UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

PRÁVNICKÁ FAKULTA

Ústav európskeho práva

INFORMAČNÁ SPOLOČNOSŤ A MEDZINÁRODNÉ PRÁVO

ZBORNÍK PRÍSPEVKOV ZO VI. ŠTUDENTSKÉHO SYMPÓZIA
KONANÉHO V DŇOCH 21. - 22. APRÍLA 2013
V UČEBNO-VÝCVIKOVOM ZARIADENÍ UPJŠ V DANIŠOVCIACH

ADAM GIERTL A ĽUBICA GREGOVÁ ŠIRICOVÁ (eds.)

KOŠICE 2013

Univerzita Pavla Jozefa Šafárika v Košiciach
Právnická fakulta
Ústav európskeho práva

INFORMAČNÁ SPOLOČNOSŤ A MEDZINÁRODNÉ PRÁVO

Zborník príspevkov zo VI. študentského sympózia

konaného v dňoch 21. - 22. apríla 2013
v učebno-výcvikovom zariadení UPJŠ v Danišovciach

Košice 2013

Zborník vznikol v rámci riešenia projektu APVV-0823-11 Regionalizmus a jeho prínos pre medzinárodné právo.

Informačná spoločnosť a medzinárodné právo

Zborník príspevkov zo VI. študentského sympózia konaného v dňoch 21. - 22. apríla 2013 v učebno-výcvikovom zariadení UPJŠ v Danišovciach

Zostavovatelia: Mgr. Adam Giertl
Mgr. Ľubica Gregová Širicová

Za odbornú a jazykovú stránku tejto štúdie zodpovedajú autori jednotlivých príspevkov. Rukopis neprešiel redakčnou ani jazykovou úpravou.

Umiestnenie:
http://www.upjs.sk/pracoviska/univerzitna-kniznica/e-publikacia/#prf

Dostupné od: 25.07.2013

ISBN 978-80-8152-027-3 (tlačená verzia publikácie)
ISBN 978-80-8152-028-0 (e-publikácia)

Predhovor

„Členovia Komisie musia vziať do úvahy fakt, že ich práca sa týka budúcnosti a nie minulosti; nikto nedokáže predvídať, aké informačné médiá budú existovať o sto rokov neskôr."

Francúzsky delegát v Komisii pre ľudské práva, diskutujúc o zaradení pojmu „médiá" do článku o slobode prejavu v návrhu Medzinárodného paktu o občianskych a politických právach, prezieravo vyzýval ostatných členov komisie k predvídavosti ohľadne informačných médií budúcnosti.[1] Diskusia prebehla v roku 1950, kedy o vplyve internetu na spoločenské vzťahy ešte naozaj nemohli delegáti tušiť. Keďže je v dnešných dňoch už jasné, že informačné technológie významne vplývajú na právo, medzinárodné právo nevynímajúc, rozhodli sa organizátori študentského sympózia venovať jeho šiesty ročník téme „*Informačná spoločnosť a medzinárodné právo*".

Študenti Právnickej fakulty sa po prihlásení na sympózium najskôr venovali príprave svojho príspevku, pričom každý z účastníkov mal v prípade potreby k dispozícii konzultanta. Zoznam konzultantov popri členoch Ústavu európskeho práva, oddelenia medzinárodného práva, bol tohto roku rozšírený o odborníka na právo duševného vlastníctva, Mgr. Martina Husovca, absolventa našej Právnickej fakulty a v súčasnosti IMPRS-CI doktoranda pôsobiaceho na Inštitúte Maxa Plancka pre duševné vlastníctvo a súťažné právo. Aj touto cestou ďakujeme, že venoval svoj čas študentom a pomohol im cennou radou pri príprave ich príspevkov. Po ukončení prípravnej fázy sa konalo samotné sympózium, ktorého cieľom bolo prezentovať vypracované príspevky a rozvinúť o nich diskusiu. Prednesené príspevky svojím zameraním odrážali široké spektrum prienikov medzinárodného práva a informačnej spoločnosti.

Ukončená „päťročnica" bola pre organizátorov výzvou, ako myšlienku sympózií posunúť ďalej a úroveň podujatia vylepšovať. Zmenou oproti predchádzajúcim ročníkom sa stalo nové miesto konania sympózia. Učebno-výcvikové zariadenie Univerzity Pavla Jozefa Šafárika v Danišovciach poskytlo pre účastníkov sympózia príjemné prostredie pre diskusie v rámci sympózia i mimo neho. Po prvý krát bol program sympózia rozdelený do dvoch dní. Umiestnenie podujatia do priestorov mimo fakulty sa stretlo s pozitívnym ohlasom u účastníkov. Mimoriadne nás teší, že aj v tomto roku sa opätovne na Právnickej fakulte našla skupina študentov ochotných venovať svoj čas a námahu medzinárodnému právu i mimo rámca jeho povinnej výučby.

