantné informácie pre užívateľa ako pre potenciálneho zákazníka, ktorý je zároveň adresátom digitálnej reklamy, či už cielenej alebo necielenej. Zobrazovanie výsledkov vyhľadávania sa za posledné roky stalo predmetom globálnej pozornosti. Digitálny priestor totiž prináša príležitosti na podporu konkurenčného prostredia, zároveň však predstavuje výzvu pre regulátorov hospodárskej súťaže pri preverovaní, či v tomto priestore nedochádza k narušovaniu férovosti súťaže. Cieľom tohto príspevku je analyzovať, z hľadiska subjektívneho pohľadu autora, vybrané súťažnoprávne výkladové aspekty najmä v štádiu vymedzovania relevantného trhu a zisťovania dominantného postavenia na ňom. Nie je však cieľom príspevku poskytnúť finálny pohľad na otázku či je alebo nie je možné identifikovať zneužitie dominantného postavenia v konkrétnych skutočných prípadoch.

Key words: digital single market of the EU, definition of the relevant market, market dominance, leveraging of market power, abuse of dominance

Kľúčové slová: jednotný digitálny trh EÚ, vymedzenie relevantného trhu, trhová dominancia, prenášanie trhovej sily, zneužitie dominantného postavenia

1 ÚVOD

Na úvod je nevyhnutné zdôrazniť, že nie len vzhľadom na prebiehajúce neuzatvorené úradné konania v oblastiach, ktorých sa tento príspevok týka, všetky názory naznačené v tomto príspevku predstavujú výhradne iba subjektívny pohľad autora a nemôžu byť za žiadnych okolností považované za oficiálne stanovisko Európskej komisie. Neexistuje vôbec žiadna súvislosť medzi obsahom tohto príspevku a prebiehajúcimi vyšetrovaniami Európskej komisie vo vzťahu ku konkrétnym skutočným vyhľadávačom.

1.1 Význam vyhľadávacích platforiem v digitálnej ekonomike

Fenomén internetu otvoril nový digitálny priestor, ako pre globálne šírenie informácií a komunikáciu, tak aj v neposlednom rade pre novú digitálnu ekonomiku, trh, reklamu a obchod. Vyhľadávače pomáhajú spotrebiteľovi okamžite získať informáciu a taktiež pomáhajú podnikateľom využívať výhody elektronického obchodu, najmä z hľadiska odbytu. Platformy tohto typu akumulujú

obrovské množstvo dát a využívajú sofistikované algoritmy na to, aby z týchto dát vedeli generovať relevantné informácie pre užívateľa ako pre potenciálneho zákazníka, ktorý je zároveň adresátom digitálnej reklamy, či už cielenej alebo necielenej. Niektoré vyhľadávacie platformy majú významný vplyv na trh a tým aj na úroveň dosahovaného zisku podnikov. Spôsob akým zobrazujú výsledky vyhľadávania sa za posledné roky stal predmetom globálnej pozornosti.

Digitálny priestor totiž prináša príležitosti na podporu konkurenčného prostredia, zároveň však predstavuje výzvu pre regulátorov hospodárskej súťaže pri ich preverovaní, či v tomto priestore nedochádza k narušovaniu férovosti hospodárskej súťaže. Aj skratka „dot.com“ neznamená nič iné ako „commercial“, t.j. obchodný, teda ekonomicko-konkurenčný a reklamný priestor. Ide o dynamické odvetvie, v ktorom vyhráva ten, kto vie rýchlo inovovať.

Niektoré veľmi známe internetové vyhľadávače už z celosvetového hľadiska viackrát čelili obvineniam z protisúťažného správania aj mimo európskeho kontinentu, napríklad aj na americkom kontinente. Americký protimonopolný úrad FTC (Federal Trade Commission) takéto vyšetrovanie vykonal už v rokoch 2011-2013. Podozrieval najväčší vyhľadávač z možného vykonania manipulácie zobrazovania výsledkov vyhľadávania. FTC v zmysle americkej legislatívy aplikoval § 2 tzv. „Sherman Antitrust Act“, ktorý je nosným pilierom protimonopolnej legislatívy v USA.[1] Obdobné vyšetrovania prebiehajú v EÚ, ale tiež v Brazíli či v Indii. Zásadný význam pre zodpovedanie súťažnoprávnych otázok v oblasti internetových vyhľadávačov bude mať iste aj ďalší vývoj v prebiehajúcich vyšetrovaniach vo vzťahu ku konkrétnym vyhľadávačom. Tieto kauzy, až raz budú uzatvorené, by mohli byť veľmi zaujímavé pre právnu obec, ktorá sa zaujíma o súťažne právo v digitálnej oblasti.

2 VŠEOBECNÉ VERSUS ŠPECIALIZOVANÉ VYHĽADÁVAČE

Najznámejším celosvetovým typom sporu medzi vyhľadávačmi, popri sporoch zameraných aj na iné oblasti, prebieha medzi službami všeobecného vyhľadávania a službami špecializovaného, t.j. vertikálneho vyhľadávania. Pri analýze vyhľadávacích platforiem je teda základom rozlišovanie medzi vyhľadávačmi všeobecnými a špecializovanými, t.j. vertikálnymi.

Všeobecný internetový vyhľadávač je internetový portál prostredníctvom ktorého môže zadávateľ vyhľadávania vyhľadať v digitálnom priestore internetu informáciu týkajúcu sa ním zadaného slovného výrazu alebo frázy. Naproti tomu špecializovaným, t.j. vertikálnym vyhľadávačom je platforma, ktorej úlohou je vyhľadať konkrétny typ tovaru alebo služieb prípadne poskytnúť aj príslušné cenové porovnania. Všeobecne známe sú príklady špecializovaných vyhľadávačov napríklad z oblasti cestovného ruchu alebo z oblasti ubytovacích služieb, ktoré aj vykonávajú cenové porovnania.

Spory prebiehajú najmä okolo obvinení, že všeobecné vyhľadávače manipulujú výsledky vyhľadávania tak, že zo zaujatosti nezobrazujú, alebo zobrazujú neprimerane menej prominentne im konkurujúce špecializované vyhľadávače.[2] Také podozrenia by smerovali k názoru, že konkurujúce vyhľadávacie platformy sú vytláčané z trhu vyhľadávania čo by išlo aj na úkor spotrebiteľa, ktorý by inak mal možnosť používať ich služby špecializovaného vyhľadávania. Ide tu teda o obvinenia z neférového nakladania s trhovou silou, ktorú majú všeobecné vyhľadávače, teda o obvinenia zo zneužitia dominantného postavenia. Je to obvinenie z prenášania trhovej sily z trhu všeobecného vyhľadávania do trhov špecializovaného vyhľadávania, pretože veľa zadávateľov vyhľadávania hľadá špecializované porovnávanie cien práve tak, že sa ho pokúsia vyhľadať cez všeobecné vyhľadávanie.[3]

2.1 Ekonomický podtext všeobecného a špecializovaného vyhľadávania

Pre obidva typy vyhľadávaní je príznačný ich ekonomický resp. komerčný podtext. Všeobecné vyhľadávanie má na prvý pohľad charakter najmä informatívneho vyhľadávania, je však predmetom platenej cielenej reklamy. Špecializované, t.j. vertikálne vyhľadávanie máva viac priamy komerčný podtext. Zákazníci navštevujú špecializované vyhľadávače so zámerom kúpiť konkrétny

[1] Jeho obdobou je článok 102 Zmluvy o fungovaní EÚ.
[2] Spory prebiehajú aj okolo iných obvinení voči všeobecnému vyhľadávaču, podľa ktorých napríklad tento má kopírovať cudzí obsah, alebo zavádzať do svojich zmlúv klauzuly exkluzivity.
[3] KÖRBER, T.: Internet search engines and competition law. In: Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 6, s. 518.

typ produktu. Ak zákazník vie, že potrebuje konkrétny typ produktu a má záujem o jeho kúpu, tak má viac dôvoď navštíviť práve špecializovaný vyhľadávač. V mnohých prípadoch zákazníkovi však chýba informácia, ako sa ten špecializovaný vyhľadávač, ktorý zákazník potrebuje, vlastne volá. Pre získanie tejto základnej informácie v mnohých prípadoch zákazník potrebuje zas len všeobecný vyhľadávač. Následne však zákazník uhradí útratu, a teda aj províziu za predaj kúpeného produktu, prostredníctvom špecializovaného vyhľadávača. Táto úvaha by mohla viesť k záveru, že nie je v ekonomickom záujme všeobecného vyhľadávača prominentne zobrazovať odkazy na také špecializované vyhľadávače, ktoré stoja mimo jeho podnikateľského zoskupenia.

2.2 Organické a sponzorované zobrazovanie pri všeobecnom vyhľadávaní

Všeobecné vyhľadávače uskutočňujú dva typy zobrazovania a to organické a sponzorované.

Organické zobrazovanie predstavuje tzv. hlavné výsledky vyhľadávania, ktoré nie je nikým sponzorované a nie je teda platenou reklamou. Býva označované aj za tzv. prirodzené, resp. „earned“, teda „zarobené“ či „zaslúžené“. Zo súťažnoprávneho hľadiska je relevantnou otázkou či zo strany všeobecného vyhľadávača nedochádza pri zobrazovaní webových odkazov k umelému zatláčaniu do úzadia tých odkazov, ktoré sa týkajú konkurentov, teda či nedochádza k narúšaniu neutrality vo všeobecnom vyhľadávaní. Také konanie by týmto konkurentom sťažovalo prístup k zadávateľom vyhľadávania, ako k potenciálnym zákazníkom, a teda by ich na trhu znevýhodňovalo.

Sponzorované zobrazovanie predstavuje platenú reklamu. Zo súťažnoprávneho hľadiska je relevantnou otázkou, či všeobecný vyhľadávač neuplatňuje vyššie ceny voči tým zadávateľom reklamy, ktorí patria ku konkurencii. Samozrejme, uplatňovanie vyšších cien voči konkurentom by malo v konečnom dôsledku nepriaznivý vplyv na ich postavenie na trhu.

2.3 Neutralita vyhľadávania

Odborníci zvyknú poukazovať na praktické problémy pri rozlišovaní medzi na jednej strane objektívnym, neutrálnym resp. nezaujatým zobrazovaním výsledkov vyhľadávania a na druhej strane zaujatým zobrazovaním výsledkov vyhľadávania, ktoré narušuje férovosť konkurencie medzi vyhľadávačmi.

Každý vyhľadávač totiž pracuje na báze určitého nie jednoduchého algoritmu. Každý algoritmus vyhľadávania musí byť nastavený určitým konkrétnym spôsobom. Navyše každý takýto algoritmus je svojou podstatou dynamický a podlieha zmenám, ktoré sú vykonávané na každodennej báze. Vyhľadávací algoritmus teda nie je statický.[4]

Pozícia zákazníka, ktorý je zadávateľom vyhľadávania je v tomto kontexte oslabená aj faktom, že zadávateľ vyhľadávania v mnohých prípadoch ani nemusí byť schopný posúdiť, či dostáva objektívne, teda či dostáva kvalitné výsledky vyhľadávania. Ak aj zákazník môže mať dobrý dôvod zmeniť všeobecný vyhľadávač, otázka či ho naozaj aj zmení bude závisieť od toho, či sa vôbec zo svojho subjektívneho hľadiska dozvie, že v skutočnosti má dôvod vyhľadávač zmeniť.[5]

Jadrom sporu medzi všeobecnými a špecializovanými vyhľadávačmi je teda objektivita, tzn. neutralita zobrazovania výsledkov všeobecného vyhľadávania.

3 VYHĽADÁVAČE A VYMEDZENIE RELEVANTNÉHO TRHU

Pre súťažnoprávne posudzovanie správania sa účastníkov trhu je však primárnou otázkou vymedzenie relevantného trhu, teda príslušná trhová definícia. Vyhľadávače fungujú na báze dvojstrannej trhovej platformy, ktorá funguje obdobne ako obchodný sprostredkovateľ. Vyhľadávače spájajú zadávateľov vyhľadávania s obchodníkmi, ktorí ponúkajú tovary a služby ako zadávatelia platenej reklamy. Vyhľadávače teda pôsobia na dvojstrannom trhu, teda na dvoch vzájomne naviazaných trhoch.

Nakoľko ide o dvojstranný trh, bolo by nepochybne omylom myslieť si, že zákazník ako zadávateľ vyhľadávaní dostáva túto službu od vyhľadávača bezplatne, a že teda nie je klasickým spotrebiteľom zasluhujúcim právnu ochranu. Reklama, ktorá je na internetových platformách prítomná je síce platená primárne zadávateľmi platenej reklamy, je však zároveň aj odzrkadlená vo finálnych cenách tovarov a služieb, ktoré zákazník nakupuje, a teda v konečnom dôsledku je

[4] KÖRBER, T.: cit. dielo, s. 518.

[5] PATTERSON, M. R.: Google and Search Engine Market Power. In: Harvard Journal of Law & Technology Occasional Paper Series, July 2013, s. 5.

platená samotným zákazníkom. Ako príklad obdobného dvojstranného trhu je možné uviesť napr. komerčné televízie. Obsah, ktorý komerčné televízie poskytujú televíznemu divákovi mu taktiež neposkytujú bezplatne. Cena za vysielaný obsah je krytá platbami za reklamu od obchodníkov ponúkajúcich tovary a služby, ktorí sú zadávateľmi platenej reklamy.

Výška ceny, ktorú konkrétny zákazník fakticky platí za vyhľadávanie sa teda samozrejme neodvíja od kvantity ním zadaných vyhľadávacích dopytov. Cena nie je faktorom, ktorý by bol variabilný. Avšak kvalita, ktorú zákazník dostáva v podobe zobrazovaných výsledkov vyhľadávania je faktorom, ktorý môže variovať. Keďže je však v prípade služieb internetových vyhľadávačov variabilnou zložkou nie cena ale je ňou kvalita, má význam sústrediť sa na zložku kvality ako na indikátor hodnoty, ktorú dostáva zákazník.[6] Kvalitou je pre zadávateľa vyhľadávania jeho neutralita, teda objektivita vyhľadávania.

3.1 Sieťový efekt

Pre vyhľadávacie platformy je príznačný aj tzv. sieťový efekt, a teda hodnota poskytovanej služby, ktorú pre užívateľa reprezentuje pomer medzi jej kvalitou a cenou, je do veľkej miery závislá od celkovej kvantity jej užívateľov.

Ako všeobecne známy príklad fungovania sieťového efektu môžu v tomto kontexte poslúžiť mobilné telefónne siete. Ešte pred niekoľkými rokmi bolo volanie cez mobilné telefóny drahšie ako dnes taktiež z toho dôvodu, že nie každý bol v pozícii užívateľa mobilných sietí. Relatívne malé množstvo ich užívateľov tak muselo prispievať na sieť, ktorá mala prakticky rovnaké pokrytie ako má dnes. Čím je teda počet užívateľov dvojstrannej platformy väčší, tým viac sa aj v oblasti internetových vyhľadávacích platforiem zvyšuje potenciál pre zvýšenie kvality služieb internetového vyhľadávania.

Ako ďalší príklad znázorňujúci vzťah medzi kvalitou a množstvom užívateľov môžu poslúžiť online prekladače, ktoré sú voľne dostupné na stránkach jednotlivých vyhľadávačov. Pre kvalitu prekladania, ktorú tieto poskytujú, platí ten istý princíp ako aj pre kvalitu vyhľadávania. Aj tu platí, že väčšiu kvalitu prekladania dosahujú práve tie väčšie. Väčšie množstvo užívateľov im umožňuje dosiahnuť aj akýsi samoučiaci efekt, tzv. „self-learning effect“.

Tieto aspekty patria k dôvodom prečo dvojstranné trhové platformy v rámci ktorých funguje sieťový efekt majú na voľnom trhu tendenciu dospieť len k malému počtu silných dominujúcich hráčov, ba dokonca v niektorých prípadoch prakticky iba k jednému dominujúcemu subjektu. Ide tu o tzv. trhy „winner takes all markets“.

3.2 Trhová definícia

Pre účely tohto príspevku autor vychádza z predpokladu, že pre oblasť internetových vyhľadávacích služieb je možné na maloobchodnej, teda na spotrebiteľskej úrovni definovať relevantné trhy ako jeden maloobchodný, teda spotrebiteľský, relevantný trh všeobecného vyhľadávania a iné mnohopočetné maloobchodné spotrebiteľské relevantné trhy jednotlivých špecializovaných vertikálnych vyhľadávacích služieb, vrátane cenového porovnávania v konkrétnych oblastiach ich špecializácie.

Pokiaľ ide o veľkoobchodnú úroveň, v nadväznosti na maloobchodné spotrebiteľské trhy v oblasti vyhľadávacích služieb, autor vychádza z predpokladu, že na veľkoobchodnej úrovni je možné definovať veľkoobchodné relevantné trhy poskytovania platenej cielenej reklamy, ktorú vyhľadávače zobrazujú zadávateľom vyhľadávaní ako potenciálnym zákazníkom zadávateľov reklamy.

Keďže ide o nadväzujúce trhy, je potrebné brať do úvahy obe strany tohto dvojstranného trhu z globálneho hľadiska ako celku v ich vzájomnej súvzťažnosti. Uvedené platí aj pre analýzu v následnom štádiu skúmania otázok dominancie.

4 VYHĽADÁVAČE A ZISŤOVANIE TRHOVEJ DOMINANCIE

Pre účely zisťovania trhových podielov a dominancie v oblasti internetových vyhľadávacích služieb sa primárne naskytuje možnosť postupovať prostredníctvom porovnávania kvantity využívania jednotlivých vyhľadávačov v porovnaní s kvantitou využívania iných vyhľadávačov

[6] PATTERSON, M. R.: cit. dielo, s. 7.

a následného dovodenia trhovej dominancie toho subjektu, ktorý má veľmi vysoký, prípadne až prevládajúci trhový podiel, ak taký subjekt na trhu existuje.

Kritici takéhoto prístupu však poukazujú na možnosť, ktorú každý zadávateľ vyhľadávaní má, a síce jednoducho a pohodlne prejsť na iný vyhľadávač „one click away".[7] Tento pohľad však môže naraziť na protiargument, že zadávateľ vyhľadávania sám zo svojej pozície nemusí byť schopný posúdiť či mu ním používaný vyhľadávač poskytuje objektívne výsledky vyhľadávania alebo nie, keďže nemá vždy možnosť dozvedieť sa, že v danej situácii má dôvod prejsť na iný vyhľadávač. Zákazník je totiž mnohokrát v pozícii kedy nie je schopný posúdiť, aká je kvalita výsledku vyhľadávania, ktorý mu jeho vyhľadávač poskytuje. Taká úvaha by smerovala k záverom, že neznalosť zákazníka pôsobí smerom k posilneniu trhovej sily toho vyhľadávača, na ktorý je zákazník už zvyknutý.

Pokiaľ by vyhľadávač s veľmi vysokým a prevládajúci podielom na trhu mal navyše také postavenie na trhu, ktoré by mu umožňovalo bez primeraného, resp. technicky, industriálne alebo redakčne podloženého dôvodu do značnej miery znížiť objektivitu svojho vyhľadávania, a teda kvalitu vyhľadávania, pričom by zároveň zákazník nemal možnosť rozpoznať takéto zníženie kvality, tak potom by uvedená trhová pozícia vyhľadávača mohla naznačovať prítomnosť jeho trhovej dominancie.

Centrálnym problémom pri diskusii o zmene kvality vyhľadávania pri zobrazovaní výsledkov neplateného, t.j. organického vyhľadávania je otázka uprednostňovania tých webových odkazov, ktoré nekonkurujú všeobecnému vyhľadávaču, čo by v takom prípade predstavovalo diskrimináciu konkurenčných webových odkazov.

Zároveň je však potrebné mať na pamäti aj to, aký manévrovací priestor na zníženie objektivity vyhľadávania pre jeho zadávateľa, bez jeho možnosti rozpoznať takéto zníženie kvality, majú menšie nedominantné vyhľadávače. Ak takýto priestor majú aj malé vyhľadávače, potom je zrejme na mieste porovnanie medzi možnosťami zníženia objektivity vyhľadávania u malých vyhľadávačov v porovnaní s tými dominantnými.

Pri posudzovaní otázky do akej miery si v trhovom prostredí vyhľadávač môže dovoliť hýbať, resp. manipulovať objektivitou, teda kvalitou vyhľadávania, môže byť problémom aj to, že v praxi neexistuje modelový príklad „správneho" vyhľadávacieho algoritmu. Neexistuje teda tzv. „benchmark",[8] voči ktorému by bolo možne uskutočniť porovnania pri analyzovaní konkrétnych vyhľadávačov v kontexte hodnotenia ich trhovej sily.

Ako už bolo uvedené vyššie, v nadväznosti na maloobchodné trhy v oblasti všeobecných vyhľadávacích služieb stoja veľkoobchodné trhy poskytovania platenej cielenej reklamy, ktorú vyhľadávače zobrazujú zadávateľom vyhľadávaní ako potenciálnym zákazníkom. Vo vzťahu medzi internetovým vyhľadávačom a objednávateľom cielenej reklamy, ktorú vyhľadávače zobrazujú zadávateľovi vyhľadávania, už cena za zobrazenie reklamy samozrejme úlohu zohráva. Pokiaľ by vyhľadávač s veľmi vysokým a prevládajúci podielom na maloobchodnom trhu v oblasti všeobecných vyhľadávacích služieb mal navyše také postavenie na trhu, ktoré by mu umožňovalo neprimerane zvyšovať cenu za reklamu aj na veľkoobchodnom trhu poskytovania platenej cielenej reklamy, naznačovalo by to taktiež prítomnosť jeho trhovej dominancie. Hlavným problémom pri diskusii o cenovom správaní sa všeobecného vyhľadávača je teda analýza jeho možností cenovo uprednostňovať tie webové odkazy, ktoré nekonkurujú všeobecnému vyhľadávaču, teda analýza jeho možností cenovo diskriminovať konkurenčné webové odkazy.

Z pohľadu európskeho súťažného práva je dominanciou taká ekonomicky silná pozícia podniku, ktorá tomuto podniku umožňuje správať sa na trhu do značnej miery nezávisle na svojich konkurentoch, zákazníkoch a spotrebiteľoch.[9] Ak si uvedené premietneme na situáciu internetových vyhľadávačov, tak dominanciu by mohol mať ten vyhľadávač, ktorý je ekonomický schopný do značnej miery znížiť kvalitu, teda neutralitu vyhľadávania a zároveň do značnej miery zvýšiť cenu za zobrazovanie cielenej reklamy nad úroveň konkurenčných trhových cien.

---

[7] CANDEUB, A.: Behavioral Economics, Internet Search, and Antitrust. In: I/S: A Journal of Law and Policy for the Information Society, Vol. 9 (2014); MSU Legal Studies Research Paper No. 12-03, s. 408.

[8] PATTERSON, M. R.: cit. dielo, s. 24.

[9] Kauza 27/76 United Brands Company a United Brands Continental BV verzus Komisia Európskych spoločenstiev [1978] ECR 207.

5 VYHĽADÁVAČE A BUDÚCE EURÓPSKE REGULAČNÉ PROSTREDIE PRE 'ONLINE' PLATFORMY V RÁMCI STRATÉGIE EK PRE JEDNOTNÝ DIGITÁLNY TRH V EURÓPE

V máji tohto roku prijala nová Junckerova Európska komisia svoju ambicióznu stratégiu pre jednotný digitálny trh v Európe.[10] Nosnou ambíciou tejto stratégie je vytvorenie budúceho jednotného digitálneho trhu EÚ.

V tomto svojom politickom pláne pre digitálnu oblasť je oblasti online platforiem venovaná sekcia 3.3, ktorá má už vo svojom názve ambíciu vytvoriť ‚vhodné regulačné prostredie' pre platformy a sprostredkovateľov. To, že je použitý pojem ‚regulačné prostredie' by mohlo naznačovať úvahy o budúcom vytvorení všeobecného regulačného rámca ex-ante, ktorý bude stáť mimo súťažného práva, teda mimo sféry regulácie ex-post, ktorá postihuje iba konkrétne presne identifikované prípady.

Tento dokument zdôrazňuje vo vzťahu k nemenovaným online platformám, že hoci vplyv platforiem závisí od ich druhu a od ich trhovej sily, niektoré platformy kontrolujú prístup k online trhom a môžu mať významný vplyv na to, ako sú odmeňovaní rôzni účastníci trhu. V tomto kontexte sú zdôraznené obavy z rastúcej trhovej sily niektorých platforiem. Patrí medzi ne aj nedostatočná transparentnosť, pokiaľ ide o spôsob, akým platformy využívajú získané informácie, ich silná vyjednávacia pozícia v porovnaní s ich klientmi, ktorá sa môže odraziť v ich obchodných podmienkach, podpora ich vlastných služieb na úkor konkurentov a netransparentné cenové politiky alebo obmedzenia týkajúce sa stanovovania cien a podmienok predaja. Tento dokument predmetnú úvahu uzatvára konštatovaním, že niektoré online platformy sa stali aktérmi schopnými konkurovať v mnohých sektoroch hospodárstva a spôsob, akým využívajú svoju trhovú silu, vyvoláva niekoľko otázok, ktoré si vyžadujú ďalšiu analýzu „nad rámec uplatňovania práva hospodárskej súťaže v špecifických prípadoch".

Európska komisia si dala v tejto svojej stratégii za úlohu pracovať na komplexnom hodnotení úlohy platforiem. Toto hodnotenie bude zamerané na otázky relevantné ako pre maloobchodnú, tak aj pre veľkoobchodnú úroveň. Pokiaľ ide o maloobchodnú úroveň, predmetom analýzy Komisie bude transparentnosť výsledkov vyhľadávania vrátane platených odkazov a reklamy. Na úrovni veľkoobchodnej budú samozrejme predmetom pozornosti vzťahy medzi platformami a dodávateľmi. Komisia bude taktiež skúmať obmedzenia možností jednotlivcov a podnikov zmeniť platformu.