Radi by sme zároveň na tomto mieste vyjadrili vďaku p. prof. JUDr. Jánovi Klučkovi, CSc., doc. JUDr. Kristiánovi Csachovi, PhD., LL.M., a JUDr. Ľudmile Pošivákovej za podporu pri organizácii podujatia a množstvo podnetných vystúpení v rámci sympózia. Osobitné poďakovanie by sme chceli vysloviť odbornému garantovi sympózia, p. prof. JUDr. Jánovi Klučkovi, CSc., ktorému vďačí sympózium za mnohé: počnúc výberom témy až po cenné postrehy v priebehu sympózia. Prof. Klučka sa na sympóziu tradične ujal aj záverečného slova a zhrnul závery, ktoré vyplynuli z vystúpení študentov a z následných diskusií. Pí-

---

[1] Commission on Human Rights, 6th Session, 54, U. N. Doc. E/CN.4/SR.165 (May 2, 1950). Citované podľa LAND, M., Toward an International Law of the Internet (November 19, 2012). In: *Harvard International Law Journal*, Vol. 54, 2013 (Forthcoming). Dostupné na SSRN: http://ssrn.com/abstract=2177993.

somné zachytenie „Ohliadnutia za sympóziom“ uverejňujeme v zborníku ako úvodné priblíženie, ktorá zaznamenáva najdôležitejšie momenty sympózia.

Zostavitelia

Obsah

Podrobný obsah

Ohliadnutie za študentským sympóziom „Informačná spoločnosť a medzinárodné právo“

prof. JUDr. Ján Klučka, CSc.

- Súčasná úprava používania internetu sa skladá z vlastných pravidiel neprávnej povahy, ako aj pravidiel vnútroštátneho a medzinárodného práva, pričom právne pravidlá upravujú rôzne účinky používania internetu vo vybraných oblastiach.
- Samotné fungovanie a „management“ internetu sú v rozhodujúcej miere predmetom úpravy pravidiel neprávnej povahy prijímaných samotnými užívateľmi internetu (ich skupinami) alebo špecializovanými organizáciami nevládnej povahy.
- Vnútroštátne a medzinárodné právo sa zaoberá predovšetkým trestnoprávnou úpravou a/alebo kvalifikáciou škodlivých účinkov pôsobenia internetu v oblasti ľudských práv (ochrana detí, zákaz pornografie), ako aj právom na prístup k internetu ako ľudského práva tvoriaceho súčasť práva na informácie. Potenciálnou oblasťou vnútroštátnej úpravy sa stáva aj otázka informačnej (kybernetickej) bezpečnosti štátov.
- Trestnoprávna úprava tzv. počítačovej kriminality zostáva na úrovni vnútroštátneho práva, nakoľko medzinárodné dohovory ukladajú svojim zmluvným stranám určité konania trestnoprávne kvalifikovať v rámci a na úrovni vnútroštátnych právnych poriadkov. Pre trestný postih páchateľov sa uplatňuje pravidlo *aut dedere aut iudicare* používané v súčasnom medzinárodnom práve pre postih páchateľov trestnej činnosti s medzinárodným prvkom (napríklad trestné činy ohrozujúce bezpečnosť medzinárodného civilného letectva). Predovšetkým z tohto dôvodu sa návrhy na vznik medzinárodného súdu na postihovanie počítačovej kriminality nejavia veľmi reálne, čo nevylučuje medzinárodnú spoluprácu pri jej potieraní v iných oblastiach a inými spôsobmi (EÚ, Interpol a pod.)
- Používanie internetu v diplomatickom práve neposkytuje (zdá sa) taký stupeň ochrany prenášaných informácií ako tradičné prostriedky používané na prepravu správ (diplomatická pošta, diplomatickí kuriéri) vzhľadom na možnosť napadnutia napr. hackermi.
- Existujú rôzne názory doktríny, či tzv. kyberútoky možno kvalifikovať ako ozbrojený útok podľa čl. 51 Charty OSN, ktorý by zakladal právo na použitie individuálnej alebo kolektívnej sebaobrany takto „napadnutého“ štátu. Budúca prax predovšetkým BR OSN ukáže, či a ak áno, v akom rozsahu je Charta OSN schopná „absorbovať“ aj výklad termínu ozbrojený útok v naznačenom smere.

Miesto a úloha internetu v informačnej spoločnosti (obsah, špecifiká, elementy)

Peter Kaňuch

Úvod

V posledných rokoch nás čoraz viac a intenzívnejšie obklopujú informačné a komunikačné technológie. IT odvetvie a telekomunikačný sektor zaznamenáva neustále silnejúci rozmach, ktorý so sebou prináša zásadné zmeny v našom živote a pohľade na okolitý svet. Nové technológie a digitálna technika umožňujú vznik nových multimediálnych služieb a aplikácii, ktoré sú prostredníctvom telekomunikácie prístupné kdekoľvek na svete. Samozrejmosťou sa pre nás stali platobné karty, telefóny, televízia, počítače, internet a mnohé ďalšie vymoženosti moderného sveta. Prenikanie týchto nových informačno-komunikačných technológií (IKT) do všetkých úrovni ekonomiky a spoločenského života je to, čo našu spoločnosť zásadne mení. Tento jav ktorého sme na začiatku 21. storočia svedkami, sa dá charakterizovať ako prechod od priemyselnej spoločnosti k informačnej spoločnosti.

Charakter spoločnosti sa mení, vznikajú nové možnosti uplatnenia v nových odvetviach hospodárstva. Rozvoj informačnej spoločnosti vytvára nové pracovné príležitosti, odstraňuje menej kvalifikované pracovné miesta a vytvára väčší počet pracovných miest závislých na spracovaní informácií. Nové technológie lákajú aj nové investície. Rozvoj informačnej spoločnosti sa stáva politickým programom pre najvyspelejšie štáty sveta a tiež pre Európsku úniu. Vzhľadom na to, že vývoj v tejto oblasti napreduje veľkou rýchlosťou, prijímajú sa viaceré opatrenia na zabezpečenie prípravy obyvateľov na novú dobu, ako i zachovanie ekonomických a politických štandardov. Technologický vývoj musí byť sprevádzaný aj zmenami v ekonomicko-sociálnej oblasti, aby žiadna časť populácie nebola odstavená od možnosti participácie na týchto zmenách.[2]

1. Internet

K charakteristike informačnej spoločnosti je nutné vymedziť pojem internet, bez ktorého je dnešná informačná spoločnosť nemysliteľná. Internet ako sieť sietí vznikol pre vojenské účely, neskôr sa začal využívať v akademickej sfére, až pred niekoľkými rokmi komerčný svet objavil potenciál tohto nástroja.

Dnes je z internetu celosvetová informačná sieť, určená pre vzájomnú komunikáciu. Spája milióny počítačov a iných zariadení po celom svete. Aplikácie internetu sú neustále zdokonaľované tak, aby bol umožnený rýchly prenos nielen textov ale hlavne multimediálnych súborov - obrazu, zvuku, videa a podobne. Internet predstavuje nevyčerpateľný zdroj informácií každého druhu a odvetvia. Každý užívateľ si medzi, v súčasnosti najbohatšou všeobecnou databázou dokumentov, nájde tému, ktorá ho zaujíma a obohatí, dokonca môže o nej diskutovať s miliónmi ďalších ľudí, ktorí sú pripojení k internetu.

Táto prevratná technológia vniesla novú dimenziu do komunikácie. Rýchlosť, jednoduchosť, prístupnosť, flexibilita a rýchly rozvoj sú základné charakteristiky tohto média. Úspech človeka v tejto imformačnej spoločnosti do veľkej miery závisí od znalosti práce

---

2 http://www.informatizacia.sk/zahranicie/453s.

s informáciami. Schopnosť vylúčiť nepotrebné informácie a vyhľadať tie správne zdroje je základom pre úspech. A práve internet priniesol do práce s informáciami nový pohľad.

Medzi základné služby internetu patrí: Elektronická pošta (e-mail), World Wide Web, Mailing List, Electronic Banking, Telnet, Gopher, Wais (Wide Area Information Servers), Intranet.

1.1. Sloboda prejavu v informačnej spoločnosti

Sloboda prejavu patrí medzi základné ľudské ľudské práva. V medzinárodnom práve slobodu prejavu upravuje aj OSN vo Všeobecnej deklarácii ľudských práv, ktorú ako jeden z najvýznamnejších dokumentov medzinárodného práva akceptuje a zakotvuje do svojich právnych poriadkov väčšina štátov medzinárodného spoločenstva. Sloboda prejavu je zakotvená v článku 19:

„Každý má právo na slobodu názoru a prejavu; toto právo zahŕňa slobodu zastávať názor bez zasahovania a vyhľadávať, prijímať a rozširovať informácie a myšlienky prostredníctvom ľubovoľných médií a bez ohľadu na hranice.“3

Európsky dohovor o ochrane ľudských práv a základných slobôd je najdôležitejšou medzinárodnou ľudskoprávnou zmluvou na európskom kontinente, ktorá zabezpečuje dodržiavanie najdôležitejších práv človeka a takisto sa v článku 10 venuje slobode prejavu:

1. Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice. Tento článok nebráni štátom, aby vyžadovali udeľovanie povolení rozhlasovým, televíznym alebo filmovým spoločnostiam.
2. Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci.