6 ZÁVER

Služby internetových vyhľadávačov zohrávajú v modernej digitálnej ekonomike neprehliadnuteľnú úlohu. Posudzovanie ich správania z pohľadu európskeho súťažného práva je predmetom ešte neuzatvorených právnych vyšetrovaní a sporov. Ich právne posúdenie dá odpovede na mnohé neuzatvorené a pritom fundamentálne otázky v oblasti súťažného práva v digitálnom ekonomickom priestore. Nie menej zaujímavé bude však aj sledovať tvorbu možného budúceho regulačného prostredia pre vyhľadávacie online platformy, ktorý bude stáť mimo rámca súťažného práva.

Použitá literatúra:

CANDEUB, A.: Behavioral Economics, Internet Search, and Antitrust. In: I/S: A Journal of Law and Policy for the Information Society, Vol. 9 (2014); MSU Legal Studies Research Paper No. 12-03.

KÖRBER, T.: Internet search engines and competition law. In: Journal of Intellectual Property Law & Practice, 2014, Vol. 9, No. 6.

PATTERSON, M. R.: Google and Search Engine Market Power. In: Harvard Journal of Law & Technology Occasional Paper Series, July 2013.

[10] Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Stratégia pre jednotný digitálny trh v Európe, 6. 5. 2015, COM(2015) 192 final.

Kontaktné údaje:
JUDr. Rastislav Luby
Rastislav.LUBY@ec.europa.eu
Generálne riaditeľstvo pre komunikačné siete, obsah a technológie
Európska komisia
Avenue de Beaulieu 33
B-1160 Brussels
Belgium

THE ELECTRONIC COMMUNICATION MEANS IN PASSING A RESOLUTION IN COMMERCIAL COMPANIES UNDER POLISH LAW

Piotr Pinior

University of Silesia in Katowice, Faculty of Law and Administration

Abstract: The electronic communication means are nowadays frequently used not only in every-day life but also in legal practice, including commercial companies. The new communication means should enable passing resolutions and exercising rights of the shareholders in more convenient way, the aim of the paper is to focus on some specific aspects of using electronic means at the general meeting, by executing minorities rights of shareholders and in passing the supervisory board resolutions by means of the direct communication facilities.

Key words: commercial companies, general meeting, supervisory board, passing resolutions, electronic form, direct communication facilities.

1. INTRODUCTION

The electronic communication means are frequently used under the Polish Commercial Companies Code[1], principally after the implementation of the new rules for castng votes at shareholders' meetings according to the provisions of Directive 2007/36/EU[2] and after changes of information rights in mergers and divisions. As the new communication means should facilitate the exercise of the rights of the shareholders, in particular of non-resident shareholders of a company with its registered office in a different state, the aim of this paper is to focus on some specific aspects of passing resolutions at the shareholders' meetings, such as minorities' rights to convene the meetings and putting items on the agenda, as well as casting votes by correspondence or from remote places. Moreover, some doubts arising over passing the supervisory board resolutions by means of direct communication facilities shall be discussed.

2. ELECTRONIC COMMUNICATION MEANS IN PASSING RESOLUTIONS AT THE SHAREHOLDERS' MEETING

2.1. Minorities' rights

According to article 6 of the Directive, Member States shall ensure that shareholders, acting individually or collectively have the right to put items on the agenda of the general meeting, provided that each such item is accompanied by a justification or a draft resolution to be adopted in the general meeting and have the right to table draft resolutions for items included or to be included on the agenda of a general meeting.

Member States may provide that this right may be exercised only in relation to the annual general meeting, provided that shareholders, acting individually or collectively, have the right to call, or to require the company to call, a general meeting which is not an annual general meeting with an agenda including at least all the items requested by those shareholders. In the Polish Code the right to put items on the agenda is not restricted to the annual meeting (art. 400 § 1 CCC). Generally, the shareholders of companies with their registered office in Poland have three different minorities' rights: the right to demand that a general meeting be called, the right to put items on the agenda and the right to table draft resolutions for items included in the general meeting (art. 400 § 1 and art. 401 § 1, § 4 CCC). The first right can be generally exercised in all companies (listed and non-listed), but

[1] The Code of Commercial Companies of 15 September 2000, Journal of Laws. 2000.94.1037 with amendments (abbreviated as CCC).

[2] Directive 2007/36/EU of 11 July 2007 on the exercise of certain rights of shareholders in listed companies (Dz.U.UE.L.2007.184.11).

the second one is excluded in case of convoking the general meeting by means of registered mail or a notice sent by courier, and the last one can be enjoyed only in listed companies.

According to EU law, any of these rights is subject to the condition that the relevant shareholder or shareholders hold a minimum stake in the company, such minimum stake shall not exceed 5 % of the share capital. In Poland such a stake for all three minorities' rights is determined for 5% of shares (1/20 of the share capital). The statues of the company may authorize shareholders representing less than 5% of the share capital.

Member States may provide that those rights shall be exercised in writing (submitted by postal services or electronic means). Under Polish law such a request may be submitted in both ways. But the Code literally distinguishes between different forms of putting in the request, as according to art. 400 § 2 and art. 401 § 1, the request to call the general meeting and the request to put items on the agenda may be submitted "in electronic form," but the request to table draft resolutions (art. 401 § 4) may be submitted "by electronic means of communication". The question is whether these two expressions mean the same or have a different meaning, and there is no unanimity in the literature on the issue. Some of the researchers claim that both expressions should be understood in the same way, even though they literally differ, as there are basically no practical differences between these two expressions[3]. However, other researchers claim that there is a difference between these expressions, and the term "electronic means of communications" should be interpreted more widely as the expression "electronic form"[4]. Taking into account the aim of the Directive and the lack of definitions concerning these expressions, they should be interpreted in the same way. The expression "electronic form" itself is interpreted as any electronic carrier (e.g. pen drive) or e-mail[5]. The general problem is that the Civil Code does not identify "the electronic form" with "the written form," therefore taking into consideration some new regulations in the Commercial Companies Code, the Polish legislator should intervene in order to harmonize the provisions of these two acts.

Member States shall ensure that, where the exercise of the right to put items on the agenda entails a modification of the agenda for the general meeting already communicated to shareholders, the company shall make available a revised agenda in the same manner as the previous agenda in advance of the applicable record date or, if no record date applies, sufficiently in advance of the date of the general meeting so as to enable other shareholders to appoint a proxy or, where applicable, to vote by correspondence. So as to present this issue more clearly, it is necessary to point out a few matters concerning the procedure of convocation of the general meeting.

In this respect the means for making announcements about the agenda of the forthcoming meeting have also been amended. In listed companies a general meeting shall be called by means of an announcement made on the internet site of the company and through the electronic system of passing the information on the stock-exchange, and such announcement shall be made at least 26 days prior to the date of the general meeting (art. 402^1 CCC). The formal announcement must provide information prescribed in art. 402^2 CCC, such as time and venue of the meeting, proposed agenda, record date and the precise procedure of exercising the rights, particularly of the voting rights, during the meeting. Besides, according to the art. 402^3 which regulates the duty to run a

[3] POPIOŁEK W. In: STRZĘPKA, J.A., POPIOŁEK, W., PINIOR, P., ZIELIŃSKA, E., Kodeks spółek handlowych. Komentarz. p. 922; HERBET, A., SZWAJA, J., In: SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. p. 976; KIDYBA, A., Kodeks spółek handlowych. Komentarz. Vol. II. p, 620; NAWORSKI, J.P. In: NAWORSKI, J.P., POTRZESZCZ, R., SIEMIĄTKOWSKI, T., STRZELCZYK, K., Kodeks spółek handlowych. Komentarz. Vol. III. p. 709.

[4] KRUKOWSKA-KOROMBEL, J., Prawa akcjonariuszy wykonywane za pośrednictwem środków elektronicznych w świetle przepisów kodeksu spółek handlowych. PPH 2010 Nr 9, p. 38.

[5] POPIOŁEK W. In: STRZĘPKA, J.A., POPIOŁEK, W., PINIOR, P., ZIELIŃSKA, E., Kodeks spółek handlowych. Komentarz. p. 917; PINIOR, P.: Ochrona praw mniejszości w Kodeksie spółek handlowych, p. 293; HERBET, A., SZWAJA, J., In: SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. p. 976; KIDYBA, A., Kodeks spółek handlowych. Komentarz. Vol. II. p, 620.

website of a listed company, the company has an obligation to provide further information, such as the number of shares and votes, documents prepared for the meeting, draft resolutions and forms for giving votes by correspondence. In non-listed companies the announcement informing about the general meeting is published in the electronic Court and Economic Journal at least three weeks prior to the date of the general meeting. Where all shares issued by the company are registered shares, the general meeting may be convened by means of registered mail or a notice sent by courier, no later than two weeks before the date of the general meeting. The notice may also be sent by e-mail, provided that the shareholder has given his written consent to such form, which is, parenthetically, another example of using electronic means relating to the general meeting.

In case of putting new items on the agenda on request of the shareholders, the revised agenda shall be announced in these two possible ways, depending on the type of the company. In listed companies, the revised agenda shall be published 18 days before the general meeting, which corresponds with the record date entitling persons who are company shareholders 16 days prior to the date of the general meeting to participate therein. In non-listed companies, the revised agenda shall be announced 4 days before the general meeting. This date does not correspond with the formal legitimacy because bearer shares shall entitle the holders to participate in the general meeting in a non-listed company, provided that the share certificates are deposited with the company at least one week prior to the general meeting. This regulation must undoubtedly be amended since the shareholders are not entitled to participate in the meeting, unless they have deposited their share at the proper date, but the revised agenda may contain some new significant items which can appear after the date for depositing share certificates[6]. A proposal to postpone the date of the general meeting has been formulated in the literature[7], nevertheless, this solution is not sufficient as in that case the meeting should be convened again, and yet new demands to put items on the agenda could be presented.

2.2. Giving votes by shareholders

According to the preamble of the Directive 2007/36/EU, as significant proportions of shares in listed companies are held by shareholders who do not reside in the Member State in which the company has its registered office, such non-resident shareholders should be able to exercise their rights in relation to the general meeting as easily as shareholders who reside in the Member State in which the company has its registered office. This requires that existing obstacles which hinder the access of non-resident shareholders to the exercise of voting rights without physically attending the general meeting be removed. Shareholders should be able to cast informed votes at, or in advance of, the general meeting, no matter where they reside.

To realize its aim, the Directive 2007/36/EU in art. 8 enables adopting resolutions in listed companies by electronic means, including:

- real-time transmission of the general meeting;
- real-time two-way communication enabling shareholders to address the general meeting from a remote location;
- a mechanism for casting votes, whether before or during the general meeting, without the need to appoint a proxy holder who is physically present at the meeting. This regulation was implemented without changes into Polish law (art. 406^5 CCC).

Actually only the second form of adopting resolutions mentioned above makes it possible to vote "virtually" without personal participation in the meeting. The first possibility is just a transmission, which does not allow the shareholder to participate in the general meeting, but in case of sending a proxy to the meeting, it is possible to watch the meeting, communicate with the proxy and to give him instructions for voting or to ask questions. The third possibility allows the shareholder to vote by correspondence using electronic means before or during the general meeting.

The use of electronic means for the purpose of enabling shareholders to participate in the general meeting may be made subject only to such requirements and constraints as are necessary

[6] PINIOR, P.: Ochrona praw mniejszości w Kodeksie spółek handlowych, p. 298.

[7] SZWAJA J., HERBET A. In: SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. p. 975.

to ensure the identification of shareholders and the security of the electronic communication. In Poland such restrictions have not been introduced into the code and the company itself may restrict shareholders participation only to the extent enabling shareholders' identification.

Moreover, according to Article 11 of the Directive, Member States shall permit shareholders to appoint a proxy holder by electronic means. Member States shall permit companies to accept the notification of the appointment by electronic means, and shall ensure that every company offers to its shareholders at least one effective method of notification by electronic means. This regulation is also new in Polish law, as the proxy holder used to be designated in the written form. Now the proxy holder in a listed company can be appointed in the written or electronic form (art. 412^1 § 2 CCC). As it has been mentioned above, the Polish Civil Code does not recognize the electronic form as the written form, so the regulation in the Commercial Companies Code concerning the form of appointing a proxy holder is *lex specialis* towards the Civil Code.

A listed company shall indicate to the shareholders at least one manner of notification by electronic means that the right of proxy holder has been granted in the electronic form. The company shall take appropriate measures to identify a shareholder and the manner of notification shall be set forth in the general meeting by-laws, and in the absence of by-laws, by the management board. Such regulation guarantees flexibility in appointing proxies but can also lead to great diversity among companies in practice. Moreover, there is a difference now in appointing the proxy holder in listed and non-listed companies, since the appointment in a non-listed company still shall be made in writing, otherwise it shall be null and void. In conclusion, such a difference does not actually have sufficient substantiation.

Apart from the above mentioned possibilities of adopting resolutions in listed companies by electronic means, art. 12 of the Directive provides for another possibility of voting, namely in the form of a special right to vote by correspondence. Member States shall permit companies to offer their shareholders the possibility to vote by correspondence in advance of the general meeting. Voting by correspondence may be made subject only to such requirements and constraints as are necessary to ensure the identification of shareholders and only to the extent that they are proportionate to achieving that objective. This provision has been implemented into Polish law in the art. 411^1 CCC. A dispute concerning the form of this right has arisen in the literature among Polish specialists. Some representatives of the company law claim that this right can be exercised in the traditional form or by electronic means[8], but others claim that such voting can take place only in the traditional (written) form[9]. Taking into account the aim of the Directive, the facilitation of participation and exercise of voting rights in listed companies, the imposition of such a restriction is not appropriate, thus this provision should be interpreted more widely to allow voting by correspondence in both the traditional or electronic form[10]. To illustrate the inconvenience a shareholder may suffer whist casting his vote suffice it to imagine an American shareholder sending a postal mail to Poland, giving his votes in the traditional written form by correspondence. All in all, this provision should be given a wider interpretation to allow shareholders to exercise the right to vote by correspondence in both the electronic and written form.

Preserving the written form of voting by correspondence entails a risk that the moment of voting may differ from the moment in which the vote is binding for the company. When calculating the quorum and the voting results, votes cast by mail which the company receives no later than at the time the vote is taken at the general meeting are counted (art. 411^2 § 1 CCC). A vote cast by mail may, however, be revoked by a statement made to the company and such a statement shall be effective if it is delivered to the company no later than at the time the voting at the general meeting is ordered (art. 411^2 § 4 CCC). The same rules should be applicable also to the mechanism for casting

[8] SOŁTYSIŃSKI, S. In: System Prawa Prywatnego Prawo spółek kapitałowych. Vol. 17B, p. 565.

[9] HERBET, A., In: SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. p. 1139; HORWATH, O., Głosowanie korespondencyjne na walnych zgromadzeniach – implementacja postanowień dyrektywy 2007/36/WE. Monitor Prawniczy 2010 Nr 2, p. 73; NAWORSKI, J.P. In: NAWORSKI, J.P., POTRZESZCZ, R., SIEMIĄTKOWSKI, T., STRZELCZYK, K., Kodeks spółek handlowych. Komentarz. Vol. III. p. 836.

[10] KIDYBA, A., Kodeks spółek handlowych. Komentarz. Vol. II. p, 686, also sees such a solution as a better one.

votes before the general meeting, mentioned in the provision of art. 406^5 § 1 p.3 CCC[11], but the Code does not refer directly to that case, that is why it is recommended to regulate such issues in the statues of the company.

3. SUPERVISORY BOARD RESOLUTIONS

Another example of using electronic means in adopting resolutions in Polish companies are the resolutions of the supervisory board. According to art. 388 § 3 CCC, the adoption of resolutions by the supervisory board by means of direct communication facilities shall be admissible only if the statues provide so. A resolution so adopted shall be valid if all members of the supervisory board have been notified of the content of the draft resolution. The adoption of resolutions by means of direct communication facilities shall not apply to the elections of the chairman and vice chairman of the supervisory board, the appointment of members of the management board, either removal or suspension of such persons in performance of their duties. The same regulation shall be provided for private limited liability companies, according to art. 222 CCC, however, the supervisory bodies are not compulsorily appointed in private companies, unless the statues or legal act provide otherwise, so it does not occur with great frequency.

The possibility of adopting resolutions by the supervisory board should be precisely regulated in the statues of the company, so as to avoid practical problems. It is suggested in the literature to focus on the following problems: the types of electronic means and technical issues of voting, the number of votes necessary for the validity of the resolutions, and the determination of the maximum time limit for casting votes by electronic means[12]. In case the statues do not provide any additional provision, it should be assumed that the minimum of half the votes of the supervisory board members are necessary for the validity of the resolution.[13] As for the period for casting votes it should be determined in the statues or the supervisory board's chairman should indicate such a date in the case when members of the supervisory board are in delay with casting their votes.

Generally, the provisions concerning supervisory board's resolutions are very laconic, so it is preferred to regulate specific details of the voting in the statues of the company.

4. CONCLUSIONS

Implementation of the Directive 2007/36/EU has introduced many amendments into Commercial Companies Code which have modified the rules of adopting resolutions in companies. The aim to facilitate the participation of non-resident shareholders in general meetings has been achieved, but obviously new problems occur in practice.

Some provisions must be amended in order to enable shareholders to exercise their rights in a proper manner, particularly the provisions concerning the announcement of the new agenda after its revision on demand of the shareholders in non-listed companies. It is also important to note that some additional regulation must be introduced into the statues, for instance to address the issue of adopting a resolution by the supervisory board, so as to avoid practical problems with using electronic communication means in passing resolutions.

---

[11] HERBET, A., In: SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. p. 1089.

[12] PINIOR, P.,: Szczególne sposoby podejmowania uchwał przez radę nadzorczą, p. 781 – 786.

[13] SOŁTYSIŃSKI, S. In: System Prawa Prywatnego Prawo spółek kapitałowych. Vol. 17B, p. 527; KIDYBA, A., Kodeks spółek handlowych. Komentarz. Vol. II. p, 529. There is no consent about it and in the literature it is possible to find different opinions. Some of the representatives claim that the quorum is not required and the majority of votes is counted in proportion to the votes cast but not to the number of supervisory board members, OPALSKI, A.: Rada nadzorcza w spółce akcyjnej, p. 300. It is also stated that all members of the supervisory board should cast their votes, SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, Kodeks spółek handlowych. Komentarz. Vol. II. p. 601; STRZELCZYK, K. In: NAWORSKI, J.P., POTRZESZCZ, R., SIEMIĄTKOWSKI, T., STRZELCZYK, K., Kodeks spółek handlowych. Komentarz. Vol. III. p. 613.

Bibliography:
HORWATH, O., Głosowanie korespondencyjne na walnych zgromadzeniach – implementacja postanowień dyrektywy 2007/36/WE. Monitor Prawniczy 2010 Nr 2, p. 73 – 77.
KIDYBA, A., Kodeks spółek handlowych. Komentarz. Vol. II. 10th edition. Warsaw Wolters Kluwer 2013. 1608 pages. ISBN 978-83-264-4494-4.
KRUKOWSKA-KOROMBEL, J., Prawa akcjonariuszy wykonywane za pośrednictwem środków elektronicznych w świetle przepisów kodeksu spółek handlowych. PPH 2010 Nr 9, p. 36 – 43.
NAWORSKI, J.P., POTRZESZCZ, R., SIEMIĄTKOWSKI, T., STRZELCZYK, K., Kodeks spółek handlowych. Komentarz. Vol. III. 1st edition. Warsaw Lexis Nexis 2012. 1416 pages. ISBN 978-83-762-0554-0.
OPALSKI, A.: Rada nadzorcza w spółce akcyjnej. Warsaw C.H. Beck 2006. 552 pages. ISBN 978-83-7483-443-8.
PINIOR, P.: Ochrona praw mniejszości w Kodeksie spółek handlowych. In: Kodeks spółek handlowych po dziesięciu latach. Wrocław 2013, p. 287 – 302. ISBN 978-83-229-3346-6.
PINIOR, P.,: Szczególne sposoby podejmowania uchwał przez radę nadzorczą. In: Prawo handlowe XXI wieku. Czas stabilizacji, ewolucji, czy rewolucji. Księga jubileuszowa Profesora Józefa Okolskiego. Warsaw Wolters Kluwer 2010, p. 779 – 793. ISBN 978-83-264-0652-2.
SOŁTYSIŃSKI, S. (ed.) System Prawa Prywatnego Prawo spółek kapitałowych. Vol. 17B, Warsaw C. H. Beck 2010. 1102 pages. ISBN 978-83-255-2066-3
SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, Kodeks spółek handlowych. Komentarz. Vol. II. 2nd edition. Warsaw C.H. Beck 2005. 995 pages. ISBN 83-7387-661-8.
SOŁTYSIŃSKI, S., SZAJKOWSKI, A., SZUMAŃSKI, A., SZWAJA, J., HERBET, A., MATACZYŃSKI M., MIKA, I.B., SÓJKA, T., TARSKA, M., WYRWIŃSKI M., Kodeks spółek handlowych. Komentarz. Vol. III. 3rd edition. Warsaw C.H. Beck 2013. 1978 pages. ISBN 978-83-255-5251-0.
STRZĘPKA, J.A., POPIOŁEK, W., PINIOR, P., ZIELIŃSKA, E., Kodeks spółek handlowych. Komentarz. 6th edition. Warsaw: C.H. Beck 2013. 1418 pages. ISBN 978-83-255-5212-1.

Contact information:
Dr hab. Piotr Pinior
piotr.pinior@us.edu.pl
University of Silesia in Katowice
Bankowa 11B
40-007 Katowice
Poland

REALIZAČNÉ ASPEKTY ELEKTRONICKÝCH VOLIEB A ICH DOPAD NA PRÁVNY PORIADOK SLOVENSKEJ REPUBLIKY

Soňa Sopúchová

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The author in this paper deals with the possibilities of electronic execution of the right to vote. The first part is devoted to the analysis of current methods of voting in elections in the Slovak Republic, in particular the rules and principles of the electoral law. The second part focuses on the electronic elections that can be approached in several ways. The author in the next section goes back to the principles of the electoral law and the question of its fulfillment in a case of electronic voting. The paper also contains comparison of the advantages and disadvantages of classic elections as well as challenges and risks of electronic elections. At the end of the article the author summarizes lessons learned and possible ways of electronic execution of the right to vote in the Slovak Republic.

Abstrakt: Autorka sa v príspevku zaoberá možnosťami elektronického výkonu volebného práva. Prvá časť je venovaná analýze súčasných spôsobov hlasovania vo voľbách v podmienkach Slovenskej republiky, najmä právnej úprave a zásadám volebného práva. Druhá časť príspevku sa zameriava na elektronické voľby, ktoré možno uskutočňovať viacerými spôsobmi. Autorka sa v ďalšej časti vracia k zásadám volebného práva a otázke ich naplnenia v prípade elektronického hlasovania. Súčasťou príspevku je porovnanie výhod a nevýhod klasických volieb a rovnako výziev a rizík volieb elektronických. V závere príspevku autorka sumarizuje získané poznatky a navrhuje možné spôsoby elektronického výkonu volebného práva v Slovenskej republike.

Key words: electronic voting, e-voting, e-election, informatization of society

Kľúčové slová: voľby, elektronické hlasovanie, e-voting, e-election, informatizácia spoločnosti

1 ÚVOD

Voľby predstavujú v pluralitnej spoločnosti nástroj pre výkon volebného práva a sú súčasťou osvietenského konceptu ľudských práv. Voľby sú zaraďované do kategórie politických a občianskych práv jednotlivca, prostredníctvom ktorých občania volia svojich zástupcov a tým vykonávajú správu verejných vecí a realizáciu svojich záujmov. Vyberanie zástupcov ľudu hlasovaním je súčasťou ľudskej spoločnosti už od nepamäti a spôsob jeho uskutočnenia sa v priebehu ľudských dejín rozmanito vyvíjal. Starovekí Rimania hlasovali pomocou farebných guľôčok, starovekí Gréci používali hlinené čriepky, nazývané ostraka. Týmto spôsobom hlasovali napr. o vylúčení niektorých nežiaducich osôb z verejného života. V Benátkach v 13. storočí využívali, v snahe minimalizovať vplyv bohatých a známych rodín pri voľbe vojvodu, systém pozostávajúci z 10 kôl, v ktorých sa striedalo náhodné losovanie a schvaľovacie volenie. Tento systém reflektoval záujmy väčšiny aj menšiny a s miernymi zmenami sa udržal do konca 18. storočia.