Bližšie sa k slobode prejavu v informačnej spoločnosti a o slobode prejavu na internete vyjadruje aj Medzinárodná asociácia vydavateľov a Medzinárodná federácia knižničných asociácií a inštitúcií.

2. Spoločné vyhlásenie IFLA/IPA o slobode prejavu na Internete[4]

Medzinárodná asociácia vydavateľov (International Publishers Association, IPA) a Medzinárodná federácia knižničných asociácií a inštitúcií (International Federation of Library Associations and Institutions, IFLA) vyhlasujú, že prejav na internete a prístup k internetu a všetkým jeho zdrojom by mali byť v súlade so Všeobecnou deklaráciou ľudských práv Organizácie spojených národov (Universal Declaration of Human Rights, UDHR), najmä s jej článkom 19.

– Vyhlasujú, že bezbariérový prístup k informáciám je nevyhnutný pre slobodu, rovnosť, globálne porozumenie a mier.

---

3 Všeobecná deklarácia ľudských práv, dostupná online: http://www.un.org/en/documents/udhr.

4 Informačná spoločnosť, informačná politika a knižnice – dokumenty IFLA, dostupné online: http://www.cvtisr.sk/itlib/itlib111/ifla.htm.

- Potvrdzujú, že základné princípy ochrany autorských práv materiálov v tlačovom prostredí zostávajú rovnaké aj v elektronickom prostredí.
- Presadzujú, že intelektuálna sloboda je právom každého jednotlivca mať a vyjadrovať svoje názory, vyhľadávať a prijímať informácie a je podstatou tak vydavateľských, ako aj knižničných a informačných služieb.

Upozorňujú, že:

- internet sa stal nevyhnutným prostriedkom pre slobodu prejavu a slobodný prístup k informáciám,
- poskytovanie bezbariérového prístupu k informáciám prostredníctvom internetu pomáha komunitám a jednotlivcom dosiahnuť slobodu, prosperitu, kreativitu a rozvoj.

IFLA a IPA zdôrazňujú, že:

- prístup by nemal podliehať žiadnej forme ideologickej, politickej alebo náboženskej cenzúry.

IFLA a IPA nabádajú:

- medzinárodné spoločenstvo, aby podporilo dostupnosť internetu na celom svete, najmä v rozvojových krajinách, a tým im umožnilo naplno využívať globálne výhody, ktoré poskytuje internet,
- vlády štátov, aby rozvíjali národné informačné infraštruktúry, ktoré zabezpečia prístup k internetu pre celú svoju populáciu;
- všetky vlády, aby podporovali bezbariérový tok informácií dostupných prostredníctvom internetu a odmietali akékoľvek pokusy o cenzúru alebo potláčanie slobody prejavu.

3. Slobodný prístup k informáciam

O slobodnom prístupe k informáciám a vedomostiam sa zmieňuje Svetový summit o informačnej spoločnosti,[5] ktorý sa konal v dvoch fázach. Prvá fáza summitu bola v Ženeve v roku 2003 decembri a druhá fáza sa uskutočnila v Tunise v novembri roku 2005. Tento summit o informačnej spoločnosti sa koná z rozhodnutia Medzinárodnej telekomunikačnej únie a je súčasťou agendy Spojených národov. Stretávajú sa tu hlavy štátov, medzinárodní delegáti, medzivládne a mimovládne organizácie, riaditelia spoločností zo súkromného sektora, občania, médiá, akademici a ďalší podporovatelia myšlienky informačnej spoločnosti.

Výsledkom tohto summitu je vyjadriť spoločnú vôľu zúčastnených subjektov vybudovať informačnú spoločnosť vo svete, ktorá by mala byť orientovaná na ľudí, inkluzívna a rozvojová. Každý človek by mal mať možnosť šíriť, využívať a prijímať informácie a vedomosti. Treba umožniť ľuďom a komunitám využívať potenciál infokomunikačných technológií (IKT) na zabezpečenie trvalo udržateľného rozvoja, zlepšenia kvality života a ochrany ľudských práv. Deklarácia princípov definuje výzvy, ktoré stoja pred ľudstvom a v článkoch 24 až 28 sa venuje prístupu k informáciám a vedomostiam.[6] Hovorí o tom že každý má právo na prístup k informáciám a vedomostiam a preto sa majú odstrániť všetky prekážky, ktoré tomu odporujú. Informácie vo verejnej sfére by mali byť ľahko prístupné na podporu informačnej spoločnosti a chránené pred zneužitím. Prístup k informáciám a ve-

---

5 http://www.itu.int/wsis/index.html.

6 Declaration of Principles, Building the Information Society: a global challenge in the new Millennium, dostupné online: http://www.itu.int/wsis/docs/geneva/official/dop.html.

domostiam zvyšuje životný štandard miliónov ľudí na svete. Napriek tomu sa neustále zväčšuje priepasť medzi vzdelanými a nevzdelanými, medzi chudobnými a bohatými. Je v záujme celého sveta a medzinárodného rozvoja snažiť sa tieto priepastné rozdiely preklenúť.

Ďalším významným dokumentom v medzinárodnom práve týkajúci sa slobodného prístupu k informáciám na internete, internetových knižníc a informačných služieb je Manifest IFLA/UNESCO o internete[7] prijatý správnou radou Medzinárodnej federácie knižničných asociácií a inštitúcií (IFLA) v roku v auguste 2002 v Glasgowe.

4. Manifest IFLA/UNESCO o internete

Neobmedzený prístup k informáciám má zásadný význam pre dosiahnutie slobody, rovnosti, globálneho porozumenia a mieru. Z tohto dôvodu Medzinárodná federácia knižničných asociácií a inštitúcií (IFLA) vyhlasuje:

- Intelektuálna sloboda je právom každého jednotlivca zastávať a vyjadrovať svoje názory a vyhľadávať a získavať informácie; je základom demokracie a je stredobodom knižničných služieb.
- Sloboda prístupu k informáciám, nezávisle od média a hraníc štátov, je základnou zodpovednosťou knihovníckej a informačnej profesie.
- Zabezpečenie neobmedzeného prístupu na internet prostredníctvom knižníc a informačných služieb napomáha dosiahnuť slobodu, prosperitu a rozvoj.
- Prekážky brániace toku informácií by mali byť odstránené, najmä tie, ktoré prehlbujú nerovnosť, chudobu a beznádej.

4.1. Slobodný prístup k informáciám, internet, knižnice a informačné služby

Knižnice a inštitúcie poskytujúce informačné služby sú dynamické inštitúcie, ktoré spájajú ľudí s globálnymi informačnými zdrojmi, myšlienkami a kreatívnymi prácami, ktoré hľadajú. Knižnice a informačné služby sprístupňujú celé bohatstvo ľudského poznania a kultúrnej rozmanitosti prostredníctvom všetkých dostupných médií.

Globálna sieť internetu umožňuje jednotlivcom aj komunitám na celom svete rovnocenný prístup k informáciám v záujme osobného rozvoja, vzdelávania, motivácie, kultúrneho obohacovania, ekonomických aktivít a informovanej účasti na demokracii, bez ohľadu na to, či už sa nachádzajú v najmenších a najvzdialenejších obciach alebo vo veľkomestách. Každý môže prezentovať svoje záujmy, znalosti a kultúru a sprístupniť ich svetu.

Knižnice a informačné služby predstavujú hlavné vstupné brány k internetu. Niekomu poskytujú technické vymoženosti, poradenstvo a pomoc, pre iných sú jedinými dostupnými prístupovými miestami. Knižnice a informačné služby poskytujú mechanizmus na prekonanie prekážok vytvorených rozmanitosťou zdrojov, technológií a nadobudnutých zručností.

5. Princípy slobodného prístupu k informáciám prostredníctvom internetu

Prístup k internetu a všetkým jeho zdrojom by mal byť v súlade so Všeobecnou deklaráciou ľudských práv Organizácie spojených národov, najmä s článkom 19:

---

7 Informačná spoločnosť, informačná politika a knižnice – dokumenty IFLA, dostupné online: http://www.cvtisr.sk/itlib/itlib111/ifla.htm.

„Každý má právo na slobodu názoru a prejavu; toto právo zahŕňa slobodu zastávať názor bez zasahovania a vyhľadávať, získavať a šíriť informácie a myšlienky prostredníctvom ľubovoľných médií a nezávisle od hraníc štátov."