Spoločnosť zaznamenala v posledných desaťročiach veľké zmeny súvisiace s vedou a technikou. Koniec dvadsiateho storočia a začiatok dvadsiateho prvého storočia možno označiť za modernú dobu, charakteristickú rozsiahlym využívaním informačných a komunikačných technológií, akými sú napríklad počítače, počítačové programy, mobilné telefóny, platobné karty či televízia. V súčasnosti stále prebieha explozívny rozvoj novodobých technológií a tento postupne mení industriálnu spoločnosť na spoločnosť informačnú[1], pričom vzhľadom na rýchlosť a globálnosť

[1] Výkladový terminologický slovník elektronických komunikácií, ktorý poskytuje Výskumný ústav spojov definuje informačnú spoločnosť ako: *„spoločnosť, ktorá je založená na výraznom prenikaní*

týchto zmien sa niekedy hovorí aj o informačnej revolúcii.[2] Informatizácia spoločnosti predstavuje dlhodobý projekt, ktorého cieľom je prechod k maximálnemu využívaniu informačných a komunikačných technológií vo všetkých oblastiach spoločenského, politického a hospodárskeho života. Ide o globálny fenomén týkajúci sa všetkých vyspelých štátov sveta, v rámci ktorých sa informatizácia spoločnosti stala jednou z primárnych úloh stanovených v programových vyhláseniach vlád. Súčasným lídrom v rozvoji informatizácie spoločnosti je Európska únia, ktorá zakotvila hlavné otázky tohto procesu v najnovšom dokumente *Digitálna agenda pre Európu.*

Informatizácia spoločnosti má podľa sociológov a politológov význam aj z hľadiska demokracie a jej princípov. Prikláňame sa k tomuto názoru s dodatkom, že v informačnej dobe majú občania lepší prístup k informáciám než tomu bolo v minulosti a s tým súvisí aj vyššia miera uplatňovania jednotlivých práv a posilňovanie demokratického spôsobu vládnutia. Využívanie informačných a komunikačných technológii a s tým súvisiaca modernizácia nachádza svoje uplatnenie v rôznych oblastiach spoločenského života, akými sú napríklad *verejná správa (e-Government)*, *súdnictvo (e-Justice)*, *zdravotníctvo (e-Health)*, *vzdelávanie (e-Learning)*, ale taktiež problematika *volieb (e-Voting alebo e-Election)*.

Cieľom tohto príspevku je poukázať na prienik informačno-komunikačných technológií do výkonu volebného práva občanov prostredníctvom elektronických volieb a ich porovnanie s „klasickým" spôsobom hlasovania.

2 VÝKON VOLEBNÉHO PRÁVA V SLOVENSKEJ REPUBLIKE

2.1 Právna úprava

Volebné právo patrí medzi základné politické práva občanov a jeho kvalita má ústavnoprávne dimenzie premietnuté tak v ústavnej úprave volebného práva a zákonnej úprave, ako aj na medzinárodnej úrovni. Okrem dôležitej formálnej úpravy a ochrany, má toto právo nezastupiteľný materiálny význam a dosah na jeden z najdôležitejších princípov v práve – demokraciu.[3]

Výrazný vplyv na slovenskú právnu úpravu majú ***medzinárodné dokumenty*** týkajúce sa práv občanov, predovšetkým Medzinárodný pakt o občianskych a politických právach otvorený na podpis v New Yorku dňa 19. decembra 1966 (ďalej len „Pakt"). V mene vtedajšej Československej socialistickej republiky bol Pakt podpísaný 7. októbra 1968. Článok 25 Paktu ustanovuje, že: „*každý občan má právo a možnosť bez akýchkoľvek rozdielov uvedených v článku 2 a bez neodôvodnených obmedzení:*

a) *zúčastňovať sa na vedení verejných záležitostí priamo alebo prostredníctvom slobodne volených zástupcov;*
b) *voliť a byť volený v pravidelných voľbách, ktoré sa budú konať na základe všeobecného a rovného hlasovacieho práva, tajným hlasovaním zabezpečujúcim slobodu hlasovania;*
c) *vstúpiť za rovnakých podmienok do verejných služieb svojej krajiny.*[4]

Ústavnoprávnu rovinu v Slovenskej republike reflektuje Zákon č. 460/1992 Zb. Ústava Slovenskej republiky (ďalej len „Ústava SR"), ktorá upravuje inštitút volieb vo viacerých ustanoveniach. Predovšetkým ide o článok 2 ods. 1, ktorý zakotvuje, že štátna moc pochádza od občanov, ktorí ju vykonávajú prostredníctvom slobodnej voľby svojich zástupcov alebo priamo. Samotné voľby a výkon volebného práva potom bližšie upravuje článok 30. Jednou z ústavných podmienok je skutočnosť, že voľby sa musia konať v lehotách nepresahujúcich pravidelné volebné obdobie stanovené zákonom. Na výkon volebného práva musia byť aplikované základné zásady, ktoré vyplývajú z Paktu a ktoré Ústava SR zakotvuje v článku 30 odsek 3 nasledovne: *„Volebné právo je všeobecné, rovné a priame a vykonáva sa tajným hlasovaním. Podmienky výkonu*

informačných a komunikačných technológií, poznatkov a informácií do všetkých okruhov spoločenského života, a to v takej miere, že zásadným spôsobom menia spoločenské vzťahy a procesy."

[2] VLÁDA SLOVENSKEJ REPUBLIKY: Politika informatizácie spoločnosti v Slovenskej republike. Bratislava, 2001.

[3] CIBULKA, Ľ. Štátoveda, s. 124.

[4] Článok 25 Medzinárodného paktu o občianskych a politických právach.

volebného práva ustanoví zákon.“ [5] Okrem uvedených všeobecných ustanovení ďalej Ústava SR upravuje základné rámce jednotlivých druhov volieb, a to v článku 73 - Voľby do Národnej rady Slovenskej republiky, v článku 101 - Voľby prezidenta Slovenskej republiky a v článku 69 - Voľby do obecných zastupiteľstiev a zastupiteľstiev vyšších územných celkov a voľby starostov obcí a predsedov vyšších územných celkov.

Na medzinárodnoprávnu a ústavnoprávnu rovinu regulácie volieb nadväzuje **zákonná úprava**, ktorá v súčasnosti na Slovensku obsahuje jeden volebný kódex – Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o voľbách“), ktorý predstavuje technickú možnosť výkonu volebného práva. Zákon musí byť konštruovaný tak, aby umožňoval výkon práva a nevytváral žiadne bariéry. Pred nastúpením účinnosti uvedeného Zákona o voľbách, ktorá nastala dňa 1. júla 2014, sa voľby uskutočňovali na základe viacerých právnych predpisov upravujúcich jednotlivé druhy volieb. Tieto boli ku dňu účinnosti nového zákona zrušené. Prijatím nového Zákona o voľbách teda došlo k zjednoteniu úprav existujúcich druhov volieb. Zrušené boli nasledovné predpisy:

- Zákon č. 333/2004 Z. z. o voľbách do Národnej rady Slovenskej republiky,
- Zákon č. 346/1990 Zb. o voľbách do orgánov samosprávy obcí,
- Zákon č. 564/1992 Zb. o spôsobe vykonania referenda,
- Zákon č. 46/1999 Z. z. o spôsobe voľby prezidenta Slovenskej republiky, o ľudovom hlasovaní o jeho odvolaní a o doplnení niektorých ďalších zákonov,
- Zákon č. 303/2001 Z. z. o voľbách do orgánov samosprávnych krajov a o doplnení Občianskeho súdneho poriadku,
- Zákon č. 331/2003 Z. z. o voľbách do Európskeho parlamentu.

2.2 Zásady volebného práva

Volebné dedičstvo Európy, tak ako ho opísala Európska komisia pre demokraciu prostredníctvom práva (Benátska komisia) v dokumente z 18. februára 2002 [6], sa opiera o päť základných princípov volebného práva, a to, že voľby majú byť všeobecné, priame, rovné a slobodné s tajným hlasovaním.

V nadväznosti na medzinárodnoprávne dokumenty zakotvuje slovenská legislatíva (Ústava SR i Zákon o voľbách) štyri kvalitatívne znaky výkonu volebného práva, a to ***všeobecnosť, rovnosť, priamosť a tajnosť hlasovania***. V tejto súvislosti dodávame, že uvedené znaky sa vzťahujú na všetky druhy volieb (prezidentské, európske, parlamentné i samosprávne). V ďalšej časti príspevku vymedzujeme podstatu jednotlivých zásad a ich aplikovanie v klasických voľbách.

Všeobecnosť – Tento znak sa v pozitívnom vymedzení chápe ako spôsobilosť každého spravovať štátne záležitosti. V negatívnom ponímaní ide o absenciu kvalifikačných, vzdelanostných, majetkových, národnostných a iných predpokladov na výkon volebného práva. Zjednodušene povedané, ľudia nie sú menej alebo viac kvalifikovaní na riadenie štátu. Volebné zákony jednotlivých krajín však upravujú určité kritéria pre účasť vo voľbách, a to najmä v súvislosti s aktívnym a pasívnym volebným právom, pri ktorých sa zohľadňuje vek.[7]

Rovnosť – Rovnosť volebného práva konkretizoval v roku 1998 Ústavný súd Slovenskej republiky v náleze PL. ÚS 19/98, a to nasledovne:

a) každý občan má mať rovnaké postavenie pri výkone volebného práva,
b) každý občan má jeden hlas, ktorý ma rovnakú váhu oproti hlasom ostatných voličov,
c) rovnaké podmienky uchádzania sa o zvolenie,
d) rovnaké šance na získanie mandátu.

Prvé dve možnosti sa týkajú aktívneho volebného práva a ďalšie dve pasívneho volebného práva. Nerovné volebné právo by bolo v tom prípade, ak by voliči mali väčší počet hlasov na základe napríklad dosiahnutého vyššieho vzdelania, majetkových pomerov alebo platenia daní. K

[5] Článok 30 ods. 3 Ústavy SR.
[6] EUROPEAN COMMISION: Europe´s Electoral Heritage. Strasbourg, 2002.
[7] V Slovenskej republike je aktívne volebné právo (právo voliť) spojené s dosiahnutím veku 18 rokov a pasívne volebné právo (právo byť volený) s dosiahnutím veku 21 rokov.

dôležitým predpokladom zachovania tohto princípu patrí rovnosť volebných obvodov, pretože len tak má hlas každého z voličov rovnakú váhu.

Priamosť – Priamosťou volebného práva sa rozumie neexistencia sprostredkovateľa medzi voličom a kandidátom, to znamená, kandidáti sú volení priamo voličmi a voliči volia priamo kandidátov. V tejto súvislosti dopĺňame, že možnosť udeliť hlas konkrétnej osobe v rámci politickej strany a nehlasovať len za politickú stranu, bolo Ústavným súdom SR v náleze II. ÚS 48/97 vyhlásené za ústavnú hodnotu.

Tajnosť – Tajnosť hlasovania v praxi znamená, že volič upraví hlasovací lístok takým spôsobom, že nie je možné zistiť, ako hlasoval, resp. aký bol obsah jeho rozhodnutia. Sloboda a tajnosť volieb by bola vylúčená, ak by bolo možné dodatočne zistiť, ktorý občan hlasoval akým spôsobom. V súvislosti s tajnosťou hlasovania vznikla otázka, či je dodržiavanie tejto zásady právom alebo povinnosťou voliča a teda či si volič nachádzajúci sa za plentou môže napríklad odfotografovať svoj hlasovací lístok. Ústavný súd Slovenskej republiky v náleze ÚS 76/2001 prišiel k jednoznačnému záveru, podľa ktoré ide o povinnosť, ktorá má dve roviny – vertikálnu (vzťahujúce sa na štát a jeho garanciu tajnosti hlasovania) a horizontálnu (vzťahujúce sa na fyzické osoby, pri ktorej sa zakazuje preukazovanie voľby, napr. fotografovaním hlasovacieho lístka).

2.3 Spôsob hlasovania

V Slovenskej republike je v súčasnej dobe možné vykonávať obsah volebného práva dvoma spôsobmi, ktoré sú upravené v Zákone o voľbách. Ide o voľby prostredníctvom hlasovacích lístkov prebiehajúce za účasti voliča alebo poštou. Pre účely tohto príspevku sme prvý spôsob nazvali *klasický*. Ide o voľbu hlasovacími lístkami, pri ktorej sa osoby s aktívnym volebným právom musia dostaviť do volebnej miestnosti a uskutočniť svoju voľbu. Volič v tomto prípade hlasuje osobne a zastúpenie nie je prípustné. Priebeh volieb začína preukázaním totožnosti občianskym preukazom alebo iným úradným dokladom, ktorý obsahuje podobizeň voliča a všetky údaje uvedené o ňom v zozname voličov. Člen volebnej komisie následne odovzdá voličovi hlasovací lístok, čo volič potvrdí vlastnoručným podpisom. Po prevzatí hlasovacieho lístka a obálky vstupuje volič do osobitného priestoru na úpravu hlasovacích lístkov. Po uskutočnení voľby vkladá volič obálku pred okrskovou volebnou komisiou do volebnej schránky. Okrsková volebná komisia sčíta obálky a porovná ich počet so záznamami v zozname voličov. Obálky, ktoré nemajú potrebné zákonné náležitosti a hlasovacie lístky, ktoré neboli v obálke, okrsková volebná komisia vylúči.[8]

Alternatívnym spôsobom hlasovania sú *voľby poštou*, ktoré Zákon o voľbách pripúšťa len pre voľby do Národnej rady Slovenskej republiky. Požiadať o voľbu poštou možno písomne alebo elektronicky. Takýmto spôsobom môže svoj hlas odovzdať:

a) volič, ktorý nemá trvalý pobyt na území Slovenskej republiky a ktorý bol na základe žiadosti zapísaný do osobitného zoznamu voličov,
b) volič, ktorý má trvalý pobyt na území Slovenskej republiky, v čase volieb sa zdržiava mimo jej územia a o voľbu poštou požiada obec, v ktorej má trvalý pobyt.[9]

Voľby poštou prebiehajú na základe systému dvoch obálok, a to obálky podľa ustanovenia § 22 ods. 3 Zákona o voľbách a návratnej obálky, do ktorej sa okrem obálky s hlasovacím lístkom vkladá čestné prehlásenie. Štátna komisia po otvorení návratných obálok a po vybratí obálok s hlasovacími lístkami vkladá obálky do volebnej schránky. Voľby poštou predstavujú prvý krok k elektronickým voľbám, ktoré fungujú na podobnom obálkovom princípe.

2.4 Výhody a nevýhody

Súčasný spôsob volieb v Slovenskej republike má bezpochyby viaceré výhody, a to najmä nespochybniteľnosť hlasovania, nemožnosť dodatočne zistiť obsah hlasovania, väčšia technická bezpečnosť volieb a v neposlednom rade slávnostný charakter volebného aktu. Na druhej strane však možno identifikovať aj niektoré negatívne stránky klasického hlasovania, za ktoré považujeme spätosť s miestom trvalého pobytu a s tým súvisiaci nezáujem voličov o vybavenie hlasovacieho

[8] Celý spôsob hlasovania je upravený v ustanovení § 24 Zákona o voľbách.
[9] Ustanovenia § 59 a 60 Zákona o voľbách.

preukazu, finančná, časová a personálna náročnosť predovšetkým vo vzťahu k štátu a mechanický spôsob sčítavania hlasov, ktorý umožňuje vznik chýb.

3 ELEKTRONICKÉ VOĽBY

3.1 Typy elektronického hlasovania

Elektronické hlasovanie (e-hlasovanie) je hlasovanie prostredníctvom širšieho spektra zariadení založených na informačných technológiách (napr. digitálny TV, mobilný telefón, počítač – online i offline, ako aj iné terminály podobné počítačom, telefón).

Elektronické hlasovanie sa v dnešnej dobe používa iba ako alternatíva k hlasovaniu bežným spôsobom. Elektronické hlasovanie však neznamená len hlasovanie vzdialeným prístupom, to znamená cez Internet, ale ide o všeobecný pojem, ktorý zahŕňa široké spektrum možností udelenia hlasu. Medzi najčastejšie spôsoby elektronického hlasovania sa zaraďujú:

a) *Hlasovanie použitím počítača alebo iného zariadenia pre priamy záznam, ktorý je nainštalovaný vo volebnej miestnosti a ktorý zaznamenáva a súčasne ukladá hlasy. Hlasovať možno pomocou dotykovej obrazovky alebo stlačením tlačidla.*
b) *Hlasovanie prostredníctvom Internetu, a to buď vo verejných a kontrolovaných oblastiach (napr. volebné miestnosti) alebo v nekontrolovaných oblastiach vzdialeným prístupom (napr. špeciálne kiosky alebo domovy),*
c) *Hlasovanie pomocou optického alebo digitálneho skenovacieho zariadenia umiestneného vo volebnej miestnosti, ktoré zaznamenáva hlasovacie lístky v počítači. Účelom je najmä zlepšenie presnosti procesu sčítavania a zníženie potenciálnych manuálnych chýb.*
d) *Hlasovanie kombinovaným spôsobom, ktoré prebieha vo volebnej miestnosti za použitia jedného média pre záznam hlasu a ďalšieho zariadenia pre uloženie hlasu. Tento systém sa podstatne líši od prvej možnosti v tom, že na médiu na zaznamenávanie hlasov neexistuje pamäť pre ukladanie hlasov a je prakticky nemožné, aby volič manipuloval pamäť druhého zariadenia obsahujúce hlasovania*.[10]

Elektronické hlasovanie môžeme rozdeliť na hlasovanie *online* a *offline*. Pri offline hlasovaní nie sú hlasovacie počítače alebo iné elektronické zariadenia vzájomne prepojené, pri online hlasovaní sú počítače prepojené v sieti klient (volič) - server.

V Spojených štátoch amerických sú aktivity smerujúce k hlasovaniu cez Internet známe už dlhšiu dobu. V januári 2000 vypracovala Kalifornská expertná skupina (California Internet Task Force) Správu o hlasovaní cez Internet.[11] Správa opisuje hlasovanie cez Internet ako proces hlasovania, ktorý umožňuje voličovi použitím Internetu bezpečne a tajne označiť a „vhodiť" hlasovací lístok. Rozoznáva dva základné spôsoby hlasovania: *hlasovanie vo volebnej miestnosti* a *hlasovanie mimo nej*.

Pri hlasovaní vo volebnej miestnosti za použitia počítačov sú prítomní členovia volebnej komisie, ktorí vykonávajú identifikáciu (overenie totožnosti) voliča. Takéto hlasovanie si nevyžaduje digitálnu alebo elektronickú identifikáciu.

Hlasovanie mimo volebnej miestnosti, najmä ak nie sú členovia volebnej komisie prítomní, si už vyžaduje elektronickú identifikáciu; volič je povinný sa preukázať elektronickou identifikačnou kartou alebo osobným kľúčom, ktoré ho identifikujú ako oprávneného hlasovať. Tento postup je nevyhnutný aj pre zachovanie princípu jeden volič - jeden hlas. Na druhej strane je potrebné zabezpečiť, aby nebolo možné zistiť, ako konkrétny volič hlasoval, to znamená preukazovanie totožnosti a samotné hlasovanie musia byť dva technicky oddelené procesy. Digitálna identifikácia si vyžaduje náročné technologické zabezpečenie a považuje sa za jeden z najzložitejších problémov, ktoré je nutné pri zavádzaní elektronického hlasovania vyriešiť.

Významným aspektom elektronických volieb je nenarušenie dôvery verejnosti vo volebný systém, ktorá je základom legitimity štátnej moci. Počiatočné finančné náklady sú vysoké a návratnosť sa očakáva len v dlhodobom výhľade a aj to len vtedy, ak by väčšina voličov skutočne hlasovala elektronicky.

[10] COUNCIL OF EUROPE. E-voting handbook, p. 9.
[11] Dostupné na: www.ss.ca.gov/executive/ivote

3.2 Zásady volebného práva a ich naplnenie

Rovnako ako pri klasických voľbách, aj v prípade elektronických volieb je nevyhnutné dodržiavať zákonné zásady výkonu volebného práva. V tejto časti príspevku uvádzame špecifiká pri ich aplikácii, ktoré vznikajú v súvislosti s virtuálnym prostredím.

Všeobecnosť – Zásada všeobecnosti volebného práva je v elektronickom hlasovaní zabezpečená skutočnosťou, že elektronické voľby predstavujú vždy alternatívu k existujúcim spôsobom hlasovania a nie je vhodné ich legislatívne upraviť ako jediný možný spôsob hlasovania. V opačnom prípade by došlo k problému tzv. digitálneho vylúčenia. Digitálne vylúčenie v tomto konkrétnom prípade znamená, že občania, ktorí nedisponujú potrebnými informačno-komunikačnými prostriedkami alebo nie sú dostatočne digitálne gramotní, nemôžu vykonať svoje volebné právo.

Rovnosť – Ďalším aspektom je rovnosť hlasovania. Tu je potrebné zdôrazniť, že je nevyhnutné znemožniť voličom voliť viac ako jedenkrát a zároveň neumožniť hlasovať tým, ktorí na to nie sú oprávnení, čo súvisí s procesom identifikácie voliča. Rovnako dôležité je zabezpečiť, aby bol každý platný hlas započítaný, nepozmenený alebo neodstránený z hlasovacieho procesu, čo súvisí s bezpečnosťou a spoľahlivosťou elektronického volebného systému. Identifikácia občana by prebiehala prostredníctvom elektronického občianskeho preukazu a sčítanie hlasov by fungovalo na základe princípu obálok za použitia zaručeného elektronického podpisu. Bližšie sa problematikou spôsobu hlasovania zaoberáme v ďalšej podkapitole príspevku.

Priamosť – Ako už bolo uvedené, zásada priamosti znamená, že neexistujú sprostredkovatelia medzi voličmi a kandidátmi, voliči volia priamo kandidátov a kandidáti sú volení priamo voličmi. Tu vzniká problém tzv. rodinného volenia, kde rodinný príslušník môže bez problémov odvoliť za ostatných, najmä starších príbuzných alebo ženy (v niektorých krajinách ide o bežnú realitu) alebo taktiež problém kupčenia hlasov. Tieto riziká možno eliminovať napr. zavedením viacnásobnej možnosti hlasovať. Bližšie sa problematikou spôsobu hlasovania zaoberáme v ďalšej podkapitole príspevku.

Tajnosť – Najproblematickejší aspektom elektronických volieb je dodržanie princípy tajnosti hlasovania. Nekontrolované prostredie Internetu, v rámci ktorého by dochádzalo k výkonu hlasovania, teoreticky umožňuje odtajnenie, fotografovanie alebo spomínané rodinné hlasovanie.

3.3 Spôsob hlasovania

Spôsob, akým volič odovzdáva svoj hlas v elektronickom hlasovaní, je výrazne odlišný od klasických spôsobov. Najzreteľnejší rozdiel spočíva v identifikácii voliča, ktorá sa v prípade elektronických volieb prebiehajúcich mimo volebnej miestnosti musí uskutočniť vo virtuálnom priestore. Pre elektronické zistenie a overenie totožnosti je potrebný počítač alebo iné zariadenie, elektronický občiansky preukaz alebo iná identifikačná karta so zabudovaným čipom a čítačka čipových kariet. Po vložení elektronického občianskeho preukazu do čítačky čipových kariet, za súčasného použitia PIN kódu, dochádza k autentifikovaniu totožnosti občana, a to buď doma alebo vo volebnej miestnosti. Následne sa na obrazovke otvorí príslušná aplikácia, v ktorej sa zobrazí zoznam politických strán a kandidátov. Elektronický hlasovací lístok je zašifrovaný verejným kľúčom (krok analogický s vložením do obálky) a digitálne podpísaný zaručeným elektronickým podpisom voliča (analógia s vložením do návratnej obálky). Zaručený elektronický podpis má podľa Zákona č. 40/1964 Zb. Občiansky zákonník (ďalej len „Občiansky zákonník“) silu vlastnoručného podpisu.[12] V úložisku všetkých hlasov existuje spojenie medzi identitou voliča a jeho zašifrovaným hlasom, avšak po ukončení elektronického hlasovania je táto väzba odstránená a na systém spočítavania hlasov sú prenesené iba zašifrované hlasy bez informácie o identite voliča. Ústredná volebná komisia

[12] Ustanovenie § 40 Občianskeho zákonníka ustanovuje: *„Písomná forma je zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila. Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný zaručeným elektronickým podpisom.“*

potom použije svoj kľúč na dešifrovanie hlasov. Za účelom zamedzenia kupovania hlasov a nátlaku medzi členmi spoločnej domácnosti, je volič oprávnený hlasovanie viackrát zopakovať, pričom sa počíta iba jeho posledný odovzdaný hlas. V prípade, že sa rozhodne neskôr voliť vo volebnej miestnosti, elektronicky odovzdaný hlas sa neberie do úvahy. Toto je možné vďaka faktu, že v úložisku hlasov spočiatku existuje spojenie medzi identitou voliča a jeho zašifrovaným hlasom. Ako už bolo uvedené, toto spojenie po skončení hlasovania zaniká. V prípade viacnásobného hlasovania však existuje polemika, či toto nie je v rozpore s rovnosťou hlasovania, pretože volič má k dispozícii viac možností udelenia hlasu Napriek tomu, že do úvahy sa berie a počíta len jeden hlas, eventuálnym problémom zostáva skutočnosť, že pri klasických voľbách nemôžu občania svoje rozhodnutie zmeniť.

Ďalšou zaujímavou otázkou je problematika potvrdzovania hlasovania. Zatiaľ čo pri klasických voľbách si je volič vedomý svojho rozhodnutia a vie, že do schránky vhadzuje svoj označený hlasovací lístok, pri elektronických voľbách, ktoré fungujú za pomoci technických prístrojov a programov, táto istota bez možnosti overenia hlasovania neexistuje. Doručenie potvrdenia o obsahu hlasovania do elektronickej schránky voliča je z vyššie uvedených dôvodov vylúčené. Jediným prípadom, pri ktorom by bolo možné uvažovať o podobnom potvrdení, je elektronické hlasovanie vo volebnej miestnosti, kde možno voličovi odovzdať po hlasovaní anonymné potvrdenie o tom, ako hlasoval a ktoré by po nahliadnutí vhodil do urny. Iné existujúce možnosti potvrdenia hlasovania sú:

a) *verifikácia voľby tzv. end to end metódou*, pomocou ktorej je voličovi zaslaný číselný kód, ktorého zadaním potvrdzuje svoju voľbu a vzdáva sa budúceho spochybňovania,
b) *opakovaná voľba*, ktorú sme objasnili vyššie.