Celosvetová prepojenosť internetu predstavuje médium, prostredníctvom ktorého môžu využívať toto právo všetci. V dôsledku toho by prístup na internet nemal byť predmetom ideologickej, politickej alebo náboženskej cenzúry ani ekonomických bariér. Knižnice a informačné služby majú tiež povinnosť slúžiť všetkým členom ich komunít bez ohľadu na vek, rasu, národnosť, vieru, kultúru, politickú orientáciu, fyzické alebo iné postihnutie, pohlavie, sexuálnu orientáciu alebo akékoľvek iné dôvody.

Knižnice a informačné služby by mali podporovať právo používateľov vyhľadávať informácie podľa ich výberu a mali by rešpektovať súkromie svojich používateľov a rešpektovať, že informácie o vyhľadávaní v informačných zdrojoch, ktoré používatelia používajú, by mali zostať dôverné. Knižnice a informačné služby majú povinnosť umožniť a podporovať verejný prístup ku kvalitným informáciám a komunikačným prostriedkom. Používatelia by mali mať k dispozícii odbornú pomoc a vhodné prostredie, v ktorom môžu vybrané informačné zdroje slobodne a s dôverou využívať.

Okrem množstva hodnotných informačných zdrojov prístupných prostredníctvom internetu, sú niektoré z nich nesprávne, zavádzajúce a môžu byť urážlivé. Knihovníci by mali poskytovať používateľom knižníc také informácie a informačné zdroje, ktoré by ich naučili využívať internet a elektronické informácie účelne a efektívne. Mali by aktívne podporovať a uľahčovať spoľahlivý prístup ku kvalitným sieťovým informáciám všetkým svojim používateľom vrátane detí a mládeže. Rovnako ako ostatné základné služby aj prístup na internet v knižniciach a informačné služby by mali byť bezplatné.

5.1. Uplatnenie Manifestu

IFLA vyzýva medzinárodné spoločenstvo k podpore rozvoja dostupnosti internetu na celom svete, najmä v rozvojových krajinách, aby globálne výhody internetu boli dostupné pre všetkých.

IFLA vyzýva národné vlády k rozvoju národnej informačnej infraštruktúry, ktorá zabezpečí prístup na internet celej populácii štátu. IFLA vyzýva všetky vlády, aby podporovali neobmedzený tok informácií prístupných na internete prostredníctvom knižníc a informačných služieb a aby čelili akýmkoľvek pokusom cenzurovať alebo obmedziť tento prístup.

6. Internet a bezpečnosť

Používanie internetu so sebou prináša aj otázku bezpečnosti a ochrany pred rôznymi kybernetickými útokmi v kyberpriestore. Práve bezpečnosťou a ochranou kyberpriestoru sa zaoberá aj Európske spoločenstvo. Európska komisia 7. februára 2013 zverejnila **stratégiu pre oblasť kybernetickej (informačnej) bezpečnosti: "otvorený, bezpečný a chránený kybernetický priestor"**, ktorá má určiť spoločnú politiku členských štátov v tejto oblasti.

Stratégia identifikuje 5 priorít:

1. dosahovanie odolnosti voči kybernetickým útokom,
2. prudké zníženie počítačovej kriminality,
3. rozvíjanie politiky a spôsobilostí kybernetickej obrany, ktoré súvisia so spoločnou bezpečnostnou a obrannou politikou,

4. rozvíjanie priemyselných a technologických zdrojov na účely kybernetickej bezpečnosti,
5. vytvorenie politiky súdržného medzinárodného kybernetického priestoru pre Európsku úniu a presadzovanie základných hodnôt EÚ.[8]

Komisia zároveň zverejnila pripravovanú smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v celej Únii,[9] ktorá je hlavným mechanizmom, vyplývajúcim z tejto stratégie. Medzi hlavné opatrenia smernice patria nasledovné:

1. členský štát musí prijať národnú stratégiu bezpečnosti sietí a informácií a určiť vnútroštátny orgán príslušný pre bezpečnosť sietí a informácií, disponujúci dostatočnými finančnými a ľudskými zdrojmi, na účely predchádzania rizikám a incidentom v tejto obalsti, ich riešenia a reagovania na ne,
2. vytvára sa mechanizmus spolupráce medzi členskými štátmi a Komisiou na účely vzájomného včasného varovania o rizikách a incidentoch prostredníctvom chránenej infraštruktúry, a na účely spolupráce a organizácie pravidelných hodnotení,
3. prevádzkovatelia mimoriadne dôležitých infraštruktúr v niektorých odvetviach (finančné služby, doprava, energetika, zdravotníctvo), aktéri sprístupňovania služieb informačnej spoločnosti (osobitne: platformy elektronického obchodu založené na tzv. app stores, platby cez internet, cloud computing, internetové vyhľadávače, sociálne siete) a orgány verejnej správy musia prijať postupy riadenia rizík a podávať správy o významných bezpečnostných incidentoch na ich hlavných službách.