3.4 Riziká a výzvy

Elektronické voľby sú vo svete sprevádzané kritikou na mnohé riziká, napriek tomu v niektorých štátoch fungujú. V Slovenskej republike sa zatiaľ o tejto metóde hlasovania neuvažuje, preto možno vyhodnocovať iba riziká a výzvy.

Medzi najväčšie výzvy bezpochyby patria pohodlnosť a jednoduchosť vo vzťahu k voličom. Tieto by tiež mohli spôsobiť zvýšenie volebnej účasti, o ktorej sa v čase volieb veľmi často diskutuje. Elektronizáciou volieb možno zlepšiť hlasovanie hendikepovaným osobám a taktiež možno zvýšiť záujem mladých ľudí o tento dôležitý inštitút právneho štátu. Počítačové programy dokážu pomocou systému upozornenia na chybu eliminovať neplatné hlasy a rovnako umožňujú rýchlejšie a objektívnejšie sčítanie hlasov. Vo vzťahu k štátu možno spomenúť zníženie finančných nákladov vynaložených na priebeh volieb a úsporu času.

Kyberpiestor, v ktorom by elektronické hlasovanie prebiehalo, je citlivé prostredie prinášajúce viaceré riziká. V prvom rade sa možno stretnúť s technickým problémami, rôznymi výpadkami sietí, (ne)stabilitou informačných systémov a pod., ktorých vznik v prípade klasických volieb nehrozí. Najslabším článkom je počítač voliča, ktorý nemôže byť kontrolovaný. Servery volebnej komisie musia byť kontrolované, ale riziko útoku nemožno úplne eliminovať. Súvisiacim rizikom je ľudský faktor, a to v podobe hackerov, ktorí dokážu páchať počítačovú kriminalitu veľkých rozmerov. V súvislosti so zásadami volebného práva sú problematickými zásada tajnosti, v rozpore s ktorou sú najmä problémy rodinného hlasovania, a zásada všeobecnosti, ktorá môže byť narušená v prípade digitálneho vylúčenia. Za potenciálne negatívum elektronických volieb možno označiť tiež stratu ich slávnostného charakteru, ktorý tento akt sprevádza od počiatku. V tejto súvislosti dopĺňame, že tento aspekt môže byť vnímaný subjektívne. Celý priebeh elektronických volieb môže pri nedostatočnej legislatívnej a technickej opore postrádať transparentnosť a dôveru verejnosti, ktoré sú významnými aspektmi ovplyvňujúcimi ďalšie smerovanie.

4 ZÁVER

Elektronizáciu volieb možno považovať za významný krok v procese modernizácie spoločnosti. Slovenská republika sa dlhodobo zaraďuje medzi štáty, ktoré majú záujem ponúkať občanom možnosť využívať moderné technológie pri vybavovaní svojich úradných či súdnych záležitostí.

Predkladaný príspevok mal za cieľ poukázať na prienik informačno-komunikačných technológií aj do oblasti výkonu volebného práva, a to najmä v podobe elektronických volieb.

V jednotlivých krajinách sveta je vývoj rôznorodý, avšak za priekopníkov sa považujú Spojené štáty americké a Estónsko.[13] Na základe uskutočnenia analýzy elektronických volieb a ich porovnania s voľbami klasickými a vyhodnotenia pozitívnych a negatívnych stránok možno poskytnúť úvahy o spôsoboch využitia moderných technológií hlasovania v Slovenskej republike.

Pred takou zásadnou zmenou, akou sú elektronické voľby, je potrebné uskutočniť viacero dôležitých krokov. V prvom rade ide o dôkladnú analýzy všetkých oblastí, ktorých sa môže elektronické hlasovanie dotýkať, predovšetkým ide o právnu úpravu a jej zjednotenie. Domnievame sa, že vhodným by bolo tiež zisťovanie záujmu a informovanosti verejnosti v spojitosti so zvyšovaním osvety a digitálnej gramotnosti obyvateľstva. Elektronizácia volieb môže prebiehať po etapách, pričom prvá fáza by mohla byť zameraná na pilotné projekty, napríklad v rámci komunálnych volieb alebo referenda o určitej otázke a neskôr by sa mohlo uvažovať o ďalšom rozširovaní overených postupov. Jedným z konceptov by mohlo byť použitie počítačov pre účely elektronického hlasovania len vo volebných miestnostiach, ktoré by nahradilo papierové hlasovacie lístky a ručné sčítavanie hlasov. Ďalšou alternatívou sú volebné terminály umiestnené v rôznych častiach miest a obcí alebo priklonenie sa k online hlasovaniu so vzdialeným prístupom prostredníctvom siete Internet. V oboch uvedených prípadoch by mohlo dôjsť k vytvoreniu elektronického zoznamu voličov, a to za účelom umožnenia hlasovania v ktorejkoľvek volebnej miestnosti bez ohľadu na trvalý pobyt a bez nutnosti vybavovania voličského preukazu. Slovenská republika vydáva občanom od roku 2013 elektronické občianske preukazy s čipom a bezpečnostným kódom, prostredníctvom ktorých je možné využívať elektronické schránky umiestnené na webovom portály www.slovensko.sk. Z toho dôvodu je na mieste uvažovať o ich využití aj v prostredí volebného práva.

Použitá literatúra

CIBULKA, Ľ. Štátoveda. Bratislava: Právnická fakulta UK, 2013. 280 s. ISBN 9788071603498.
COUNCIL OF EUROPE: E-voting handbook, p. 9.
EUROPEAN COMMISION: Europe´s Electoral Heritage. Strasbourg, 2002.
ORGANIZÁCIA SPOJENÝCH NÁRODOV: Medzinárodný pakt o občianskych a politických právach. New York, 1966.
VÝSKUMNÝ ÚSTAV SPOJOV: Výkladový terminologický slovník elektronických komunikácií.
VLÁDA SLOVENSKEJ REPUBLIKY: Politika informatizácie spoločnosti v Slovenskej republike. Bratislava, 2001.
Zákon č. 40/1964 Zb. Občiansky zákonník.
Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov.
Zákon č. 460/1992 Zb. Ústava Slovenskej republiky.
www.e-politics.cz

Kontaktné údaje:

JUDr. Soňa 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

[13] Prvé elektronické voľby prebehli v Estónsku v roku 2005 (komunálne) a 2007 (parlamentné). Zdroj: http://e-politics.cz/elektronicke-volby-v-estonsku-2/

KYBERNETICKÉ HROZBY A MEDZINÁRODNÁ BEZPEČNOSŤ

Jozef Valuch

Univerzita Komenského v Bratislave, Právnická fakulta

Abstract: The international community is currently facing not only the „traditional threats“ known at the time of signing the UN Charter, but also some new challenges. One of the most important is „cyber threats“. This article deals with this kind of threats and their impact on international security as well as the view and response of the international community to these threats.

Abstrakt: Medzinárodné spoločenstvo čelí v súčasnosti nielen „klasickým hrozbám“ známym už v čase vzniku Charty OSN, ale aj novým výzvam. Medzi najvýznamnejšie z nich patria aj kybernetické hrozby. Príspevok približuje tento druh hrozieb a jeho vplyv na medzinárodnú bezpečnosť, ako i pohľad a reakcie medzinárodného spoločenstva naň.

Key words: cyber threats, international security, cyber attack

Kľúčové slová: kybernetické hrozby, medzinárodná bezpečnosť, kybernetický útok

1 ÚVOD

Na univerzálnej úrovni má v súvislosti s medzinárodnou bezpečnosťou nezastupiteľné miesto Organizácia spojených národov (OSN), ktorej zakladajúcim dokumentom je Charta OSN podpísaná 26. júna 1945.[1] Práve tento dokument ako prvý z cieľov OSN uvádza zachovanie medzinárodného mieru a bezpečnosti.[2] Bezpečnostný systém tejto organizácie je pritom inštitucionalizovaný vo vytvorení jedného z jej hlavných orgánov, ktorým je Bezpečnostná rada. Táto zároveň nesie hlavnú zodpovednosť za zachovanie medzinárodného mieru a bezpečnosti.[3] Od vzniku tejto organizácie však uplynulo už viac ako sedemdesiat rokov a medzinárodné spoločenstvo i jednotlivé štáty musia v súčasnosti čeliť novým výzvam a bezpečnostným hrozbám, ktoré sa od seba líšia vo viacerých ohľadoch a ktoré neboli známe v čase vzniku OSN. O to viac, že Charta OSN prešla doposiaľ len menšími „kozmetickými úpravami“ a jej zásadnejšia reforma je v nedohľadne.

Meniaci sa charakter bezpečnostných hrozieb si uvedomujú i mnohí štátni predstavitelia a uznávané autority, ktorých myšlienky sa „pretavujú“ do medzinárodnoprávnych dokumentov rôznej právnej sily. Jedným z dokumentov súvisiacich s otázkou medzinárodnej bezpečnosti je správa tzv. Panelu na vysokej úrovni s názvom „Bezpečnejší svet: naša spoločná zodpovednosť“.[4] Vypracoval ho tím uznávaných autorít na základe poverenia vtedajšieho generálneho tajomníka OSN Kofiho Annana v roku 2004. Aj táto správa uvádza, že žijeme vo svete nových hrozieb, ktoré nemohli byť

[1] Charta OSN vstúpila do platnosti 24. októbra 1945. Bližšie pozri: GRANT, J., P., BARKER, J. C.: Parry & Grant Encyclopaedic Dictionary of International Law, Third Edition, s. 635

[2] Charta OSN, čl. 1 ods. 1: „Zachovať medzinárodný mier a bezpečnosť a pre tento cieľ robiť účinné kolektívne opatrenia, aby sa predišlo ohrozeniu mieru, odstránilo sa jeho ohrozenie a potlačil každý útočný čin alebo iné porušenie mieru, a v zhode so zásadami spravodlivosti a medzinárodného práva uskutočňovať mierovými prostriedkami úpravu alebo riešenie sporov alebo situácií, ktoré by mohli viesť k porušeniu mieru“.

[3] Charta OSN, čl. 24 ods. 1: „Aby bola zabezpečená rýchla a účinná akcia Organizácie spojených národov, zverujú jej členovia Bezpečnostnej rade hlavnú zodpovednosť za zachovanie medzinárodného mieru a bezpečnosti a uznávajú, že Bezpečnostná rada, plniac svoje povinnosti vyplývajúce pre ňu z tejto zodpovednosti, koná v ich mene.“

[4] *A more secure world: Our shared responsibility*. Report of the Secretary - General's High-level Panel on Threats, Challenges and Change (2004). Dostupné na: http://www.un.org/en/peacebuilding/pdf/historical/hlp_ more_secure_world.pdf (stránka navštívená dňa 4.10.2015)

známe ani predvídané v čase vzniku OSN, teda v roku 1945. Z tohto pohľadu je vhodné uviesť, že správa vymedzuje šesť nasledovných kategórií najvážnejších hrozieb pre medzinárodnú bezpečnosť: medzištátne konflikty, násilie vo vnútri štátov, ekonomické a sociálne hrozby, zbrane hromadného ničenia, terorizmus a medzinárodný organizovaný zločin.[5] Medzičasom aj od predloženia tejto správy uplynulo viac ako desať rokov a pokrok vo vývoji nových technológií a ich dostupnosti nás núti zamyslieť sa nad tým, či vyššie uvedený výpočet je stále aktuálny a dostatočný.

2 KYBERNETICKÉ HROZBY

V porovnaní s minulosťou sa nachádzame v období, kedy informačné technológie prenikajú takmer do všetkých oblastí života, čím sa informácie stávajú dostupnejšími, komunikácia flexibilnejšou a spoločnosť celkovo „rýchlejšou". Na druhej strane sa ale komunikácia a celkovo spoločnosť stáva viac anonymnou a zraniteľnou. Práve pomerne jednoduchá dostupnosť, ale i anonymita a priestorová neuchopiteľnosť informačných technológií spôsobujú, že sa stále väčšia časť aktivít presúva do kybernetického priestoru, umožňujúcemu rýchle a jednoduché splnenie aj nekalých cieľov s minimálnym rizikom postihu. 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. Azda najjednoduchšie a najvýstižnejšie ho charakterizuje to, že funguje vo virtuálnej rovine, ktorú nedokážeme vidieť ani uchopiť. 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.[6]

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 ovládnutiu 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.[7] 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[8], 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.[9] Hrozby tak dnes už nepochádzajú len zo strany dospievajúcich 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",[10] že rozdiel medzi tradičnými aktérmi

[5] Bližšie pozri: VALUCH, J.: Hrozby medzinárodnej bezpečnosti a OSN, s. 543

[6] Bližšie pozri: MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti, s. 55-56

[7] Tamtiež, s. 57; Porovnaj: KRAMER, D.F., STARR, H. S., WENTZ, L. KUEHL,D.: Cyberpower and National Security, 664 s.

[8] *Distributed Denial of Service* (DDoS), bližšie im je pozornosť venovaná v ďalšom texte.

[9] 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 03.10.2015)

[10] *Australian Cyber Security Strategy*, 2009

hrozieb – hackermi, teroristami, organizovanými zločineckými sieťami, priemyselnými špiónmi a zahraničnými spravodajskými službami – sa stále viac stiera.[11]

Z uvedených hrozieb spätých s kybernetickým priestorom sa v ďalšom texte venujeme tým, ktoré majú alebo môžu mať najvýraznejší súvis s medzinárodnou bezpečnosťou, o čom nás presviedčajú viaceré udalosti z posledných rokov.

3 VYBRANÉ PRÍPADY ZNEUŽITIA KYBERNETICKÉHO PRIESTORU

Estónsko (2007)

Ako prvý možno spomenúť prípad z apríla 2007, keď Estónsko čelilo asi tri týždne trvajúcim DDoS útokom, ktoré predstavujú tzv. distribuované odmietnutie služby. Podnetom malo byť rozhodnutie estónskych úradov premiestniť sovietsky vojnový pamätník z centra hlavného mesta Tallinn na vojenský cintorín. Tento čin vyvolal nepokoje ruskej menšiny, ktorej príslušníci vnímali tento pamätník ako pamiatku na vojnové obete a viedlo to až k blokáde estónskeho veľvyslanectva v Moskve. Na druhej strane, Estónci vnímajú tento pamätník ako symbol cudzej okupácie. DDoS útoky zasiahli internetové stránky vládnych inštitúcií a neskôr aj stránky novín, TV staníc, bánk a iných cieľov. Viaceré z napadnutých internetových stránok boli nahradené stránkami s ruskou propagandou alebo falošným ospravedlnením, no väčšina útokov bola zameraná na ich vypnutie. Hovorca estónskeho Ministerstva obrany prirovnal tieto útoky dokonca k tým proti Amerike z 11. septembra 2001. Estónsko tvrdí, že viaceré z prvých útokov pochádzali z ruskej strany, avšak väčšina z nich prichádzala z mnoho tisíc obyčajných počítačov z celého sveta. Viaceré boli prevádzkované súkromnými osobami nahnevanými na Estónsko. Na ruských internetových stránkach boli anonymne rozosielané návody ako tieto DDoS útoky začať. Mnoho ďalších pochádzalo z počítačov napadnutých vírusom s cieľom zapojiť ich do týchto útokov bez vedomia ich majiteľov.[12] Niektoré zdroje hovoria o tom, že v druhej fáze týchto útokov sa na nich podieľalo viac ako milión počítačov z viac ako sto krajín. Celkovo však tieto útoky spôsobili obmedzené ekonomické a komunikačné narušenia, no žiadne výrazné materiálne škody, zranenia, či straty na životoch.[13]

Americká armáda (2008)

V roku 2008 sa cieľom útokov stal informačný systém americkej armády, pričom tento predstavoval príklad kybernetickej špionáže. Použitím obyčajnej zbernice USB, ktorá bola pripojená k armádnemu počítaču na vojenskej základni na Blízkom východe, sa špionážny software nedetekovane šíril v utajovaných ale i neutajovaných systémoch. Táto zbernica sa v takomto prípade stáva numerickým predmostím, z ktorého sú tisíce dátových súborov prenášané do serverov pod cudzou kontrolou. Od tejto udalosti sa kybernetická špionáž stala takmer konštantnou hrozbou a obdobné incidenty sa udiali už vo viacerých členských štátoch NATO.[14]

Rusko – Gruzínsky konflikt (2008)

Kybernetické operácie zamerané proti Gruzínsku sa uskutočnili na prelome júla a augusta 2008, pred a počas ozbrojeného konfliktu s Ruskou Federáciou. Spôsobili, že vládne webové stránky sa dostali do režimu offline a spomalili internetové služby. Najmä bezprostredne pred tým a po tom ako ruské jednotky vstúpili do Gruzínskej provincie Južné Osetsko, niekoľko vládnych webových stránok bolo znefunkčnených a ich obsah bol nahradený anti - Gruzínskou propagandou, zatiaľ čo DDoS útoky znemožnili schopnosť kaukazskej krajiny šíriť informácie. Z týchto počítačových útokov obvinilo Gruzínsko Ruskú Federáciu, ale Rusko to poprelo a tvrdilo, že útoky

[11] 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

[12] The Economist: A Cyber-riot. May 10th 2007, dostupné na: http://www.economist.com/node/9163598, (stránka navštívená dňa 01.10.2015).

[13] ROSCINI, M.: Cyber Operations and the Use of Force in International Law, s. 4-5

[14] NATO Review: Nové hrozby - kybernetické dimenzie, dostupné na: http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm (stránka navštívená 10.10.2015)

sú dielom súkromných osôb, ktorý tak konajú dobrovoľne. Týmto kybernetickým operáciám bola venovaná pozornosť v Správe Nezávislej vyšetrovacej misie o konflikte v Gruzínsku z roku 2009,[15] ktorá však nedospela k záveru o ich pripísateľnosti alebo zákonnosti, ale uvádza, že „ak tieto útoky boli riadené vládou alebo vládami, je pravdepodobné, že táto forma vedenia vojny bola použitá po prvýkrát v medzištátnom ozbrojenom konflikte".[16] Niektoré pramene uvádzajú, že zdrojové umiestnenie uvedenej blokády pochádzalo z piatich anonymných systémov, z ktorých až štyri sa nachádzali v Rusku a len jeden v Turecku a zároveň boli všetky kontrolované zločineckým syndikátom RNB.[17] Práve uvedený prípad nám potvrdzuje, že kybernetický priestor sa stal už aj reálnym dejiskom konfliktov medzi štátmi a popri klasickom vedení ozbrojenej vojny môže zohrávať čoraz väčšiu úlohu aj v budúcnosti.

Irán (2010)

Medzi ciele kybernetických útokov v posledných rokoch patrí aj Irán, pričom viaceré z nich boli spojené s jeho jadrovým programom a výskumom.[18] Jedným z najznámejších je počítačový červ Stuxnet, ktorý bol zameraný na jadrové zariadenia. Ide o jeden z najsofistikovanejších a najinteligentnejších počítačových červov. Objavený bol v druhej polovici roka 2010, ľahko sa šíri prostredníctvom Microsoft Windows a zameriava sa predovšetkým na priemyselný software Siemens a jeho zariadenia. Jeho útok je pomerne jednoduchý. Šíri sa tajne a dokáže zasiahnuť mimoriadne dôležité body v systéme, napr. programy ktoré riadia a monitorujú procesy, alebo sa dokonca starajú o spoluprácu s rôznymi systémami a aplikáciami. Doposiaľ je známych päť rôznych druhov Stuxnetu, ktoré boli zamerané na iránske zariadenia, pričom v dôsledku týchto útokov došlo k poškodeniu iránskeho jadrového programu.[19] Ide o dôkaz ďalšieho kvalitatívneho kroku vpred vo využívaní kybernetických možností vo forme manipulácie dôležitých technických procesov v jadrových zariadeniach v Iráne. A aj napriek tomu, že stanovenie rozsahu škôd je stále nejasné, táto skutočnosť potvrdzuje potenciálne nebezpečenstvo zákerného malwaru, ktorý dokáže zachvátiť dôležité počítačové systémy, riadiace zásobovanie energetickými zdrojmi alebo dopravné siete. Práve v tomto prípade bol po prvýkrát získaný skutočný dôkaz existencie kybernetických útokov, ktoré spôsobujú potenciálne reálne fyzické škody a ohrozujú ľudské životy.[20] Aj na základe uvedeného možno konštatovať, že Stuxnet je prvou svetovou kybernetickou zbraňou geopolitického významu.[21]

---

[15] *Report of the Independent Fact-Finding Mission on the Conflict in Georgia*

[16] ROSCINI, M.: Cyber Operations and the Use of Force in International Law, s. 7-8, porovnaj: *Report of the Independent Fact-Finding Mission on the Conflict in Georgia*, September 2009, Vol II, s. 217–19, dostupné na: http://www.ceiig.ch/Report.html, (stránka navštívená dňa 10.10.2015)

[17] *The Russian Business Network* je ruskou kybernetickou kriminálnou organizáciou špecializujúcou sa predovšetkým na krádeže identít za účelom ich ďalšieho predaja. RBN vznikla ako poskytovateľ internetových služieb pre detskú pornografiu, phishing, spam a malware s fyzickým sídlom v meste Petrohrad. MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti, s. 59. Porovnaj: SMITH, J., D.: Russian Cyber Strategy and the War Against Georgia, January 17, 2014, dostupné na: http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia, (stránka navštívená dňa 03.10.2015)

[18] Samotná otázka iránskeho jadrového programu je pritom pomerne zložitá a má za sebou už dlhoročný vývoj. Bližšie k iránskemu jadrovému programu pozri napr.: VALUCH, J.: Jadrová otázka, Irán a medzinárodné právo, s. 484-492

[19] MACKOVÁ, V.: Cyber War of the States: Stuxnet and Flame Virus Opens New Era of War, s. 5., dostupné na: http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova-PP-No.-15-2013-Vol.-2.pdf, (stránka navštívená dňa 04.10.2015)

[20] NATO Review: Nové hrozby - kybernetické dimenzie, dostupné na: http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm (stránka navštívená 10.10.2015)

[21] MACKOVÁ, V.: Cyber War of the States: Stuxnet and Flame Virus Opens New Era of War, s. 7, dostupné na: http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova-PP-No.-15-2013-Vol.-2.pdf, (stránka navštívená dňa 04.10.2015)

Rok 2015

Z posledných udalostí možno spomenúť útok skupiny hlásiacej sa k Islamskému štátu (ISIS), ktorá sa zamerala na Twitter účet a YouTube kanál Centrálneho veliteľstva americkej armády. Centrálne veliteľstvo je súčasťou americkej armády zodpovednej za regióny sveta, kde sa môžu konať bojové operácie – v tomto prípade ide o dvadsať krajín vrátane Afganistanu, Iránu, Iraku, Saudskej Arábie a Sýrie. Vedľa hesla „Nezastavíme sa! Vieme o tebe všetko!“ sa objavili mená a telefónne čísla vojenského personálu. Ďalšie sociálne médium zobrazovalo kanceláriu s ľuďmi v uniforme, pričom šlo pravdepodobne o fotku urobenú web kamerou. Ďalšia zobrazená správa znela v duchu „Cyberkalifát pokračuje vo svojom Cyberdžiháde.“ Na stránke YouTube spätej s Centrálnym veliteľstvom sa v hornej časti objavil obrázok muža v šatke s vetou „milujem ťa ISIS“. Uvedené účty Twitter a YouTube boli pozastavené a zástupca Pentagonu sa vyjadril, že uvedené síce vyvolalo rozpaky, ale nepreukázalo sa, že by išlo o bezpečnostnú hrozbu.[22]

4 REAKCIA MEDZINÁRODNÉHO SPOLOČENSTVA A VYBRANÝCH ŠTÁTOV

Uvedené príklady sú len výberom z prípadov zneužitia kybernetického priestoru a reálnu skúsenosť s takýmito zásahmi majú aj mnohé ďalšie štáty. To podnietilo aj medzinárodné spoločenstvo, jednotlivé regionálne zoskupenia či organizácie, reagovať na tento druh hrozby, či už formou prijímania potrebných právnych noriem, budovania príslušných kapacít alebo zintenzívnením medzinárodnej spolupráce. Z pohľadu Slovenskej republiky považujeme za vhodné na tomto mieste priblížiť predovšetkým kroky Organizácie Severoatlantickej zmluvy (NATO) a Európskej únie (EÚ).

NATO

NATO predstavuje medzinárodnú organizáciu vojensko – politickej povahy, ktorá združuje krajiny s cieľom spolupráce v oblasti bezpečnosti. Prostredníctvom inštitútu kolektívnej obrany poskytuje členským štátom ochranu ako politickými, tak aj vojenskými prostriedkami.[23] Nové formy hrozieb nemohli preto zostať zo strany tejto organizácie nepovšimnutými a viaceré jej strategické dokumenty považujú kybernetický priestor za novú operačnú doménu. Spomenúť možno „Strategickú koncepciu NATO“[24] schválenú na Lisabonskom samite v roku 2010. V zmysle tejto koncepcie sú kybernetické útoky jednou z kľúčových hrozieb súčasnosti. Vyskytujú sa stále častejšie a sú schopné dosiahnuť úroveň, ktorá ohrozí národnú a euroatlantickú prosperitu, bezpečnosť a stabilitu. Zdrojom takýchto útokov môžu byť zahraničné vojenské a spravodajské služby, teroristické a extrémistické skupiny, ale aj organizovaní či individuálni zločinci.

V roku 2011 bola špeciálne pre oblasť kybernetickej obrany NATO prijatá „Stratégia kybernetickej obrany NATO“[25], ktorá definuje úlohy a aktivity v oblasti kybernetickej obrany, ktoré musí táto organizácia v budúcnosti rozvíjať. K tejto stratégii bol prijatý „Akčný plán kybernetickej obrany NATO“[26] konkretizujúci úlohy a prostriedky na dosiahnutie cieľov kybernetickej obrany. Uvedená stratégia bola v máji 2014 aktualizovaná dokumentom „Posilnená stratégia kybernetickej obrany NATO“[27] a na samite vo Walese bol schválený aj aktualizovaný „Akčný plán kybernetickej obrany NATO“. Tento stanovuje konkrétne úlohy za účelom naplnenia vyššie uvedenej politiky,

[22] Načasovanie bolo v tomto prípade zaujímavé. V danom období prezident USA Barack Obama prezentoval nové veľké plány týkajúce sa kybernetickej bezpečnosti, ktoré boli navrhnuté tak, aby uistil Američanov, že rok po útoku na Sony Pictures sú ich osobné informácie na internete v bezpečí. LEE, D.: Top US military Twitter feed 'hacked by Islamic State', 12 Jan 2015, dostupné na: http://www.bbc.co.uk/newsbeat/article/30781377/top-us-military-twitter-feed-hacked-by-islamic-state (stránka navštívená dňa 09.10.2015). V roku 2014 boli totiž napadnuté filmové štúdiá Sony Pictures Entertainment, z ktorých unikli mnohé významné dokumenty o filmoch, osobnostiach a prístupových údajoch. Útok bol pripisovaný Severnej Kórei v súvislosti s tým, že štúdiá pripravovali film, v ktorom mal zomrieť severokórejský vodca.

[23] VALUCH, J., RIŠOVÁ, M., SEMAN, R.: Právo medzinárodných organizácií, s. 289

[24] *Strategic Concept for the Defence and Security of the Members of the NATO, 2010*

[25] *NATO Policy on Cyber Defence, 2011*

[26] *NATO Cyber Defence Action Plan*

[27] *Enhanced NATO Policy on Cyber Defence, 2014*

pričom jednou z kľúčových úloh je posilnenie vzájomnej spolupráce medzi štátnym sektorom, súkromným sektorom a akademickou obcou.[28]

Práve vyššie uvedené útoky v Estónsku v roku 2007 mali totiž mimo iného za následok nastolenie zásadnej otázky v Bruseli: „*ak je komunikačné centrum členského štátu napadnuté raketou, nazýva sa to vojnovým aktom. Ako ale nazveme situáciu, keď je rovnaké zariadenie vyradené z prevádzky v dôsledku kybernetického útoku?*“[29] Následkom toho generálny tajomník NATO Fogh Rasmussen po rokovaní vo Walese uviedol: *„Dnes deklarujeme, že kybernetická obrana je súčasťou kolektívnej obrany“.* Uvedené rozhodnutie je posunom v tradičnom chápaní kolektívnej obrany NATO, pretože doteraz sa tento článok o kolektívnej obrane[30] vzťahoval na klasické konvenčné a jadrové hrozby a len minimálne bol spájaný s novými bezpečnostnými výzvami. Lídri členských krajín NATO sa tak dohodli, že kybernetický útok na niektorého z členov by mohol byť považovaný za útok na celú Alianciu, a mohol by teda podnietiť vojenskú odpoveď.[31]

Európska únia

Na potrebu zabezpečenia kybernetickej bezpečnosti reaguje aj EÚ. Spomedzi jej aktuálnejších krokov v tejto oblasti možno uviesť dokument s názvom „Stratégia kybernetickej bezpečnosti Európskej únie“[32], ktorý predstavuje víziu EÚ vo vzťahu k predchádzaniu kybernetickým narušeniam a útokom a tiež protiopatrenia k nim. Cieľom je zvyšovanie odolnosti informačných systémov voči kybernetickým útokom a posilňovanie politiky EÚ v oblasti medzinárodnej kybernetickej bezpečnosti a kybernetickej obrany. V nadväznosti na uvedené Európska rada schválila úlohu spracovať „Politický rámec pre kybernetickú obranu“, ktorý bol schválený na zasadnutí ministrov obrany v novembri 2014. Jeho základnými cieľmi sú podpora rozvoja kybernetickej obrany členských štátov, podpora misií a operácií Spoločnej obrannej a bezpečnostnej politiky, veda a výskum, synergie aj s ostatnými aktérmi mimo EÚ, hlavne NATO. Podstatné v tejto súvislosti je, že bezpečnosť kybernetického priestoru má predstavovať jednu z hlavných priorít budúcej zahraničnej politiky EÚ v oblasti bezpečnosti.[33]

---

[28] Koncepcia kybernetickej bezpečnosti Slovenskej republiky, s. 8-9. Materiál dostupný na: https://lt.justice.gov.sk/Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645& docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240, (stránka navštívená dňa 03.10.2015)

[29] The Economist: A Cyber-riot. May 10th 2007, dostupné na: http://www.economist.com/node/9163598, (stránka navštívená dňa 01.10.2015).

[30] Článok 5 Severoatlantickej zmluvy znie: „Zmluvné strany sa dohodli, že ozbrojený útok proti jednej alebo viacerým z nich v Európe alebo Severnej Amerike sa bude považovať za útok proti všetkým, a preto odsúhlasili, že ak nastane taký ozbrojený útok, každá z nich uplatní právo na individuálnu alebo kolektívnu obranu uznané článkom 51 Charty Spojených národov, pomôže zmluvnej strane alebo zmluvným stranám takto napadnutým tým, že bezodkladne podnikne sama a v súlade s ostatnými stranami takú akciu, akú bude považovať za potrebnú, vrátane použitia ozbrojenej sily s cieľom obnoviť a udržať bezpečnosť v severoatlantickej oblasti. Akýkoľvek taký ozbrojený útok a všetky opatrenia vykonané v jeho dôsledku sa bezodkladne oznámia Bezpečnostnej rade. Tieto opatrenia budú ukončené, len čo Bezpečnostná rada prijme opatrenia potrebné na obnovenie a zachovanie medzinárodného mieru a bezpečnosti.“

[31] MASARIKOVÁ, M.: Potvrdené. Kyberútoky predmetom článku 5 NATO. 05.09.2014. Dostupné na: http://www.cybersec.sk/spravy/politika/potvrdene-kyberutoky-predmetom-clanku-5-nato/, (stránka navštívená dňa 02.10.2015)

[32] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* JOIN(2013) 1 final, Brussel 2013.

[33] *An outline for Europen Cyber Diplomacy Engagement*, 9967/4/14 REV 4, DG D 1C, Brusel, september 2014. EÚ vykonáva činnosti aj v oblasti ochrany občanov pred on-line kriminalitou, o čom svedčí napr. zriadenie Európskeho centra pre boj proti počítačovej kriminalite, ktoré je súčasťou Európskeho policajného úradu (Europol) a tiež spustenie Globálnej aliancie proti sexuálnemu zneužívaniu detí on-line. Kľúčovou súčasťou celkovej stratégie kybernetickej bezpečnosti je pripravovaná smernica o bezpečnosti sietí a informácií (Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii, COM (2013) 48 FINAL, Brusel, 2013). Koncepcia kybernetickej bezpečnosti Slovenskej

Globálny index kybernetickej bezpečnosti

V súvislosti s kybernetickými hrozbami zverejnilo Svetové ekonomické fórum rebríček krajín, ktorý by mal odrážať ich schopnosť čeliť tomuto typu hrozieb. Už v roku 2012 spustilo Svetové ekonomické fórum iniciatívu „*Partnership for Cyber Resilience*“, ktorá zahŕňa viac ako sto súkromných a štátnych inštitúcií a jej cieľom je zvyšovanie povedomia o kybernetických rizikách a posilnenie spolupráce pri ochrane pred nimi. Jedným z výsledkov tejto iniciatívy je Globálny index kybernetickej bezpečnosti,[34] ktorý meria úroveň rozvinutosti kybernetickej bezpečnosti vo všetkých štátoch sveta. Je výsledkom spolupráce medzinárodnej organizácie (Medzinárodná telekomunikačná únia) a predstaviteľa súkromného sektora. Pri zostavovaní rebríčka bola pozornosť zameraná na päť kľúčových oblastí – právne (legislatívne) opatrenia, technické a organizačné opatrenia, medzinárodnú spoluprácu a budovanie kapacít. Uvedených päť ukazovateľov vytvára index, ktorý odzrkadľuje pripravenosť krajiny v oblasti kybernetickej bezpečnosti.

Na prvom mieste sa umiestnili Spojené štáty americké, na druhom Kanada a na treťom sú spoločne Austrália, Malajzia a Omán. Spomedzi európskych krajín sa najvyššie umiestnilo Nórsko, ktoré sa spolu s Novým Zélandom delí o štvrtú priečku.

Slovenská republika sa spolu s Hong Kongom, Fínskom, Katarom a Uruguajom umiestnila na ôsmom mieste. Nakoľko však môže byť na jednej priečke umiestnených aj viacero štátov, reálne nás predbehlo dvadsaťdva krajín, z toho osem členov EÚ. Posledné miesto patrí Somálsku.

Spomedzi regiónov je po spriemerovaní jednotlivých výsledkov na prvom mieste Európa a na poslednom Afrika.[35]

Spojené štáty americké

Jedným z najaktuálnejších materiálov týkajúcich sa kybernetických hrozieb je dokument prezentovaný riaditeľom Národnej spravodajskej služby Spojených štátov amerických, Jamesom R. Clapperom v septembri 2015 s názvom „Celosvetové kybernetické hrozby.“[36] Mimo iného sa v tomto dokumente konštatuje, že kybernetické hrozby majú stúpajúcu frekvenciu, sofistikovanosť a intenzitu zásahu. Rozširuje sa aj okruh aktérov kybernetických hrozieb, metódy útokov, ciele a obete. Je pravdepodobné, že i naďalej budú prebiehať snahy o narušenie jednotlivých systémov, avšak „katastrofický útok“ je v súčasnosti považovaný za nepravdepodobný. Skôr než „kybernetický armagedon“, ktorý by ochromil celú americkú infraštruktúru, sa očakáva séria kybernetických útokov na nízkej až strednej úrovni, pochádzajúcich z rôznych zdrojov. Uvedený dokument rozlišuje vo vzťahu k USA nasledovných aktérov týchto hrozieb:

a) štáty s vysoko sofistikovanými kybernetickými programami (napr. Rusko alebo Čína),
b) štáty s menšími technickými vymoženosťami, ale možno horším zámerom (napr. Irán alebo Severná Kórea),
c) ziskom motivovaní zločinci,
d) ideologicky motivovaní hackeri alebo extrémisti.

Rozlišovanie medzi štátnymi a neštátnymi aktérmi v rámci jednej krajiny je pritom mimoriadne náročné, najmä keď spolupracujú (či už aktívne alebo mlčky), prehliadajú trestnú činnosť ktorá poškodzuje zahraničné obete, alebo využívajú podobné kybernetické nástroje.[37]

---

republiky, s. 9-10. Materiál dostupný na: https://lt.justice.gov.sk/Attachment/Vlastn%C3%BD%20materi%C3%A1ldocx.pdf?InstEID=1&attEID=75645&docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240, (stránka navštívená dňa 03.10.2015)

[34] *Global Cybersecurity Index & Cyberwellness Profiles*, April 2015, materiál je dostupný na: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (stránka navštívená dňa 02.10.2015)

[35] CYBERSEC: Najlepšie sú na kybernetické hrozby pripravené USA, Slováci sú na ôsmom mieste, 11.08.2015, dostupné na: http://www.cybersec.sk/spravy/politika/najlepsie-su-na-kyberneticke-hrozby-pripravene-usa-slovaci-su-na-osmom-mieste/ (stránka navštívená dňa 02.10.2015)

[36] *Worldwide Cyber Threats*, September 10, 2015

[37] CLAPPER, R., J.: Worldwide Cyber Threats, September 10, 2015, materiál je dostupný na: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ClapperOpening09102015.pdf (stránka navštívená dňa 03.10.2015)

Slovenská republika

Aj Slovenská republika si je vedomá skutočnosti, že nastáva zmena globálneho bezpečnostného prostredia a stúpa výskyt a sofistikovanosť asymetrických hrozieb, medzi ktoré patrí aj zneužitie kybernetického priestoru. Kybernetickú bezpečnosť preto vníma aj ako podsystém národnej bezpečnosti a kybernetický priestor ako novú operačnú doménu. To odzrkadľuje aj dokument s názvom „Koncepcia kybernetickej bezpečnosti Slovenskej republiky" (ďalej len „Koncepcia"). Samotná kybernetická bezpečnosť je v tomto dokumente charakterizovaná ako „*schopnosť ľubovoľnej elektronickej komunikačnej siete, elektronického informačného alebo riadiaceho systému odolávať náhodným udalostiam a škodlivým aktivitám, ktoré môžu negatívne ovplyvniť integritu, dôvernosť a dostupnosť uchovávaných, spracovávaných, alebo prenášaných dát a služieb poskytovaných prostredníctvom siete, informačného, alebo riadiaceho systému a tým narušiť, alebo negatívne ovplyvniť funkčnosť najmä niektorej oblasti kritickej infraštruktúry*."[38]

Napriek tomu, že v Globálnom indexe kybernetickej bezpečnosti sa Slovenská republika umiestnila na ôsmom mieste (viď text vyššie), Koncepcia uvádza, že problematika kybernetickej bezpečnosti na našej národnej strategickej úrovni ešte nie je vyriešená uceleným a konzistentným spôsobom. Možno však uviesť niekoľko ďalších dokumentov týkajúcich sa kybernetickej bezpečnosti v podmienkach Slovenskej republiky: „Národná stratégia pre informačnú bezpečnosť"[39] a nadväzujúci „Akčný plán informačnej bezpečnosti."[40] Ďalším je napr. materiál s názvom „Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany, vyplývajúcich z cieľov spôsobilostí Slovenskej republiky."[41] Tento definuje spôsobilosti nášho štátu v oblasti kybernetickej obrany, ktoré bude potrebné vybudovať a rozvíjať do konca roka 2017. Pre Národný bezpečnostný úrad z tohto dokumentu napr. vyplýva úloha zabezpečiť a koordinovať vybudovanie spôsobilostí v oblasti kybernetickej obrany.

Samozrejme, na medzinárodnej úrovni sa Slovenská republika ako člen relevantných štruktúr (napr. EÚ a NATO) zúčastňuje aj na rôznych aktivitách. Napríklad na kybernetických cvičeniach (*Cyber Coalition*, *Locked Shields*, *Cyber Europe* a pod.) preverujúcich reakcie na kybernetické útoky. Spolupracuje s Centrom výnimočnosti pre oblasť spoločnej kybernetickej obrany[42] v estónskom Tallinne, Európskou agentúrou pre sieťovú a informačnú bezpečnosť[43] a s nedávno vzniknutým Centrom pre boj proti počítačovej kriminalite.[44]

Z Koncepcie vyplýva, že za hlavné oblasti kybernetickej bezpečnosti sú považované:

- všeobecná bezpečnosť elektronických sietí vrátane správy internetu,
- ochrana kritickej informačnej infraštruktúry,
- kybernetický boj a reakcia na kybernetický útok,
- kybernetická kriminalita,
- kybernetický terorizmus,
- bezpečnosť elektronického obchodu,
- ochrana osobných údajov a súkromia,
- ochrana pred nevyžiadanou elektronickou poštou,
- ochrana pred kybernetickou špionážou.

Práve od týchto oblastí sa následne odvíjajú úrovne pripravenosti v rámci kybernetickej bezpečnosti, pripravenosť na prípadnú kybernetickú kriminalitu a útok, obzvlášť na útok podstatný pre národnú bezpečnosť.

---

[38] Koncepcia kybernetickej bezpečnosti Slovenskej republiky, materiál dostupný na: https://lt.justice.gov.sk/ Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645&docEID=413095&matEID=7996& langEID=1&tStamp=20150218154455240 (stránka navštívená dňa 03.10.2015)

[39] Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č. 570/2008.

[40] Vláda Slovenskej republiky materiál (č. mat. ÚV-30315/2009) schválila 19. januára 2010 uznesením č. 46/2010.

[41] Vláda Slovenskej republiky materiál (č. mat. UV-V-226/2014) schválila 2. októbra 2014 uznesením č. 497/2014.

[42] *NATO Cooperative Cyber Defence Centre of Excellence*, NATO CCD COE

[43] *European Union Agency for Network and Information Security Agency*, ENISA

[44] *European Cybercrime Centre*; EC3

V dôsledku kybernetických hrozieb môže dôjsť k ohrozeniu nasledovných základných bezpečnostných oblastí fungovania štátu:

- bezpečnostné záujmy Slovenskej republiky v zahraničnej a obrannej politike,
- ochrana ústavného zriadenia, verejného poriadku, bezpečnosť občana a štátu,
- sociálna stabilita štátu,
- ekonomická stabilita štátu,
- ochrana životného prostredia.

Vo vzťahu k Slovenskej republike Koncepcia uvádza, že najvážnejším problémom v oblasti kybernetickej bezpečnosti je skutočnosť, že táto ešte nie je výslovne a komplexne ošetrená v platnej legislatíve, v dôsledku čoho sa odporúča vypracovať Návrh zákona o kybernetickej bezpečnosti a Návrh Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2019.[45]

5 KYBERNETICKÝ ÚTOK A JEHO VZŤAH K *IUS AD BELLUM* A *IUS IN BELLO*

Z vyššie uvedeného vymedzenia vyplýva, že jednou z hlavných oblastí kybernetickej bezpečnosti je aj reakcia na kybernetický útok. Na tomto mieste sa preto pokúsime v stručnosti priblížiť vzťah tohto druhu útoku k *ius ad bellum* ako aj *ius in bello*. 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,[46] vypracovaný v roku 2012. Ide o výsledok činnosti nezávislých expertov, ktorý nemá záväzný charakter. Pozostáva z dvoch častí – časť A je venovaná kybernetickej bezpečnosti a *ius ad bellum* a časť B sa zaoberá *ius in bello* alebo právom ozbrojených konfliktov.[47] Základný rámec pre priblíženie uvedeného vzťahu preto vyplýva z analýzy ustanovení Tallinnského manuálu a relevantných rozhodnutí Medzinárodného súdneho dvora (ďalej len „MSD“).

Z posudku MSD o nukleárnych zbraniach[48] vyplýva, že právo ozbrojených konfliktov sa aplikuje na akékoľvek použitie sily, bez ohľadu na použité zbrane.[49] Pre samotné posúdenie, či je kybernetický útok použitím sily v zmysle čl. 2 ods. 4 Charty OSN môže byť nápomocný prípad Nikaragua,[50] v ktorom MSD určil, že rozhodujúcimi faktormi pri určení existencie ozbrojeného konfliktu sú účinky a rozsah kybernetickej operácie. Z toho dôvodu by nedeštruktívne kybernetické operácie, ktoré sú zamerané napr. na podkopanie dôvery vlády alebo ekonomickej situácie, nebolo možné kvalifikovať ako kybernetické útoky s použitím sily.[51] Na základe uvedeného možno vidieť odlišnosti vo vyššie opísaných prípadoch ku ktorým došlo v Estónsku v r. 2007 a v Gruzínsku v r. 2008. V prípade Estónska totiž útoky nedosiahli úroveň ozbrojeného útoku a preto nedošlo k aplikácii medzinárodného práva ozbrojených konfliktov. Na druhej strane operácie počas Rusko – Gruzínskeho konfliktu boli vykonané s cieľom jeho podpory a na tieto sa aplikovalo medzinárodné právo ozbrojených konfliktov. Jednalo sa o kybernetické operácie vykonané v kontexte ozbrojeného konfliktu, pričom kybernetické operácie zahŕňajú kybernetické útoky, no nie sú obmedzené len na ne. Uvedené potvrdzuje aj Tallinnský manuál keď uvádza, že na kybernetické operácie sa aplikuje právo ozbrojených konfliktov, pokiaľ boli vykonané v kontexte ozbrojeného konfliktu, či medzinárodného alebo nemedzinárodného.[52]

---

[45] Koncepcia kybernetickej bezpečnosti Slovenskej republiky, materiál dostupný na: https://lt.justice.gov.sk/ Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645&docEID=413095&matEID=7996& langEID=1&tStamp=20150218154455240 (stránka navštívená dňa 03.10.2015)

[46] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2012

[47] GÁBRIŠ, T.: Cyber Law, s.174

[48] Posudok Medzinárodného súdneho dvora o legalite hrozby alebo použitia nukleárnych zbraní z 8. júla 1996, ods. 39.

[49] ŠMIGOVÁ, K.: Kybernetické útoky a medzinárodné právo, s. 1225

[50] Rozsudok Medzinárodného súdneho dvora z 27. júna 1986 vo veci Vojenské a polovojenské aktivity v a proti Nikarague, Nikaragua v. USA, ods. 195

[51] ŠMIGOVÁ, K.: Kybernetické útoky a medzinárodné právo, s. 1226

[52] Tamtiež, s. 1227

6 ZÁVER

V súčasnosti už niet pochýb o tom, že nastáva zmena globálneho bezpečnostného prostredia. Do popredia nastupujú nové výzvy a bezpečnostné hrozby, ktoré sa od seba líšia vo viacerých ohľadoch a ktoré neboli a ani nemohli byť známe v čase konštituovania OSN. Napriek tomu najvýznamnejším nástrojom v oblasti ochrany bezpečnosti na univerzálnej úrovni stále zostáva rámec stanovený Chartou OSN.

Príkladom nového druhu hrozieb sú kybernetické hrozby, ktoré idú ruka v ruke s rozvojom a dostupnosťou informačných technológií. Kybernetický priestor totiž poskytuje okrem množstva výhod aj možnosti pre rozmanité hrozby a informačnú kriminalitu, ktoré zahŕňajú širokú škálu negatívnych fenoménov rôzneho stupňa závažnosti.

O tom, že hrozby v kybernetickom priestore predstavujú jednu z kľúčových výziev súčasnosti nás presviedčajú aj prípady uvedené v tomto príspevku: či už ide o kybernetickú špionáž zameranú na informačný systém americkej armády v r. 2008, Rusko - Gruzínsky konflikt v roku 2008, počas ktorého sa kybernetický priestor stal už reálnym dejiskom konfliktu medzi štátmi, alebo o počítačový červ Stuxnet, nasadený na iránsky jadrový program v r. 2010, ktorý je mnohými považovaný za prvú kybernetickú zbraň geopolitického významu a pod.

Okrem dotknutých štátov si vážnosť situácie uvedomuje aj medzinárodné spoločenstvo a jednotlivé zoskupenia štátov, ktoré v tomto smere prijímajú opatrenia a dokumenty rôzneho významu a právnej sily. Členské krajiny NATO sa dokonca uzniesli na tom, že kybernetická obrana je súčasťou kolektívnej obrany, čo predstavuje posun v tradičnom chápaní kolektívnej obrany tejto organizácie.

V súvislosti s kybernetickými hrozbami dokonca Svetové ekonomické fórum zverejnilo rebríček krajín, ktorý by mal odrážať ich schopnosť čeliť tomuto typu hrozieb, tzv. Globálny index kybernetickej bezpečnosti. Na prvom mieste sa umiestnili Spojené štáty americké, a na poslednom mieste Somálsko. Slovenskej republike patrí ôsma priečka a to aj napriek tomu, že v Koncepcii kybernetickej bezpečnosti Slovenskej republiky sa uvádza, že problematika kybernetickej bezpečnosti na našej národnej strategickej úrovni ešte nie je vyriešená uceleným a konzistentným spôsobom. Zároveň táto Koncepcia mimo iného konštatuje, že jednou z hlavných oblastí kybernetickej bezpečnosti je aj reakcia na kybernetický útok. Z toho dôvodu bol predmetom nášho záujmu aj vzťah tohto druhu útoku a práva ozbrojených konfliktov. Zaujímavým zdrojom odpovedí je tzv. Tallinnský manuál, ktorý je výsledkom trojročného skúmania ako aplikovať existujúce normy medzinárodného práva na tento nový druh vedenia vojny.

Použitá literatúra:

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,

KRAMER, D.F., STARR, H. S., WENTZ, L. KUEHL,D.: Cyberpower and National Security. National Defense University: Potomac Books Inc., 2009,

MACKOVÁ, V.: Cyber War of the States: Stuxnet and Flame Virus Opens New Era of War. In: CENAA Policy Papers No. 15/2013, Vol. 2,

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

ROSCINI, M.: Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014,

ŠMIGOVÁ, K.: Kybernetické útoky a medzinárodné právo. In: Bratislavské právnické fórum 2013. Bratislava: Univerzita Komenského, Právnická fakulta, 2013, s. 1224-1230

VALUCH, J., RIŠOVÁ, M., SEMAN, R.: Právo medzinárodných organizácií. Praha: C. H. Beck, 2011,

VALUCH, J.: Hrozby medzinárodnej bezpečnosti a OSN. In: Míľniky práva v stredoeurópskom priestore 2008. Bratislava: Vydavateľské oddelenie Praf UK, 2008,

VALUCH, J.: Jadrová otázka, Irán a medzinárodné právo. In: Ekonomické, politické a právne otázky medzinárodných vzťahov. Bratislava: Ekonóm, 2006, s. 484-492

Internetové zdroje:
CLAPPER, R., J.: Worldwide Cyber Threats, September 10, 2015, materiál je dostupný na: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ClapperOpening09102015.pdf
CYBERSEC: Najlepšie sú na kybernetické hrozby pripravené USA, Slováci sú na ôsmom mieste, 11.08.2015, dostupné na: http://www.cybersec.sk/spravy/politika/najlepsie-su-na-kybernetické-hrozby-pripravene-usa-slovaci-su-na-osmom-mieste/
LEE, D.: Top US military Twitter feed 'hacked by Islamic State', 12 Jan 2015, dostupné na: http://www.bbc.co.uk/newsbeat/article/30781377/top-us-military-twitter-feed-hacked-by-islamic-state
MASARIKOVÁ, M.: Potvrdené. Kyberútoky predmetom článku 5 NATO. 05.09.2014. Dostupné na: http://www.cybersec.sk/spravy/politika/potvrdene-kyberutoky-predmetom-clanku-5-nato/,
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
NATO Review: Nové hrozby - kybernetické dimenzie, dostupné na: http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm
SMITH, J., D.: Russian Cyber Strategy and the War Against Georgia, January 17, 2014, dostupné na: http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia,
The Economist: A Cyber-riot. May 10th 2007, dostupné na: http://www.economist.com/node/9163598,
Dokumenty:
A more secure world: Our shared responsibility. Report of the Secretary - General's High-level Panel on Threats, Challenges and Change (2004).
An outline for Europen Cyber Diplomacy Engagement, 9967/4/14 REV 4, DG D 1C, Brussels, september 2014.
Australian Government, Cyber Security Strategy, 2009,
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final, Brussel 2013.
Enhanced NATO Policy on Cyber Defence, 2014
Global Cybersecurity Index & Cyberwellness Profiles, April 2015,
Charta OSN,
Koncepcia kybernetickej bezpečnosti Slovenskej republiky,
NATO Cyber Defence Action Plan
NATO Policy on Cyber Defence, 2011
Report of the Independent Fact-Finding Mission on the Conflict in Georgia, September 2009, Vol II,
Severoatlantická zmluva
Strategic Concept for the Defence and Security of the Members of the NATO, 2010
Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012
Súdne rozhodnutia:
Posudok Medzinárodného súdneho dvora o legalite hrozby alebo použitia nukleárnych zbraní z 8. júla 1996.
Rozsudok Medzinárodného súdneho dvora z 27. júna 1986 vo veci Vojenské a polovojenské aktivity v a proti Nikaragua, Nikaragua v. USA.