Okrem počítačovej kriminality sa vyskytli aj iné problémy ktoré musí Európske spoločenstvo riešiť, ako je ochrana bezpečnejšieho používania a ochrana konečného užívateľa pred nevyžiadaným obsahom. Keďže počet internetových pripojení a používanie nových technológií v Spoločenstve stále významne rastie, naďalej existuje nebezpečenstvo, najmä pre deti, a zneužívanie uvedených technológií a objavujú sa nové nebezpečenstvá a zneužitia. S cieľom podporiť využívanie príležitostí, ktoré ponúka internet a nové online technológie, sú potrebné aj opatrenia na podporu ich bezpečnejšieho používania a ochranu konečného užívateľa pred nevyžiadaným obsahom.

Preto bol vytvorený akčný plán eEurope 2005,[10] ktorý rozvíja lisabonskú stratégiu, má za cieľ stimulovať bezpečné služby, aplikácie a obsah, založené na široko dostupnej širokopásmovej infraštruktúre. K jeho ďalším cieľom patrí bezpečná informačná infraštruktúra, vývoj, analýza a rozširovanie najlepších postupov, referenčného porovnávania a mechanizmus koordinácie elektronických politík.

Legislatívny rámec vytvorený na úrovni Spoločenstva na riešenie problémov týkajúcich sa digitálneho obsahu v informačnej spoločnosti teraz zahŕňa pravidlá týkajúce sa online služieb, najmä nevyžiadaných reklamných e-mailov v smernici o súkromí a elektronických

---

8 EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive, dostupné online: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

9 Návrh Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii, dostupný online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:SK:HTML.

10 eEurope 2005: An information society for all. An Action Plan to be presented in view of the Sevilla European Council, 21. – 22. June 2002, dostupné online: http://www.etsi.org/WebSite/document/aboutETSI/EC_Communications/eEurope2005_actionPlan.pdf.

komunikáciách, dôležitých aspektov zodpovednosti poskytovateľov sprostredkovateľských služieb v smernici o elektronickom obchode, odporúčania pre členské štáty, hospodárske odvetvie a dotknuté strany a Komisiu, spolu s indikatívnymi usmerneniami o ochrane neplnoletých osôb v odporúčaní 98/560/ES.

Jednostaj bude existovať potreba konať v oblasti obsahu s možným škodlivým účinkom na deti alebo obsahu nevyžiadaného konečným užívateľom a v oblasti nezákonného obsahu, najmä detskej pornografie a rasistického materiálu.

Správa Komisie Európskemu parlamentu, Rade, Hospodárskemu a sociálnemu výboru a Výboru regiónov z 13. septembra 2011 o uplatňovaní odporúčania Rady z 24. septembra 1998 o ochrane neplnoletých osôb a ľudskej dôstojnosti a odporúčania Európskeho parlamentu a Rady z 20. decembra 2006 o ochrane neplnoletých osôb a ľudskej dôstojnosti a o práve na vyjadrenie vo vzťahu ku konkurencieschopnosti európskeho priemyslu audiovizuálnych a online informačných služieb s názvom Ochrana detí v digitálnom svete.[11] Táto správa predstavuje opatrenia prijaté v členských štátoch na ochranu detí pri činnostiach na internete. Nadväzuje na odporúčanie z roku 2006 o ochrane neplnoletých v audiovizuálnych a informačných službách a na odporúčanie z roku 1998 o ochrane neplnoletých a ľudskej dôstojnosti. Správa poskytuje prehľad iniciatív v členských štátoch, ktoré sú zamerané na boj proti diskriminujúcemu, nezákonnému alebo škodlivému obsahu na internete. Ide predovšetkým o záväzky či kódexy správania. Umožňujú napríklad na webových lokalitách zobrazovať označenie o ich dodržiavaní.

Úrovne ochrany zabezpečené v rámci takýchto iniciatív sa však v rôznych členských štátoch líšia. Jestvujúce opatrenia by sa mali neprestajne monitorovať, aby sa zabezpečila ich účinnosť. Nezákonný alebo škodlivý obsah pochádza vo všeobecnosti z iných členských štátov EÚ alebo z krajín mimo nej. Koordinovaným prístupom na celoeurópskej úrovni a neskôr aj na medzinárodnej úrovni by sa umožnila harmonizácia ochrany voči tomuto typu obsahu.