Kontaktné údaje:

JUDr. Jozef Valuch, PhD.
jozef.valuch@flaw.uniba.sk
Právnická fakulta Univerzity Komenského v Bratislave
Šafárikovo nám. č. 6
810 00 Bratislava
Slovenská republika

THE RIGHT TO BE FORGOTTEN IN THE ERA OF "DIGITAL" INFORMATION

Anna Lucia Valvo, Kore University of Enna

Abstract: The right to be forgotten is not expressively disciplined neither at statutory level nor at constitutional level. It has been described by jurisprudence as a particular declension of the personal identity protection, which consists in the autonomous right that the person himself is represented in a way to reflect the actual social and personal dimension and in the right not to be publically represented in a different way from the one that used to be in the past.

Due to the absence of a proper legal discipline and the legislative vacuum in the field, the question has been the subject of different jurisprudential tendencies of the Supreme Court of Italy, the European Court of Human Rights and the European Court of Justice. The issues connected to the right to be forgotten firstappeared when the most relevant daily newspapers started to digitalize their historic paper archives and convert them into on-line archives. Consequently,old articles, accessible in the past only in forgotten archives by interested persons, are nowadays available for everyone and can be easily consultedat every moment.

In recent years, the number of cases which requested the removal or updating of the article by direct intervention of the provider of the search engine have increased, in order to assure the full respect of what is called the right of digital identity. Nevertheless, an identity of opinions among national and international Courts on the question actually does not exist.

Key words: internet; personal identity; right to be forgotten.

1. INTRODUCTION

The right to be forgotten, not expressively provided for neither at ordinary legislation nor at constitutional level, has been considered by the jurisprudence as a particular evolution of the protection of personal identity, which consists in the autonomous right that the person itself be represented in a way able to reflect the actual social and personal dimension. Or, in other terms, it consists in the right not to be publically represented in a manner not corresponding anymore to the past representation[1].

Since the Decision no. 3679/98 of the Civil Chamber, the Italian Supreme Court makes express reference to the right to be forgotten underlying that the need to take under consideration " … a new dimension of the right to privacy recently defined also as the right to be forgotten intended as a legitimate interest of any person not to remain indeterminately exposed to further offenses directed to his honor and reputation caused by the reiterated publication of news legitimately divulged in the past".

The lack of any proper legal discipline and the substantial *vacuum* of a legislative level in this field have been the object of attention by the Italian Supreme Court, the European Court of Human Rights and the European Court of Justice. This one, by Decision of 13 May 29014 (case C-131/12) and in clear countertendency with the orientations of the other two Courts mentioned above (in countertendency also with the opinion of the General Advocate JÄÄSKINEN), surprised almost everybody deciding that it is possible to ask the search engine to remove the contested data[2].

The issue of the right to be forgotten appeared from the moment when important newspapers began to digitalize the proper historical paper archives and published them on-line. With the consequence that old articles, which were in the past consultable in the paper archives only by who

---

∗ Full Professor of European Union Law at the Faculty of Legal and Economic Sciences, University "Kore" of Enna, Sicily. Lawyer in Rome, Italy.

[1]SeeS. SICA and V. ZENO ZENCOVICH, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, 2010, p. 387.

[2] At thisregard, seeF. PIZZETTI, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, in *federalismi.it*, n. 1, 2014.

might have a direct interest (provided that he had memory of them) are nowadays available for everybody at every moment[3].

Furthermore, the automatic mechanisms of article indexing by the mean of the search engines make the news accessible by everyone whomay easily know previous news about the person only by composing the name of the interested person as a key word.

The consequence of that is thatany persons who has been protagonist of incidents, even of judiciary nature, concluded in positive way, continue to see the proper name connected to outdated cases which do not reflect the actual situationanymore.

In the recent years, the number of cases which requested the removal or updating of the article by direct intervention of the provider of the search engine have increased, in order to assure the full respect of what is called the right of digital identity[4].Nevertheless,a common consensus among national and international Courts on the questionactually does not exist.

It is necessary to underline that, inthe equilibrium of opposite interests -freedom of expression and right to privacy or to digital identity - a particular attention is paid by the European Court of Human Rights to one of the most fundamental principles of any democratic system, i.e. the freedom of expression. Moreover, the Court identifies in a *post scriptum*, which recognizes the fact that the article at issue has been considered libelous, the right solution for an adequate balance between right to information and actual representation of the personal identity.

2. By Decision of 16 July of 2013[5], the IV Chamber of the European Court of Human Rights, considered totally inappropriate the pretension to prevalence of the right sanctioned in art. 8 of the ECHR of 1950, which sanctions the right to private (and family) life, over the right sanctioned in art. 10 of the same Convention relative to the freedom of expression[6].

The case raises from an article concerning two Polish lawyers, appeared in a newspaper, considered libelous by the Tribunal and, nevertheless, at the time still traceable in the website of the newspaper. The two lawyers, in reason of the fact that the libelous article was present in the Google search engine and that, due to the automatic indexing mechanisms anyone who might compose their names could became aware of the facts reported in the article at issue, with the aggravating that the on-line version of this article could amplify the damages in reason of the potential greater number of readers, asked for the removal of the article from the search engine database[7].

The request for removal, had been rejected and the involved persons presented compliant in front of the European Court of Human Rights, claiming the violation of the right to privacy and reputation, as sanctioned in art. 8 of ECHR.

In the quoted decision, the Court of Strasbourg, based on numerous precedent practice, reaffirms the need to find a balance point between the right to private life and to freedom of expression, In fact, the right of expression under art. 10represent one of the cornerstone principles of the democratic society and in this context it must be kept in due consideration the protections

[3]SeeG. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, 2010, p. 395.

[4] See, in this sense, G. E.VIGEVANI, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *federalismi.it*, n. 2, 2014, which underlines how it is "… emerging an instance of identification of a "right to digital identity", intended as a right of the individual to obtain the rectification, the contextualization, the progressive updating in time and, in some cases, even the de-indexing and the removal of personal data from websites, at the purposes to guarantee a correct and actual representation of the proper identity and to guarantee the right to be forgotten".

[5] Case no. 33846/07, *Wegrzynowski-Smolczewskiv.Poland*.

[6] Not specifically in the field of the right to be forgotten but on the necessity to find a balance point between counterposed rights provided for in arts. 8 and 10 of ECHR, seeL. SEMINARA, *Libertà di espressione e internet. Riflessioni sulla sentenza della Corte europea dei diritti dell'uomo Delfi AS C. Estonia*, in *KorEuropa*, 3, 2013, p. 282 ss., availableat*http://www.koreuropa.eu*.

[7] From his point of view, the website editor replied that the collocation of the article in the digital archive of the website was a sufficient measure to render the readers awareness of the fact that the article had been published in the past and that the history cannot be cancelled.

guaranteed to the press organizations. However, the press should restrain its articles within the limits of the respect for others reputations.

With regard to internet, the Court reaffirms that this important instrument of communication is not and could not be compared to the printed press. Moreover, in the awareness of the fact that through the news broadcasted by the mean of internet the risk to violate human rights and fundamental freedoms is greater (mostly with regard to private and family rights), the norms enacted in protection of the internet regulation should be distinguished by those regulating the traditional press[8].

Nevertheless, the Court considers that in the balance between the counterposed interests that emerge with regard to the conservation of the news in the online archives, there is no excessive interference in the right to freedom of expression if a judge imposes the publication of an endnote - attached to the article conserved in the archive -specifying that an action for defamation is pending with regard to the article itself.

In the specific case, the Court considered absolutely reasonable the decision of the Court of Appeal of Warsaw to add, in the article at issue, an informative endnote by which the public could have been aware of the positive ending of the defamation legal actions previously brought forward by the applicants. This indication could have adequately balanced the conflicting interests.

However, considering that the applicants had not requested any rectification nor any updating of the news, but rather asked for a total removal of the data from the digital archive, the Court, considering inexistent the violation of art. 8 of the ECHR, rejected the application. This on the grounds that, on the one hand, the State had respected the duty to balance the rights respectively sanctioned by arts. 8 and 10 of the Rome Convention and, on the other hand, the limitation of the freedom of expression - for the purposes of the protection of the reputation of the individual - might have been inadequate according to art. 10 of the ECHR[9].

3. In the same interpretative sense of the European Court of Human Rights moves the second Civil Committee of the Appeal Court of Milan which, by Decision no. 335 of 27 January 2014[10], sanctioned the duty of the publisher of the online newspaper to update and rectify the news contained in the proper website through the addition of precise reference about any finding of libel of the news at issue, provided that, obviously, the interested person has asked for such an action[11].

In fact, the case can be briefly summarized in the following terms: an article already published in a printed newspaper and found defamatory was also visible online in the digital archive of the newspaper. The offended party requested the Milan Court of Appeal to decide the removal of that article from the digital archive or, in the alternative, the insertion of a link containing the libelous content of the article at issue or, again, the cancellation of any reference to the company name to the offended party. This beside the reparation of the damages.

Considering that the insertion of an article in the digital archive of a newspaper could not be equalized to the republishing of the same article, the Civil Tribunal of Milan of first instance, by the mean of Decision no. 4527/10, rejected the application.

The decision of first instance was appealed before the Court of Appeal of Milan, which, by the mentioned Decision 335/14 in modification of the first instance Decision, condemned the

[8] About the internet archives, the Court underlines the important function carried out by them in the conservation and locating of the news, constantly set at disposition of the users. To this purpose, the Court has always ascertained that the internet archives fall within the application perimeter of the guarantees provided for in art. 10 of ECHR and constitute an important source for the historical research.

[9] See, at this regard, the comment note of 19 August 2013 of F. BUFFA, *CEDU, cancellazionedeidatidiffamatoridagliarchivi internet*, available at *www.magistraturademocratica.it*.

[10] At *Foro.it*., 2014, I, 2612.

[11] As emerges from the decision at issue, the Court of Appeal of Milan established that "if the publishing in a newspaper of an article is followed by the insertion of this article in the digital archive of the newspaper, the forthcoming declaration of defamation of the published article implies the duty, for the newspaper publisher and the holder of the relative digital archive, to update and rectify, upon request of the interested person, the information available online by mentioning the libeling character of that information".

publisher, imposing him to insertan automatic link on the margin of the article at issue in order to give cognizance of the libelous content of such an article.

The logical-argumentative *iter* followed by the judges of the Appellate Court is based essentially on the Decision no. 5525/12 of the Italian Supreme Court which, with regard to an analogous case of an article situated in the digital archive of a newspaper – but not found defamatory in its content -, decided for the right to update and the contextualization of the information situated in the digital archive,in order to protect the personal and social identity of the interested person.

The Court of Appeal of Milan, therefore, following the orientations of the Supreme Court, used to accept the appeal on the grounds that, if for a non libelous article the right to updating of the news (in order to render the reader aware on the case) was recognized, this right had to be recognized also for articles of defamatory content sanctioned by definitive judicial decision.

In the same direction of the Supreme Court case law, the Court of Appeal clarified also that the question should not be addressed in terms of republishing of the news, but rather in terms of maintaining the news in the digital memory of the web, because "the fundaments of the right of updating the news lies, definitively, in the interest of constitutional nature to the protection of the moral or personal identity of the individual in its social perspective".

4. Equally important is the above mentioned decision of the Supreme Court, which recognized the right "to be forgotten" (as a right to the protection of an actual moral and personal identity) of a well-known public personalitywho, several years after some judicial concerns he was personally involved in, used to continue, by virtue of the automatic indexing mechanisms of the web engine search, to find the proper name connected to the old concerns.

The request of the protagonist of this case "to remove an article published years before in a certain area of a web site not indexed by the web search engines" had been rejected by the Authority for the privacy, as well as by the Tribunal of first instance. This one stated, in particular, that the very function of an archive is exactly the one to render available the historical memory of important happenings (and of public interest) of a certain period through documents drawn up in the exercise of the right to journalistic reporting.

The Tribunal and the Authority for the privacy arrived at these conclusions on the grounds that, in parallel with the legitimate interest to non further publication of news of the past in which one might have been involved, has to be taken into consideration the public interest to the cognizance and divulgation of those news for particular exigencies of historical, didactical or cultural nature. Subsequently, a past news might assume historical importance and, under this particular profile, its permanence in archives different from the original one (as the historical one)could be justified[12].

In particular, the Authority, in consideration of the nature of the web - which permits the spreading of a plurality of personal data referred to the same person in relation to past happenings - and in consideration of the obsolescenceof the news, recognized that the immediate and continuous connection of the person to the happening at issue may bring to a disproportionate sacrifice of his rights[13].

[12] At this regard, the Italian jurisprudence has often confirmed that the right to journalistic reporting is legitimately exercised and may prevail over the right to privacy if any public interest exists and is actual for the purposes of the cognizance and diffusion of the news. This if the fact narrated result true after appropriate controls, and if the phrases used to diffuse the news seem to be exemplary under a formal profile. Under the Italian legislation, therefore, the right to journalistic reporting is always balanced with the right to privacy and it is destined to prevail over the latter, provided that exists a public interest to the cognizance (or memory) to the news.

[13] In the wake of such considerations the Authority has requested, as a measure for the protection of the rights of the applicant, that the website containing the personal data of the applicant is de-indexed and removed from the direct individualization through common search engines, while remaining this web-page unaltered in the context of the archive and digitally consultable by accessing the editor's website. See the measure of 12 April 2012 (*doc. web* n. 1894581); 19 July 2012 (*doc. web* n. 2065905); 4 October 2012 (*doc. web* n. 2104293); 18 October 2012 (*doc. web* n. 2130029).

The Supreme Court followed a different reasoning. In fact, although in the quoted decisionthe Court has recognized the existence of a public interest at the publication of the news, it has underlined the importance of the right to privacy under the Privacy Code. According to the code, in effect, the personal data should be treated in a legal and correct way; should be collected for legal purposes; should be real andpertinent; should never exceed the proper finalities; if the case, should be updated and not conserved for a long period of time superior to the one needed for those finalities.

However, provided that the "interested person has participated in the utilization of the proper personal data",he has the right that the information meet the criteria of proportionality, necessity, pertinence to the aim, exactness and coherence with his actual and effective moral and personal identity. He has also the right to know who possesses his data, which kind of data he possesses and, eventually, to contest their usage and treatment, as well as the right to request the removal, the transformation, the block, the rectification, the updating and the integration of the data[14].

Furthermore, the Supreme Court founded on the principle of correctness the exigency of a fair balance reconciliation among opposite interests: on the one hand, the freedom of press and the right to inform in general and, on the other hand, the right to privacy,that implies the prohibition of the divulgation of news which, in consideration of the time expired, result forgotten or, anyway, unknown for a large number of persons[15].

In other terms, the right to be forgotten protects the interest of the individuals that a news, previously of public interest but no more of such nature because of the time passed, is deleted from the web search engines or is contextualized through its insertion in the so-called historical archive[16]. This because the involved person has the right to see his moral and personal identity respected and not to see "misrepresented or altered externally the proper professional, ideological, religious, social, political and intellectual patrimony[17]. Therefore, the person involved has the right to see his image represented as it is in the actuality of the historical moment (the Supreme Court speaks about the right to contextualization and updating of the news)[18].

Nevertheless the Supreme Court, having decided about the necessity to protectpersonal data, establishesalso the modalities for a concrete realization of this protection and postulates a necessary distinction between archive and memory of the web. At this regard, the Court underlines that, unlike an ordinary archive, internet is a "place" completely de-contextualized and *non-*

[14] See, in this sense, art. 7, par. 3, lett. a) and b), of the legislative Decree of 30 June 2003, n. 196. To thisregard, seeS. NIGER, *Il diritto all'oblio*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identitàpersonale*, Padova, 2008, p. 68.

[15] As stated in the judgment, the judges of legitimacy clarify that "in this context, an essential importance assumes the balance between counterposed rights and fundamental liberties, having taking under consideration at this regard the quality of fundamental right assumed by the right to personal data protection, sanctioned in arts. 21 and 22 of the Constitution, as well as by art. 8 of the Charter of the Fundamental Rights of the EU, as a right to maintain the control over proper data that, belonging to *everybody*, (Legislative Decree No. 196 of 2003, art. 1) and to *every person* (art. 8 of the Charter), in various contexts and spaces of life, 'contributes to delineate the structure of a society respectful towards the others and their dignity in a context of equality'" (Cass., /1/2011, n. 186)

[16] The essence of the right to be forgotten has well been summarized by the Supreme Court in the following terms: "Provided that the treatment of personal data may concern even public or publicized data (see. Cass., 25/6/2004, n. 11864), the right to be forgotten safeguards the social projection of the personal identity, the exigency of the subject to be protected from the divulgation of (potentially) harmful information" in reason of the loss (considering the lapse of time passed from the happening of the fact that constitutes the object) of actuality of the same. So that the relative treatment becomes not justifiable anymore and even susceptible to impede the subject in the enjoyment and the explication of the proper personality".

[17] See, at this regard, the judgment of the Supreme Court of 22 June 1985, No. 7769.

[18]See, G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Il diritto dell'informazione e dell'informatica*, 2012, p. 383.

temporal[19], in relation to which the quality, the correctness and the reliability of the news is always to be verified.

The decision seems to be particularly interesting considering that, in perspective, it tends to relieve from any responsibility the manager of the search engine (because he "does not exercises any active role") and to confer this responsibility *in toto* to the "owners of the websites", which may have well copied and conserved (i.e. archived) what could have been already cancelled by the search engines managers[20].

In the specific instance, the judges of the Supreme Court observe how Google, as search engine, just hosts in its servers the internet websitesmanaged, in full autonomy,by their proper owners. Therefore, is on the owners that remains the duty to guarantee the "contextualization and updating of the news object of information and treatment, in order to protect the subject, whose data belong, in connection withhis moral and personal identity as well as his social projection, and to safeguard the right of the citizen-users to receive a complete and correct information".

Furthermore, the Supreme Court reaffirms, on the one hand, that internet has to be considered a "pure storage of archives"[21] and that the memorization of the data in the web is of exclusive responsibility of the "owners of the websites producing the information – so-called source sites". On the other hand, the Court states that the person whose data are involved has to see recognized his right to be forgotten, that is the right to control in order to protect his own social image. This even in case of true news, allthe more so if they are old news, with the consequent, necessary pretension to the contextualization and updating of the data and, eventually, to the cancellation of the same. This always taking into account the exigency to conserve the news in the historical archive in reason of the public interest on the information involved[22].

Beyond any consideration over the right to be forgotten[23], it is necessary to underline, for what here interests of the conclusions of the Supreme Court[24], the substantial exoneration from the

---

[19] At pg. 7 of the judgment at issue is stated that "In the Internet the information is not organized and structured, but result isolated, all placed in the same level ("flattened") without any evaluation of the relative weight, and short of any contextualization, short of connection with other publicized information …".

[20] In other terms, according to the view of the Court, the internet search engine does not play any active role but plays exclusively a mere digital intermediary role, "which offers an automatic system of data location and information through key words, a mere database that indexes the text on the network and offers to the users access for consultation".

[21] In the Decision the judges of the Court distinguish between archive and memory of web and clarify that, in effect, there is no archiving in the web, but a memorization of the information which, as such, are not isolated as it should be if, to the contrary, were effectively archived.

[22] Of particular interest seem to be the conclusions of the Judges of the legitimacy, which summarize their point of view specifying that "in case, as the present, of transfer … of journal news … in the proper historical archive, the holder of the information media (in this case, the company) which by the mean of a search engine (in this case, *Google*) memorizes the news even in the web is obliged to observe the criteria of proportionality, necessity, pertinence and non exaggeration of the information, considering the finalities permitted by the licit data treatment, as well as to guarantee the contextualization and the updating of the old news object of information and treatment, to the benefit of the right of the subject to whom the data concern the moral and personal identity in his social projection, as well as for the safeguard of the right of the single user to receive a complete and correct information, not being in this case sufficient the mere and generic possibility to find within the 'internet sea' further news concerning the specific case, but requesting, given the recognized and persistent public interest to the cognizance of the news at issue, the predisposition of a system able to signal (in the text or in the footnote) the existence the following and the sort of that news, and by facilitating the rapid and easy access by the users to the purposes of the relative adequate deepening …"

[23] The right to be forgotten is object of European discipline under discussion. Just to remind the Regulation proposal of the European Parliament and the Council concerning the protection of the natural persons with regard to personal data treatment and free movement of these data (general Regulation on personal data protection) of 25 January 2012 (COM 2012) 11 final.), which regulates the right to be forgotten at art. 17. To this purpose, see G.BUSIA, *Le frontieredella*privacy *in internet.*

responsibility of the ISP that manages the search engine and, conversely, the exclusive responsibility to the expense of the owner of the website hosted by the search engine.

Ultimately, the duty to control the licit treatment of personal data belongs exclusively to the owner of the website rather than to the ISP, to which in any case could be attributed any role of preventive control or, worse, of censure of all the information inserted in the web platform.

5. The Decision of the Court of Justice (*Case C131-12*)of 13 May 2014, better known as *Google Spain Case*[25], is in clear countertendency with the decision of the Italian Supreme Court with regard to the responsibility of the ISP that manages a search engine, and overturns the conclusions of the General Advocate JÄÄSKINEN. In the mentioned decision the Court of Justice states that the request for de-indexing of proper data has to be directed to the search enginemanager[26], andthe right to private life and protection of personal data, referred to in arts. 7 and 8 of the Fundamental Charter of Human Rights of the EU, prevails over the freedom of economic nature (of the search engine) and over the interest of the users to have access at the information in internet. In this way, the Court of Justice places itself in a opposite positions with what decided by the Court of Strasbourg.

Object of cognizance of the Court of Justice in the Case 131-12, called to decide preliminary after a petition of *Audiencia Nacional*, is the relationship between the European discipline on the personal data - as referred to in the Directive 95/46/EC - and the ISP that manages a search engine, *Google* in the concrete case.

Even in this case emerges the right to be forgotten and, therefore, the right of every citizen to obtain the removal, from the search engine, of any connection generated by the system to news dating back in time and became outdated or even inaccurate[27].

What is relevant, even in this case, is the individuation of the responsible of data treatment and, therefore, of the holder of the obligation to remove, actualize or historicize the data themselves.

La nuova corsa all'oro per i dati personali, in *Diritto e policy per i nuovi media*, a cura di BERTOLINI – LUBELLO – POLLICINO, Roma, 2013, p. 36 ff.

[24] At this regard, in the wake of the just mentioned judgment, the Authority for the Privacy accepted two appeals by sanctioning to the expenses the publisher and stating the obligation to point out the following of the news by the use of an endnote, in order to reconcile both the right of the reader to a complete and reliable information and the right of the involved person to the actualization of his identity. In other terms, in the decisions of 20 December 2012 (doc. *web* n. 2286432) and of 24 January 2013 (doc. *web* n. 2286820), the Authority has recognized the right of the affected person *to obtain the updating/integration of proper personal data when events and successive happenings (adequately documented) have altered the situations object of journalistic news (although at the time correct) affecting significantly the profile and the image of the involved person*; right which has been qualified as *indispensable corollary of the recognized lawfulness of the conservation of journalistic news at the time published* in the web as historical archives and which has to be guaranteed by the Authority as *fully included among the legal positions operated on the grounds of art. 7 of the Code.* In the same measure, by Judgment no. 5820/13 the Tribunal of Milan, recognizing the right to be forgotten of the applicant and denying the relevance of public interest in relation to the permanence in the web of the contested article, ordered the removal of the mentioned article from the digital archive of the newspaper. At this regard, see the comment note of 29 July 2013 of MANNA, *Internet e dirittoall'oblio: unarecentesentenza del Tribunale di Milano*, available at *www.diritto24.ilsole24ore.com*.

[25] The text of the Decision is available at the website of the European Court of Justice *http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT*.

[26] Following the Decision at issue, Google search engine predisposed an application form by the mean of which one can request the removal of proper personal data.

[27] In good substance, the object of the protection is the right not to suffer *ad libitum* the consequences deriving from the diffusion of any news, legitimately published in the past, not actual any more. On the right to be forgotten see also the Report of ENISA of November 2012 "The rightto be forgotten – between expectations and practice" available at *www.enisa.europa.eu.*

The case originates from the request of a Spanish citizen who tried to obtain, by*Google* and by the publisher, the removal of his personal data published in an online newspaper article, considered from this citizen no more actual.

On the compliant of the applicant,the Spanish Agency for Data Protection (*Agencia Española de Protección de Datos* - AEPD) by accepting the requests of the applicant, ordered *Google Inc*. and *Google Spain* to remove the concerned data from the search engine and to deny the access in the future. This on the basis that *Google Spain*, since established in the territory of the European Union, is bound by the EU *Directive* on the protection of personal data and, therefore, by the national legislation of adaption[28].

In turn, *Google Inc*. and its Spanish branch contested this decision in front of the *Audiencia Nacional* underlining the inapplicability of the European discipline because, while the first is the holder of the data treatment[29], the second just cares the commercialization of the advertising spaces. Moreover, the injunction of the AEPD constituted an excessive interference in the freedom of expression of the internet site managers, and identified the way to protect the right to be forgotten in the intervention on the original sites subject to indexing.

The *Audiencia Nacional,* for the purposes of the internal decision, referred the question for a preliminary ruling in front of the European Court of Justice asking if the *Directive* 95/46/EC could apply to the provider not directly resident in the EU territory when its services are directed even to citizens of the EU. The *Audiencia Nacional*also asked which was the role of the provider in the treatment of the data and if there existed an issue of the right to be forgotten, as pretended by the holder of personal data.

In his conclusions, the General Advocate of the ECJ explained that the search engine could be considered in any way a holder of the treatment of personal data situated in the websites that he indexes[30]. This because the furniture of a service for the localization of the information does not determine any control over the content of this information and, therefore, does not imply the cognizance of the content itself, with the consequence that the search engine is not able to distinguish various types of data.Subsequently, there isn't any obligation for the search engine to remove, de-index data or cancel connections to those data.

In addition, according to the General Advocate, there is no generalized right to be forgotten ascribable to arts. 7 and 8 of the Charter of the Fundamental Rights of the EU and, in any case, the removal of the information from website by the search engine would constitute an inappropriate interference over the freedom of expression if not a real act of preventive censorship perpetuated by a private.

An opposite standpoint emerges in the case law of the ECJ which considered that the European discipline on the data protection is applicable to the search engines established in the EU. Furthermore, the activity of a search engine has to be qualified, for the ECJ, as "data treatment" and, for this reason, the search engine manager should respect the European discipline on data protection, accept the requests of the applicants and, if the case, remove from the list of the results of the search over the name of a person the link connecting to the websites which contain information related to the person involved.

With regard to the right to be forgotten, the decision establishes that, if certain criteria are met, in the balancing between the right to privacy and to data protection and the right to the freedom of information, it is the latter that has to be sacrificed at the purpose to guarantee the rights previously mentioned.

The decision of the Court of Justice, that can be accepted in some ways, provokes, for other reasons, doubts and perplexities over the effective cognizance by the judges of Luxembourg of the

[28] In the Press release of the European Court of Justice no. 77/13 of 25 June 2013, available at *www.curia.europa.eu*, is reported that "The complaint against the publisher was instead rejected, since the publication on the newspaper was legally justified".

[29]*Google Inc*. objected the applicability, towards itself, of the European Directive and the internal legislation of adaptation, due to the fact that the registered office was situated in California.

[30]The figure of the responsible of data treatment is described by art. 4, par. 1, lett. *f*), of the Privacy Code. Is up to him the decision power on the finalities, the modalities of the treatment and the instruments used. To this regard, see the Decision of the III criminal Section of the Supreme Court no. 5107/14 relative to the *Case Google/Vivi Down*.

functioning of internet and the difference between a *internet service provider* and a website holder. Moreover, uncertainties arise with respect tothe apocalyptic scenarios which may appear in terms of preventive censorship, violation of the principle of freedom of *internet*, violation of the principle of freedom of expression and so on.

Nevertheless, if it is true that a swallow does not make a summer, it is also true that an isolated judgment of the Court of Justice does not make law. Anyway, the judges of the Court should acquire awarenessthat, in the era of post-globalization, the transmission and the circulation of the knowledge constitute a useful instrument for the divulgation of typical essential values of every democratic system, as well as an instrument for the purposes of the achievement of a better cultural, social and economicdevelopment of the people.

Contact information:
Anna Lucia Valvo is Full Professor of European Union Law at the Faculty of Economic and Legal Sciences, University “Kore” of Enna, Italy. Lawyer in Rome, (annavalvo@virgilio.it).

NIEKOĽKO POZNÁMOK K POĽSKEJ ÚPRAVE ZAKLADANIA OSOBNÝCH SPOLOČNOSTÍ V TELEINFORMATICKOM SYSTÉME

Mateusz Żaba

Sliezska univerzita v Katoviciach, Fakulta práva a administrácie

Abstract: This paper deals with the legal regulation of setting up commercial partnerships in ICT system that was implemented into Polish Code of Commercial Partnerships and Compnies in Amendment Act of 28.11.2014. The main subject refers to the issue of using the standarized electronic forms which are available in ICT system. The article deliberates the matter of creating the content of the deed of general partnership and also limited partnership. The concern of active capacity to conclude the articles of partnership deed in ICT system has been also discussed in this paper.

Abstrakt: Tento príspevok sa venuje právnej úprave zakladania osobných spoločností v teleinformatickom systéme, ktorá bola zavedená novelou poľského Zákonníka obchodných spoločností zo dňa 28.11.2014. Hlavným predmetom záujmu je otázka využitia štandardizovaných elektronických vzorov, ktoré sú dostupné v teleinformatickom systéme. Článok rozoberá možnosť formovať obsah spoločenskej zmluvy o založení verejnej obchodnej spoločnosti ako aj komanditnej spoločnosti. V tomto príspevku bola tiež prerokovaná otázka aktívnej legitimácie na uzavretie zmluvy osobnej spoločnosti v teleinformatickom systéme.

Key words: standardized electronic forms, commercial partnerships, setting up the partnerships, ICT system, Polish law.

Kľúčové slová: štandardizované elektronické vzory, osobné spoločnosti, zakladanie osobných spoločností, teleinformatický systém, poľské právo.

1 ÚVOD

Najnovšie zmeny poľského Zákonníka obchodných spoločností (poľ. *Kodeks spółek handlowych*)[1], ktoré boli zavedené zákonom zo dňa 28.11.2014, sú pokusom realizovať tzv. „digitálnu reformu“ práva spoločností a rozšíriť možnosť využitia elektronických komunikačných systémov pre zakladanie, organizáciu a fungovanie obchodných spoločností. Hlavným motívom novelizácie bolo umožniť širšie využitie elektronických vzorov sprístupnených v teleinformatickom systéme. Doposiaľ bolo využitie elektronických vzorov možné len v prípade spoločnosti s ručením obmedzeným (poľ. *spółka z ograniczoną odpowiedzialnością*) a týkalo sa iba situácie zakladania tejto spoločnosti[2]. Predošlé zmeny, ktoré sa vzťahovali na poľskú spoločnosť s ručením obmedzeným, boli iniciované novelou poľského ZOS zo dňa 1.4.2011 a vstúpili do platnosti ešte 1.1.2012. Cieľom nových predpisov je predovšetkým informatizácia procesov uzatvárania, zmeny a zrušenia zmlúv osobných spoločností – verejnej obchodnej spoločnosti a komanditnej spoločnosti – ako aj elektronická registrácia týchto zmien v Štátnom súdnom registri (poľ. *Krajowy Rejestr*

[1] Ustawa z dnia 15.9.2000 – Kodeks spółek handlowych (Dz. U. Z 2013 r., poz. 1030 ze zm.), ďalej tiež ako: **poľský ZOS**.

[2] Bližšie na túto tému pozri: SZUMAŃSKI, A.: Nowelizacja kodeksu spółek handlowych z 28.11.2014 r. przewidująca szersze wykorzystanie wzorca udostępnianego w systemie teleinformatycznym. In: Przegląd Prawa Handlowego, 2015, č. 4, s. 38.

Sądowy)[3]. Novelizácia poľského ZOS zo dňa 28.11.2014 nadobudla čiastočnú účinnosť už 15.1.2015, ale jeho podstatná časť bude platiť od 1.4.2016. Tu je potrebné podčiarknuť, že tieto predpisy, ktoré sa týkajú osobných spoločností, ktoré boli zavedené do poľského ZOS, zostávajú mimo rozsahu regulácie Európskej únie. Okrem toho vyššie uvedené zmeny vzťahujúce sa na poľskú spoločnosť s ručením obmedzeným neporušujú predpisy Smerníc 2009/101/ES[4] a 2013/34/EÚ[5].

Poľský Zákonník obchodných spoločností predvída štyri druhy osobných spoločností: verejnú obchodnú spoločnosť (poľ. *spółka jawna*), partnerskú spoločnosť (poľ. *spółka partnerska*), komanditnú spoločnosť (poľ. *spółka komandytowa*) a komanditno-akciovú spoločnosť (poľ. *spółka komandytowo-akcyjna*). Podľa právnej úpravy prijatej poľským zákonodarcom, osobné spoločnosti nie sú právnické osoby. V poľskom právnom poriadku jestvuje okrem fyzických osôb a právnických osôb aj tretia kategória subjektov. Osobné spoločnosti patria medzi tzv. organizačné jednotky, ktoré nie sú právnické osoby, ale ktorým bola na základe zákona udelená spôsobilosť mať práva a povinností[6].

Problematika novelizácie, ktorá sa vzťahuje na možnosť uzatvoriť spoločenskú zmluvu osobnej spoločnosti pri využití vzorov zmlúv sprístupnených v teleinformatickom systéme, nie je častým predmetom diskusie v doktríne. Niektorí autori poukazujú nato, že jedine výber dvoch zo štyroch druhov osobných spoločností, aké sú predvídané v predpisoch poľského ZOS, treba uznať ako „náhodný" a fakt, že novela poľského ZOS neobsiahla partnerskú spoločnosť a komanditno-akciovú spoločnosť, je nedôslednosťou poľského zákonodarcu[7]. S týmto názorom nie je možné úplne súhlasiť, lebo je potrebné zobrať do úvahy, že partnerská spoločnosť je tvorená osobami, ktoré vykonávajú hospodársku činnosť v rámci profesionálnych povolaní a jednou z nevyhnutných podmienok na registráciu takejto spoločnosti je predloženie dokladu, ktorý potvrdí, že daný spoločník vykonáva takéto profesionálne povolanie[8]. Predloženie tohto dokladu je fyzicky nemožné v prípade registrácie spoločnosti v teleinformatickom systéme. Vyžadovalo by si to totiž takú informatizáciu databáz, v akých sú uložené informácie týkajúce sa osôb, ako aj ich oprávnení vykonávať profesionálne povolanie, aby bol zaistený voľný pohyb informácií priamo do Štátneho súdneho registra. Okrem toho treba pamätať na to, že komanditno-akciová spoločnosť nie je tak častou formou podnikania ako verejná obchodná spoločnosť či komanditná spoločnosť.

K tomu sa žiada podčiarknuť, že proces zakladania a organizácie osobných spoločností – inak než v prípade kapitálových spoločností – je silno individualizovaný vzhľadom na prevahu osobných zväzkov nad majetkovými vzťahmi medzi spoločníkmi. Poľskí autori zdôrazňujú, že organizačná štruktúra a spôsob fungovania verejnej obchodnej spoločnosti, ako aj komanditnej spoločnosti sú také unikátne, že slúžia často na realizáciu výnimočných hospodárskych

[3] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 4.

[4] Smernica Európskeho parlamentu a Rady 2009/101/ES zo 16.9.2009 o koordinácii záruk, ktoré sa od obchodných spoločností v zmysle článku 48 druhého odseku zmluvy vyžadujú v členských štátoch na ochranu záujmov spoločníkov a tretích osôb s cieľom zabezpečiť rovnocennosť týchto záruk

[5] Smernica Európskeho parlamentu a Rady 2013/34/EÚ z 26.6.2013 o ročných účtovných závierkach konsolidovaných účtovných závierkach a súvisiacich správach určitých druhov podnikov, ktorou sa mení smernica Európskeho parlamentu a Rady 2006/43/ES a zrušujú smernice Rady 78/660/EHS a 83/349/EHS

[6] Presne po poľsky: „*jednostki organizacyjne niebędące osobami prawnymi, którym ustawa nadaje zdolność prawną*". Pozri: STRZĘPKA J. A., ZIELIŃSKA E., in STRZĘPKA J. A. (red.): Kodeks spółek handlowych. Komentarz, Warszawa: C.H. Beck, 2013, s. 59. WACH, M.: Status ułomnych osób prawnych w polskim prawie cywilnym, Warszawa: C.H. Beck, 2008, 506 s.

[7] SZUMAŃSKI, A.: Nowelizacja kodeksu spółek handlowych z 28.11.2014 r. przewidująca szersze wykorzystanie wzorca udostępnianego w systemie teleinformatycznym. In: Przegląd Prawa Handlowego, 2015, č. 4, s. 39 ako aj KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 6.

[8] Pozri čl. 93 § 2 poľského ZOS

a profesionálnych účelov účastníkov[9]. Vzhľadom na komplikovanosť vzťahov medzi spoločníkmi ako aj medzi spoločníkmi a tretími osobami nie je možné, aby štandardizované elektronické vzory, aké sú na základe zákonnej delegácie z čl. 23^1 § 5, ako aj čl. 106^1 § 5 poľského ZOS určené *ad incertas personas*, mali jednotný právny rámec. Nejestvuje totiž možnosť, aby poľský zákonodarca zhotovil vyčerpávajúci zoznam alternatívnych ustanovení a klauzúl, ktoré by bolo možné pridať do prázdnych polí formulára spoločenskej zmluvy obchodnej spoločnosti sprístupnenej v teleinformatickom systéme. Na tomto mieste treba tiež podotknúť, že poľské zákonodarstvo predvída v čl. 48 § 2^1 Zákonníka obchodných spoločností zákaz vnesenia nepeňažných vkladov do verejnej obchodnej spoločnosti založenej na základe elektronického vzoru.

Zavedenie nových riešení, ktoré súvisia s možnosťou používať moderné informačné a sieťové technológie v prípade zakladania a fungovania obchodných spoločností, vynútilo od poľského zákonodarcu potrebu vysvetlenia nových pojmov. V odôvodnení k návrhu novelizácie zo dňa 28.11.2014 bolo zdôraznené, že do čl. 4 § 1 poľského ZOS boli pridané vysvetlenia takých pojmov ako: „vzor zmluvy“ (poľ. *wzorzec umowy*), „podpis potvrdený dôverným profilom ePUAP“ (poľ. *podpis potwierdzony profilem zaufanym ePUAP*), „ustanovenia zmluvy, ktoré je možné zmeniť“ (poľ. *postanowienia zmienne umowy*) a „spoločnosť, ktorej zmluva bola uzatvorená pri využití vzoru zmluvy“ (poľ. *spółka, której umowa została zawarta przy wykorzystaniu wzorca umowy*)[10]. Navyše treba zdôrazniť, že definícia „teleinformatického systému“ sa nachádza v iných normatívnych aktoch.

Treba konštatovať, že vysvetlenie vyššie uvedených pojmov, ktoré boli zavedené do poľského ZOS, je vzhľadom na ich znenie a spôsob ich konštrukcie nejasné a neprecízne. Podľa čl. 4 § 1 bod 12 poľského ZOS, vzor zmluvy je vzor zmluvy sprístupnený v teleinformatickom systéme[11]. Nie je tajomstvo, že nejaký pojem sa nesmie definovať pomocou toho istého pojmu. V opačnom prípade sa vystavíme nebezpečenstvu vystúpenia proti nám s námietkou *idem per idem*. S podobnou námietkou možno vystúpiť aj v prípade definície „ustanovenia zmluvy, ktoré je možné zmeniť“. Podľa čl. 4 § 1 bod 14 poľského ZOS ustanovenia zmluvy, ktoré je možné zmeniť, sú ustanovenia zmluvy, ktorá bola uzatvorená pri využití vzoru zmluvy a ktoré môžu byť podľa tohto vzoru modifikované cez výber vhodných variantov zvláštnych ustanovení alebo cez zavedenie vhodných údajov do zvláštnych polí vzoru, ktoré umožňujú ich zavedenie[12]. V slovníku zákonných pojmov poľského ZOS sa nenašlo vysvetlenie pojmu „teleinformatický systém“. Z toho dôvodu si treba bližšie všimnúť dva predpisy[13]: § 1.2 nariadenia ministra spravodlivosti Poľskej republiky (poľ.

[9] Porov. KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 6.

[10] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 7.

[11] Originálne znenie: ***wzorzec umowy to wzorzec umowy*** *udostępniony w systemie teleinformatycznym*.

[12] Originálne znenie: ***postanowienia zmienne umowy to postanowienia umowy*** *spółki zawartej przy wykorzystaniu wzorca umowy, które zgodnie z wzorcem mogą być modyfikowane przez wybór odpowiednich wariantów poszczególnych postanowień albo przez wprowadzenie odpowiednich danych w określone pola wzorca, umożliwiające ich wprowadzenie.*

[13] Taká istá definícia sa objavuje v dvoch predpisoch iných nariadení ministra spravodlivosti Poľskej republiky zo dňa 13.1.2015: „o poriadku vytvorenia používateľského konta v teleinformatickom systéme, spôsobu využívania teleinformatického systému a začatia v ňom činnosti, ktoré súvisia so zakladaním verejnej obchodnej spoločnosti pri využití vzoru zmluvy aj s inými činnostiami, ktoré sa vykonávajú v teleinformatickom systéme“ (originálne znenie: *Rozporządzenie Ministra Sprawiedliwości z dnia 13.1.2015 w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki jawnej przy wykorzystaniu wzorca umowy oraz innych czynności wykonywanych w systemie teleinformatycznym*) aj „o poriadku vytvorenia používateľského konta v teleinformatickom systéme, spôsobu využívania teleinformatického systému a začatia v ňom činnosti, ktoré súvisia so zakladaním komanditnej spoločnosti pri využití vzoru zmluvy aj s inými činnostiami, ktoré sa vykonávajú v teleinformatickom systéme“ (originálne znenie: *Rozporządzenie*

Rozporządzenie Ministra Sprawiedliwości) zo dňa 14.1.2015 o určení vzorov sprístupnených v teleinformatickom systéme týkajúcich sa komanditnej spoločnosti[14] a § 1.2 nariadenia ministra spravodlivosti Poľskej republiky o určení vzorov sprístupnených v teleinformatickom systéme týkajúcich sa verejnej obchodnej spoločnosti[15]. Podľa týchto predpisov, koľkokrát ide v nariadení o teleinformatický systém, sa pod týmto pojmom rozumie teleinformatický systém podľa čl. 2 bod 3 zákona zo dňa 18.7.2002 o poskytovaní služieb elektronickou cestou[16], ktorý slúži na obsluhu založenia a urobenia iných činností týkajúcich sa komanditnej spoločnosti (resp. verejnej obchodnej spoločnosti), ktorých zmluva bola uzavretá pri využití vzoru zmluvy sprístupneného v teleinformatickom systéme ako aj podanie žiadosti o zápis takejto spoločnosti do Štátneho súdneho registra[17]..

2 VYTVORENIE POUŽÍVATEĽSKÉHO KONTA A LEGITIMÁCIA NA UZAVRETIE SPOLOČENSKEJ ZMLUVY

Za prvý a súčasne nevyhnutný krok na založenie verejnej obchodnej spoločnosti alebo komanditnej spoločnosti treba označiť vytvorenie používateľského konta. Konto možno založiť - takisto ako v prípade zakladania v teleinformatickom systéme spoločnosti s ručením obmedzeným[18] - prostredníctvom internetovej služby sprístupnenej na webovej stránke ministerstva spravodlivosti. Podľa čl. 23^1 § 2 poľského ZOS si uzavretie spoločenskej zmluvy verejnej obchodnej spoločnosti pri využití vzoru zmluvy vyžaduje vyplniť formulár, ktorý je sprístupnený v teleinformatickom systéme, a overiť ho buď zaručeným elektronickým podpisom, ktorý je verifikovaný pomocou platného kvalifikovaného certifikátu, alebo podpisom, ktorý je potvrdený dôverným profilom ePUAP. Analogický predpis pre komanditnú spoločnosť sa nachádza v čl. 106^1 § 2 poľského ZOS. Používateľské konto môže vytvoriť iba fyzická osoba. V zmysle § 3 ods. 1 dvoch nariadení ministra spravodlivosti zo dňa 13.1.2015 (ktoré sa týkajú verejnej obchodnej spoločnosti[19] a komanditnej spoločnosti[20]) sa na vytvorenie konta vyžaduje: podať meno a priezvisko, číslo PESEL[21], ak je daná osoba povinná ho mať, miesto narodenia, identifikáciu preukazu totožnosti, názov tohto preukazu, orgán s označením jeho sídla a štátu, ktorý preukaz vydal, adresu elektronickej pošty a korešpondenčnú adresu; určenie používateľského mena a hesla používateľom; verifikáciu zhodnosti mena, priezviska a čísla PESEL s číslom PESEL, ktoré sa nachádza v zozname PESEL. Na tomto mieste treba zdôrazniť, že vznikajú vážne problémy pre cudzincov, ktorí by chceli založiť

Ministra Sprawiedliwości z dnia 13.1.2015 w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki komandytowej przy wykorzystaniu wzorca umowy oraz innych czynności wykonywanych w systemie teleinformatycznym).

[14] Nariadenie ministra spravodlivosti zo dňa 14.1.2015 o určení vzorov týkajúcich sa komanditnej spoločnosti, ktoré boli sprístupnené v teleinformatickom systéme (originálne znenie: *Rozporządzenie Ministra Sprawiedliwości z 14.1.2015 w sprawie określenia wzorców dotyczących spółki komandytowej udostępnionych w systemie teleinformatycznym*).

[15] Nariadenie ministra spravodlivosti zo dňa 14.1.2015 o určení vzorov týkajúcich sa verejnej obchodnej spoločnosti, aké boli sprístupnené v teleinformatickom systéme (originálne znenie: *Rozporządzenie Ministra Sprawiedliwości z 14.1.2015 w sprawie określenia wzorców dotyczących spółki jawnej udostępnionych w systemie teleinformatycznym*).

[16] Ustawa z dnia 18.7.2002 – o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422).

[17] Originálne znenie: *system teleinformatyczny (...) służący do obsługi zawiązania i dokonywania innych czynności dotyczących spółki komandytowej (względnie spółki jawnej), której umowę zawarto się przy wykorzystaniu wzorca umowy udostępnionego w systemie teleinformatycznym oraz złożenia wniosku o wpis do Krajowego Rejestru Sądowego dotyczący takiej spółki.*

[18] Porov. STRZĘPKA J. A., ZIELIŃSKA E., in STRZĘPKA J. A. (red.): Kodeks spółek handlowych. Komentarz, Warszawa: C.H. Beck, 2013, s. 358.

[19] Dz. U. z 2015 r., poz. 64.

[20] Dz. U. z 2015 r., poz. 63.

[21] PESEL je akronym od slov: *Powszechny* (slov. všeobecný) *Elektroniczny* (slov. elektronický) *System* (slov. systém) *Ewidencji* (slov. evidencie) Ludności (slov. obyvateľstva). Je to základný register evidencie obyvateľstva v Poľsku.

takú osobnú spoločnosť, lebo oni v podstate – bez skoršej registrácie – nebudú mať takéto číslo PESEL.

Konto bude sprístupnené používateľovi iba po overení v teleinformatickom systéme. Overenie nasleduje po oznámení používateľského mena a hesla. Ďalej musí používateľ vyplniť elektronický vzor zmluvy. Poslednou etapou je však podpísanie spoločenskej zmluvy. Podpísanie zmluvy možno urobiť prostredníctvom zloženia zaručeného elektronického podpisu, ktorý je verifikovaný pomocou platného kvalifikovaného certifikátu, alebo zloženia podpisu, ktorý je potvrdený dôverným profilom ePUAP. Používateľské konto zakladajú všetky fyzické osoby, ktoré sa zúčastňujú na zakladaní danej osobnej spoločnosti. Tieto osoby musia počas podpisovania dokumentov v teleinformatickom systéme určiť, či podpisujú dokument vo vlastnom mene, alebo v mene inej osoby. Ak podpisujú dokument v mene inej osoby je potrebné označiť spôsob zastúpenia. V zmysle nariadení zo dňa 13.1.2015 môže zastúpenie vyplývať z faktu konania ako štatutárny orgán alebo konania ako spoločník, ktorý reprezentuje osobnú spoločnosť, konania ako zákonný zástupca alebo konania ako splnomocnenec.

V prípade, že zastúpenie vyplýva z faktu konania ako splnomocnenec, pre podanie žiadosti o zápis spoločnosti do Štátneho súdneho registra je potrebné vyplniť vyhlásenie, v ktorom treba určiť fakt udelenia splnomocnenia; osobu, ktorá udelila splnomocnenie; informácie o osobe alebo osobách, ktoré udelili splnomocnenie, konajúc ako reprezentanti subjektu, ak sa splnomocnenie netýka konania v mene fyzickej osoby; dátum udelenia splnomocnenia; rozsah splnomocnenia. Okrem toho treba priložiť do dokumentu vyhlásenie splnomocnenca, ktorého sa týka.

Poľský zákonodarca nepredvídal žiadne subjektívne obmedzenia týkajúce sa právneho vzťahu uzatvorenia zmluvy verejnej obchodnej spoločnosti[22]. V súvislosti s tým môže byť spoločníkom verejnej obchodnej spoločnosti fyzická osoba, právnická osoba alebo organizačná jednotka, ktorá nie je právnickou osobou, ale ktorej bola na základe zákona udelená spôsobilosť mať práva a povinnosti. V prípade komanditnej spoločnosti, v ktorej vystupujú dva druhy spoločníkov – komplementári (pol. komplementariusze) a komanditisti (poľ. komandytariusze), nie sú v podstate žiadné subjektívne obmedzenia. Niektorí autori predstavujú rôzne názory týkajúce sa okruhu subjektov, ktoré môžu byť komplementármi v komanditnej spoločnosti[23]. Tieto koncepcie majú jedine doktrinálny charakter a radšej sa všeobecne predpokladá, že nejestvujú obmedzenia vzťahujúce sa na osobu komplementára. Okruh subjektov, ktoré majú legitimáciu na založenie osobnej spoločnosti tradičným spôsobom, čiže v prípade verejnej obchodnej spoločnosti – v podstate cez uzavretie zmluvy v písomnej forme s následkom neplatnosti[24] a v prípade komanditnej spoločnosti prostredníctvom uzavretia zmluvy formou notárskej zápisnice – obsahuje fyzické osoby, ktoré majú čonajmenej obmedzenú spôsobilosť na právne úkony, právnické osoby aj „mrzácke právnické osoby“ (doslova po poľsky: „*ułomne osoby prawne*“)[25]. Tento okruh sa formálne nezhoduje s okruhom osôb, ktoré majú legitimáciu na vytvorenie používateľského konta v teleinformatickom sytéme. Fakticky len osoby oprávnené konať v mene fyzickej osoby, ktorá má obmedzenú spôsobilosť na právne úkony (zákonní zástupcovia) ako aj fyzické osoby, ktorých oprávnenie konať v mene danej osoby vyplýva z faktu, že konajú ako štatutárny orgán právnickej osoby budúceho spoločníka osobnej spoločnosti, môžu vyjadriť prejav vôle o založení osobnej spoločnosti.

3 FORMOVANIE OBSAHU ZMLUVY UZATVÁRANEJ V TELEINFORMATICKOM SYSTÉME

Oficiálne formuláre zmlúv verejnej obchodnej, ako aj komanditnej spoločnosti, ktoré sú sprístupnené v systéme, majú interaktívny charakter. Vďaka nim možno totiž uzatvoriť spoločenskú zmluvu s **minimálnym obsahom, ktorý je nutný na získanie zápisu do registra,** využívajúc

[22] Pozri: SOŁTYSIŃSKI, S., in SZAJKOWSKI, A. (red.): System Prawa Prywatnego. Tom 16. Prawo spółek osobowych, Warszawa: C. H. Beck, 2010, s. 780.

[23] Pozri: SZUMAŃSKI, A., in SZAJKOWSKI, A. (red.): System Prawa Prywatnego. Tom 16. Prawo spółek osobowych, Warszawa: C. H. Beck, 2010, s. 905.

[24] Vynechajúc situáciu, keď ako svoj vklad spoločník vnáša nehnuteľnosť (požiadavka: notárska zápisnica) alebo podnik (požiadavka: písomná forma s notársky overenými podpismi).

[25] Toto je iné určenie, ktoré jestvuje v doktríne, na tzv. organizačné jednotky, ktoré nie sú právnické osoby, ale ktorým bola na základe zákona udelená spôsobilosť mať práva a povinnosti.

pritom tzv. alternatívne ustanovenia (poľ. *alternatywne postanowienia*)[26]. Nevyvoláva pochybnosti, že uzatvorenie spoločenskej zmluvy verejnej obchodnej aj komanditnej spoločnosti v teleinformatickom systéme si bude vyžadovať vyplnenie uvedeného formulára. Ako v prípade oficiálneho interaktívneho formulára pre spoločnosť s ručením obmedzeným[27], formuláre zmlúv verejnej obchodnej spoločnosti a komanditnej spoločnosti majú tri druhy ustanovení: nemenné ustanovenia zmluvy spoločnosti, ustanovenia, ktoré je potrebné vyplniť spoločníkmi a ustanovenia, ktoré predvídajú výber variantov spoločníkmi.

Medzi nemenné ustanovenia zmluvy verejnej obchodnej spoločnosti patrí § 7 vzoru zmluvy, ktorý stanovuje, že „každý spoločník má právo reprezentovať[28] spoločnosť" a „oprávnenie urobiť prejav vôle aj podpis v mene spoločnosti majú dvaja spoločníci alebo jeden spoločník spolu s prokuristom". Oproti tomu medzi nemenné ustanovenia zmluvy komanditnej spoločnosti patrí § 6.2, aký stanovuje, že „vklady vnesené na komanditnú sumu[29] boli vnesené ako celok". Okrem toho treba pamätať na to, že podľa čl. 48 § 2^1 poľského ZOS – v prípade uzavretia alebo zmeny zmluvy verejnej obchodnej spoločnosti uzatvorenej pri využití vzoru zmluvy sprístupneného v teleinformatickom systéme môžu mať vklady iba peňažný charakter[30]. Tento predpis bude tiež platiť pre komanditnú spoločnosť, zmluva ktorej bola uzatvorená pri využití vzoru zmluvy. V zmysle čl. 103 § 2 poľského ZOS je pri komanditnej spoločnosti, ktorej zmluva bola uzatvorená pri využití vzoru zmluvy sprístupneného v teleinformatickom systéme, potrebné aplikovať primerane (poľ. *odpowiednio*) predpisy týkajúce sa verejnej obchodnej spoločnosti, ktorej zmluva bola uzatvorená pri využití vzoru zmluvy.

Medzi ustanovenia zmluvy, ktoré je potrebné vyplniť spoločníkmi, patria ustanovenia vzťahujúce sa na tieto body: určenie spoločníkov, ktorí zakladali spoločnosť (§ 1 vzoru zmluvy verejnej obchodnej spoločnosti; § 1 vzoru zmluvy komanditnej spoločnosti), určenie obchodného mena (§ 2 vzoru zmluvy verejnej obchodnej spoločnosti; § 2 vzoru zmluvy komanditnej spoločnosti), určenie sídla (§ 3 vzoru zmluvy verejnej obchodnej spoločnosti; § 3 vzoru zmluvy komanditnej spoločnosti), určenie predmetu podnikania spoločnosti (§ 4 vzoru zmluvy verejnej obchodnej spoločnosti; § 4 vzoru zmluvy komanditnej spoločnosti), určenie výšky vnesených peňažných vkladov ako aj osôb, ktoré tieto vklady vniesli (§ 5 vzoru zmluvy verejnej obchodnej spoločnosti; § 7 vzoru zmluvy komanditnej spoločnosti), určenie roku, v ktorom sa končí prvý obchodný (bilančný) rok (§ 13 vzoru zmluvy verejnej obchodnej spoločnosti; § 15 vzoru zmluvy komanditnej spoločnosti). Okrem toho sa v prípade komanditnej spoločnosti žiada vyplniť ustanovenia týkajúce sa výšky tzv. komanditnej sumy[31] (§ 6.1 vzoru zmluvy komanditnej spoločnosti) ako aj určenia komplementárov, ktorí sú oprávnení konať v mene spoločnosti (§ 9 vzoru zmluvy komanditnej spoločnosti).

Ustanovenia týkajúce sa výberu variantov spoločníkmi obsahujú v prípade verejnej obchodnej spoločnosti: § 6, v ktorom spoločníci vyberajú medzi uzavretím spoločenskej zmluvy na neurčitý čas (variant A) alebo na určitý čas (variant B); § 8, v ktorom spoločníci vyberajú medzi oprávnením všetkých spoločníkov na obchodné vedenie spoločnosti (variant A) alebo odovzdaním tohto oprávnenia v prospech niektorých spoločníkov (variant B); § 9, v ktorom spoločníci vyberajú

[26] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 12.

[27] Porov. STRZĘPKA J. A., ZIELIŃSKA E., in STRZĘPKA J. A. (red.): Kodeks spółek handlowych. Komentarz, Warszawa: C.H. Beck, 2013, s. 359; RODZYNKIEWICZ, M.: Kodeks spółek handlowych. Komentarz, Warszawa: LexisNexis, 2014, s. 259; KIDYBA, A.: Kodeks spółek handlowych. Komentarz LEX. TOM I. Komentarz do art. 1 – 300 K.S.H., Warszawa: Wolters Kluwer, 2013, s. 652.

[28] Ide však o možnosť konať v mene spoločnosti.

[29] Poľ. *suma komandytowa*. Je to ekvivalent potenciálneho vkladu komanditistu, ktorý je trebá určiť v zmluve komanditnej spoločnosti a ktorý smie byť splatený komanditistom v plnej výške. V prípade nesplatenia komanditistom vkladu v plnej výške, komanditista ručí za záväzky spoločnosti do výšky svojho nesplateného vkladu.

[30] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 6.

[31] Pozri poznámka 29.

medzi oprávnením deliť zisk rovným dielom medzi všetkých spoločníkov verejnej obchodnej spoločnosti (variant A) a percentuálnym určením podielu na zisku v prospech niektorých spoločníkov (variant B); § 10, v ktorom spoločníci vyberajú medzi povinnosťou znášať rovným dielom stratu verejnej obchodnej spoločnosti všetkými spoločníkmi (variant A) alebo určením iba niektorých spoločníkov, ktorí budú znášať stratu (variant B) alebo určením, že každý spoločník bude povinný znašať stratu verejnej obchodnej spoločnosti zhodne s jeho podielom na zisku (variant C); § 11, v ktorom spoločníci určujú, či súhrn práv a povinností možno previesť na iné osoby bez nevyhnutnosti udelenia písomného súhlasu všetkými inými spoločníkmi (variant C) alebo či ho možno previesť na iné osoby iba v prípade udelenia súhlasu všetkými inými spoločníkmi (variant B) alebo či nie je súhrn práv a povinností možné previesť vôbec (variant A); § 12, v ktorom spoločníci určujú, že si zmena zmluvy spoločnosti vyžaduje skorší súhlas vo forme uznesenia všetkých spoločníkov (variant A) alebo že si zmena zmluvy spoločnosti vyžaduje uznesenie spoločníkov, ktoré bude prijaté v prítomnosti všetkých spoločníkov, ale uznesenie môže byť prijaté úplnou väčšinou (variant B). Všetky vyššie uvedené ustanovenia, aké sa týkajú výberu variantov, sú tiež predvídané pre komanditnú spoločnosť. Číslovanie týchto uznesení vo vzorách je však niečo iné.

S ohľadom na vyššie predstavenú úpravu možno hovoriť o dvoch podtypoch každej zo spoločností: o „tradičnom" podtype a „internetovom" podtype. Treba však zdôrazniť, že zmena zmluvy spoločnosti založenej v teleinformatickom systéme urobená iným spôsobom ako teleinformaticky spôsobuje, že nemáme už dočinenia s „internetovým" podtypom verejnej obchodnej spoločnosti alebo komanditnej spoločnosti[32].

4 MOMENT UZAVRETIA ZMLUVY

Podľa čl. 23^1 § 3 poľského ZOS je zmluva verejnej obchodnej spoločnosti, ktorá bola uzatvorená pri využití vzoru zmluvy uzavretá po uvedení do teleinformatického systému všetkých nevyhnutných údajov na jej uzavretie a od momentu overenia jej elektronickými podpismi spoločníkov. V dôsledku toho dôjde k účinnému uzavretiu zmluvy verejnej obchodnej spoločnosti v momente vyjadrenia zhodného prejavu vôle všetkými spoločníkmi, ktorí uzatvárajú spoločenskú zmluvu, a teda okamihom podpísania elektronickým podpisom posledným používateľom oprávneným podpisať zmluvu. Navyše, podľa § 6.2 nariadenia ministra spravodlivosti zo dňa 13.1.2015, týkajúceho sa verejnej obchodnej spoločnosti spôsobuje podpísanie zmluvy prvým pouzívateľom nemožnosť zmeny obsahu spoločenskej zmluvy.

Treba zdôrazniť, že poľský zákonodarca predvídal analogické riešenie pre komanditnú spoločnosť. Na základe čl. 106^1 § 3 poľského ZOS, zmluva komanditnej spoločnosti je uzavretá po uvedení do teleinformatického systému všetkých nevyhnutných údajov na jej uzavretie a od momentu overenia elektronickými podpismi jej spoločníkov. Identicky ako v prípade verejnej obchodnej spoločnosti, podľa § 6.2 nariadenia ministra spravodlivosti zo dňa 13.1.2015 týkajúceho sa komanditnej spoločnosti spôsobuje podpísanie zmluvy prvým používateľom nemožnosť zmeny obsahu spoločenskej zmluvy.

V prípade uzatvorenia spoločenskej zmluvy verejnej obchodnej alebo komanditnej spoločnosti pri využití vzorov sprístupnených v teleinformatickom systéme je prípustná možnosť vyjadriť prejav vôle, ktorá bude overená prostredníctvom zaručeného elektronického podpisu alebo prostredníctvom podpisu, ktorý bude potvrdený dôverným profilom ePUAP, o ktorý ide v čl. 3 bod 15 zákonu o informatizácii činnosti subjektov, ktoré realizujú úlohy verejného sektora[33]. Pochybnosti vyvoláva fakt, či sa musia všetci používatelia podpísať tým istým spôsobom a či je možné aj alternatívne (zmiešané) používanie platných foriem elektronického podpisu (časť spoločníkov by používala zaručený elektronický podpis a časť podpis potvrdený dôverným profilom ePUAP)[34]. Podľa môjho názoru bude, vzhľadom na nedostatok zákonného zákazu, možné zmiešané

[32] SZUMAŃSKI, A.: Nowelizacja kodeksu spółek handlowych z 28.11.2014 r. przewidująca szersze wykorzystanie wzorca udostępnianego w systemie teleinformatycznym. In: Przegląd Prawa Handlowego, 2015, č. 4, s. 42.

[33] Ustawa z 17.2.2005 – o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Z 2014 r., poz. 1114 ze zm.).

[34] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 10.

používanie platných vzorov podpisu. Okrem toho treba pamätať na to, že podľa čl. 10 § 5 poľského ZOS bude mať prejav vôle vyjadrený takýmto spôsobom rovnaké následky ako prejav vôle vyjadrený písomne.

Je dôležité podčiarknuť, že podľa § 11 nariadenia ministra spravodlivosti zo dňa 13.1.2015 týkajúceho sa verejnej obchodnej spoločnosti ako aj podľa § 11 nariadenia ministra spravodlivosti zo dňa 13.1.2015 týkajúceho sa komanditnej spoločnosti, musí byť pripravenie spoločenskej zmluvy pri využití formulára zmluvy spoločnosti sprístupneného v teleinformatickom systéme a ďalej podpísanie tejto zmluvy urobené najneskôr do 24 hodín. Po tomto čase systém tento formulár dezaktivuje. Navyše, v zhode s čl. 20a ods. 2 zákona o Štátnom súdnom registri[35], registračný súd prerokuje žiadosť na zápis spoločnosti, ktorej zmluva bola uzavretá pri využití vzoru zmluvy sprístupneného v teleinformatickom systéme, v termíne jedného dňa od doručenia tejto žiadosti na súd.

5 ZÁVER

Prerokovaná novela je súčasťou zmien Zákonníka obchodných spoločností, v akom zaviedol poľský zákonodarca po prvý raz možnosť zakladať a registrovať spoločnosť s ručením obmedzeným pri využití vzoru zmluvy sprístupneného v teleinformatickom systéme. Aj teraz sú informatizácia procesu uzatvárania, zmeny a zrušenia zmlúv rozšírené na verejnú obchodnú spoločnosť a komanditnú spoločnosť. Na okraj treba povedať, že možnosť využívať vzory zmlúv v prípade zakladania daných druhov spoločnosti je aj v iných zahraničných zákonodarstvách predvídaná, ale neobsahuje osobné spoločnosti. Napríklad vo francúzskom práve možnosť využiť model zakladateľskej listiny (*modele de statuts types*), ktorý sa nachádza v prílohe do dekrétu zo dňa 9.3.2006 (JO, *unipersonelle a responsibilité limitée*), má zakladateľ jednoosobovej spoločnosti v situácii keď je súčasne aj konateľom v tejto spoločnosti. V nemeckom práve existuje možnosť založiť spoločnosť s ručením obmedzeným na základe tzv. štandardizovaných formulárov (*Musterprotokolle*)[36].

Bez ohľadu na druh spoločnosti sa sa v poľskej doktríne zdôrazňuje, že v zmysle poľského práva bude využívanie vzoru zmluvy sprístupneného v teleinformatickom systéme možné len v prípade ak: 1) zákonodarca predvídal takýto vzor (formulár) pre daný druh spoločnosti a okrem toho 2) je to možné vzhľadom na druh právneho úkonu, ako aj 3) jestvuje právna delegácia – v zmysle Ústavy Poľskej republiky – pre ministra spravodlivosti, aby určil takéto vzory (formuláre)[37]. Podmienkou platného uzavretia zmluvy verejnej obchodnej spoločnosti alebo komanditnej spoločnosti v teleinformatickom systéme je prísne dodržiavať predpisy poľského ZOS a princípy konania v tejto otázke, ktoré stanovujú nariadenia ministra spravodlivosti. Treba si všimnúť, že poľský zákonodarca zreteľne odmietol možnosť založiť verejnú obchodnú spoločnosť alebo komanditnú spoločnosť premenou (zmenou právnej formy) na základe vzoru zmluvy sprístupneného v teleinformatickom systéme. Podľa čl. 555 § 2 poľského ZOS nemôže pretvorená spoločnosť (poľ. *spółka przekształcana*) vzniknúť prostredníctvom uzatvorenia zmluvy elektronicky ani v prípade, keď bola zmluva pretváranej spoločnosti uzatvorená pri využití vzoru zmluvy.

Prostredníctvom štandardizovaného vzroru zmluvy verejnej obchodnej spoločnosti alebo komanditnej spoločnosti môžu spoločníci (komplementári, komanditisti alebo spoločníci verejnej obchodnej spoločnosti) alebo ich splnomocnenci uzatvoriť spoločenskú zmluvu, ktorá má minimálny aj nevyhnutný obsah na zápis do registra. V prípade, že by spoločníci mali v úmysle doplniť obsah zmluvy „neštandardnými" ustanoveniami, ktoré boli nimi individuálne nimi dohovorené, môžu oni iba prijať uznesenie mimo teleinformatického systému. Od momentu zmeny spoločenskej zmluvy „tradičným" spôsobom (v prípade verejnej obchodnej spoločnosti – v podstate písomne, v prípade

[35] Ustawa z 20.8.1997 – o Krajowym Rejestrze Sadowym (Dz. U. Z 2013 r., poz. 1203 ze zm.).

[36] Pozri: SZAJKOWSKI, A., TARSKA, M., in SZWAJA, J., SZUMAŃSKI, A., SZAJKOWSKI, A., SOŁTYSIŃSKI, S., TARSKA, M., HERBET, A.: Kodeks spółek handlowych. Tom II. Spółka z ograniczoną odpowiedzialnością. Komentarz do artykułów 151 – 300, Warszawa: C. H. Beck, 2014, s. 92.

[37] SZUMAŃSKI, A.: Nowelizacja kodeksu spółek handlowych z 28.11.2014 r. przewidująca szersze wykorzystanie wzorca udostępnianego w systemie teleinformatycznym. In: Przegląd Prawa Handlowego, 2015, č. 4, s. 40.

komanditnej spoločnosti – notárskou zápisnicou) nebude možné vrátiť sa do ďalšieho využívania vzorov sprístupnených v teleinformatickom systéme[38].

Treba zdôrazniť, že predpisy čl. 23^1 a 106^1 poľského ZOS zavádzajú pri zakladaní verejnej obchodnej spoločnosti aj komanditnej spoločnosti možnosť využitia jedného z variantov vzorov zmluvy pripravených zákonodarcom. To všetko malo dať vo všeobecných črtách budúcim spoločníkom istotu meritorickej správnosti obsahu zmluvy a v ďalšom poradí aj istotu, že súd nebude upierať spoločníkom zmluvy ako nezhodnú s predpismi[39]. Napriek dobrým intenciám, je na záver potrebné konštatovať, že niektoré fragmenty úpravy vzťahujúcej sa na zakladanie osobných spoločnosti sú v teleinformatickom systéme nekompletné a budú ešte pravdepodobne ďalej novelizované.

Použitá literatúra:

KIDYBA, A.: Kodeks spółek handlowych. Komentarz LEX. TOM I. Komentarz do art. 1 – 300 K.S.H., Warszawa: Wolters Kluwer, 2013, 1372 s. ISBN 978-83-264-4027-4.
RODZYNKIEWICZ, M.: Kodeks spółek handlowych. Komentarz. Wydanie 6. Warszawa: LexisNexis, 2014, 1368 s. ISBN 978-83-278-0958-2.
SOŁTYSIŃSKI, S., in SZAJKOWSKI, A. (red.): System Prawa Prywatnego. Tom 16. Prawo spółek osobowych. Warszawa: C. H. Beck, 2010, 1098 s. ISBN 978-83-7483-707-1.
STRZĘPKA J. A., ZIELIŃSKA E., in STRZĘPKA J. A. (red.): Kodeks spółek handlowych. Komentarz. 6 wydanie. Warszawa: C.H. Beck, 2013. 1418 s. ISBN 978-83-255-5212-1.
SZAJKOWSKI, A., TARSKA, M., in SZWAJA, J., SZUMAŃSKI, A., SZAJKOWSKI, A., SOŁTYSIŃSKI, S., TARSKA, M., HERBET, A.: Kodeks spółek handlowych. Tom II. Spółka z ograniczoną odpowiedzialnością. Komentarz do artykułów 151 – 300. 3 wydanie. Warszawa: C. H. Beck, 2014, 1028 s. ISBN 978-83-255-5253-4.
SZUMAŃSKI, A., in SZAJKOWSKI, A. (red.): System Prawa Prywatnego. Tom 16. Prawo spółek osobowych. Warszawa: C. H. Beck, 2010, 1098 s. ISBN 978-83-7483-707-1.
WACH, M.: Status ułomnych osób prawnych w polskim prawie cywilnym. Warszawa: C.H. Beck, 2008, 506 s. ISBN 978-83-7483-878-8.
KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 4 – 17.
SZUMAŃSKI, A.: Nowelizacja kodeksu spółek handlowych z 28.11.2014 r. przewidująca szersze wykorzystanie wzorca udostępnianego w systemie teleinformatycznym. In: Przegląd Prawa Handlowego, 2015, č. 4, s. 38 – 47.
ZAMOJSKI, Ł.: Uwagi na tle projektu „S24" dotyczącego rejestracji spółek z o.o. In: Prawo spółek, 2011, č. 2, s. 21 – 27.

Ustawa z dnia 15.9.2000 – Kodeks spółek handlowych (Dz. U. Z 2013 r., poz. 1030 ze zm.).
Ustawa z 20.8.1997 – o Krajowym Rejestrze Sadowym (Dz. U. Z 2013 r., poz. 1203 ze zm.).
Ustawa z 17.2.2005 – o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Z 2014 r., poz. 1114 ze zm.).
Ustawa z dnia 18.7.2002 – o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422).

Rozporządzenie Ministra Sprawiedliwości z 14.1.2015 w sprawie określenia wzorców dotyczących spółki komandytowej udostępnionych w systemie teleinformatycznym (Dz. U. z 2015 r. poz. 70).
Rozporządzenie Ministra Sprawiedliwości z 14.1.2015 w sprawie określenia wzorców dotyczących spółki jawnej udostępnionych w systemie teleinformatycznym (Dz. U. z 2015 r. poz. 68).
Rozporządzenie Ministra Sprawiedliwości z dnia 13.1.2015 w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania

[38] KOCOT, W. J.: Forma elektroniczna aktów założycielskich i niektórych czynności z zakresu stosunków wewnętrznych spółek handlowych – nowelizacja kodeksu spółek handlowych z 28.11.2014 r. In: Przegląd Prawa Handlowego, 2015, č. 2, s. 13.
[39] V prípade spoločnosti s ručením obmedzeným porovnaj aj: ZAMOJSKI, Ł.: Uwagi na tle projektu „S24" dotyczącego rejestracji spółek z o.o. In: Prawo spółek, 2011, č. 2, s. 24 – 25.

w nim czynności związanych z zawiązaniem spółki jawnej przy wykorzystaniu wzorca umowy oraz innych czynności wykonywanych w systemie teleinformatycznym (Dz. U. z 2015 r. poz. 64).
Rozporządzenie Ministra Sprawiedliwości z dnia 13.1.2015 w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki komandytowej przy wykorzystaniu wzorca umowy oraz innych czynności wykonywanych w systemie teleinformatycznym (Dz. U. z 2015 r. poz. 63)

Smernica Európskeho parlamentu a Rady 2009/101/ES zo 16.9.2009 o koordinácii záruk, ktoré sa od obchodných spoločností v zmysle článku 48 druhého odseku zmluvy vyžadujú v členských štátoch na ochranu záujmov spoločníkov a tretích osôb s cieľom zabezpečiť rovnocennosť týchto záruk
Smernica Európskeho parlamentu a Rady 2013/34/EÚ z 26.6.2013 o ročných účtovných závierkach konsolidovaných účtovných závierkach a súvisiacich správach určitých druhov podnikov, ktorou sa mení smernica Európskeho parlamentu a Rady 2006/43/ES a zrušujú smernice Rady 78/660/EHS a 83/349/EHS

Kontaktné údaje:
Mgr Mateusz Żaba
mazaba@us.edu.pl
Uniwesytet Śląski w Katowicach, Wydział Prawa i Administracji
Ul. Bankowa 11b
40 – 007 Katowice
Poľsko