Poskytovatelia internetových služieb (PIS) by sa mali čoraz aktívnejšie podieľať na ochrane neplnoletých. Uplatňovanie kódexov správania by malo byť rozšírenejšie a lepšie vymedzené. Združeniam PIS sa adresuje výzva, aby zahŕňali ochranu neplnoletých do svojich činností a svojim členom tak ukladali povinnosti zodpovedajúce tejto ochrane. Väčšie zapojenie spotrebiteľov a orgánov do zostavovania kódexov správania by pomohlo zabezpečiť, aby samoregulácia skutočne reagovala na rýchlo sa rozvíjajúci digitálny svet. Komisia podnecuje PIS, aby rozširovali uplatňovanie kódexov správania a zahŕňali ochranu neplnoletých do svojich mandátov. Sociálne siete od základu zmenili správanie neplnoletých, pokiaľ ide o spôsob, ako na seba navzájom pôsobia a komunikujú. Tieto siete prinášajú mnohé riziká, ako napríklad nezákonný obsah, obsah nevhodný pre neplnoletých, nevhodné kontakty a nevhodné správanie. Jedným z možných spôsobov riešenia týchto rizík zmienených v správe je vytvorenie usmernení o správaní, ktoré by boli určené poskytovateľom sociálnych sietí. Komisia podporuje znásobovanie miest na nahlasovanie problémov a zavedenie dobre fungujúcich administratívnych štruktúr, ktoré sa využijú na sociálnych sieťach.

---

[11] Správa Komisie Európskemu Parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov o uplatňovaní odporúčania Rady z 24. septembra 1998 o ochrane neplnoletých osôb a ľudskej dôstojnosti a odporúčania Európskeho parlamentu a Rady z 20. decembra 2006 o ochrane neplnoletých osôb a ľudskej dôstojnosti a o práve na vyjadrenie vo vzťahu ku konkurencieschopnosti európskeho priemyslu audiovizuálnych a online informačných služieb - Ochrana detí v digitálnom svete, dostupné online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0556:SK:NOT.

7. Elektronický obchod

Elektronický obchod je prenos a spracovanie dát v elektronickom prostredí, ktoré zahŕňa takmer všetky činnosti a operácie elektronického obchodovania, finančných transakcií a elektronickej komerčnej komunikácie. Predstavuje rýchly, efektívny, pohodlný a relatívne bezpečný spôsob obchodovania. Jednotlivé služby elektronického obchodovania by sme podľa Central European Initiative, fóra, ktoré presadzuje regionálnu spoluprácu medzi stredoeurópskymi a východoeurópskymi štátmi, mohli rozdeliť do dvoch základných kategórií,[12] a to:

1. priamy e-obchod – elektronické objednávanie nehmotných tovarov a služieb, ich elektronické doručenie a zaplatenie;
2. nepriamy e-obchod – je elektronickým objednávaním hmotných tovarov. Ich dodanie je uskutočnené fyzicky, pričom takáto operácia je ovplyvnená vonkajšími faktormi, ako sú napríklad dopravný a poštový systém.

7.1. Elektronický obchod a informačná spoločnosť

Služby e-obchodu, nazývané aj služby informačnej spoločnosti, sú realizované najmä prostredníctvom nasledujúcich operácií:

- elektronické obchodovanie s tovarmi a službami,
- elektronické prevody finančných prostriedkov,
- online doručovanie digitálneho obsahu,
- online sprístupňovanie informácií,
- elektronické obchodovanie s akciami,
- verejné obstarávanie,
- elektronická komerčná komunikácia (prostredníctvom e-mailov),
- elektronické platenie daní,
- elektronické poisťovníctvo,
- elektronické účtovníctvo,
- elektronické uzatváranie zmlúv.

Poskytovanie služieb elektronického obchodovania vyplýva aj zo základných predpokladov existencie a rozvoja informačnej spoločnosti, pretože ponúka značné príležitosti na zamestnanie, stimuluje hospodársky rast a investície európskych spoločností do inovácií a zlepšuje konkurencieschopnosť európskeho priemyslu.[13]

Európska únia sa snaží vytvoriť ešte užšie väzby medzi štátmi a ľuďmi Európy, aby zabezpečila hospodársky a spoločenský pokrok. Vnútorný trh predstavuje priestor bez vnútorných hraníc, v ktorom je zabezpečený voľný pohyb tovaru, služieb a sloboda podnikania. Rozvoj služieb informačnej spoločnosti v oblasti bez vnútorných hraníc je veľmi dôležitý pre odstránenie bariér, ktoré rozdeľujú európske národy.

---

[12] HRBEKOVÁ, V., et. al.: E-obchod v informačnej politike Európy, dostupné online: http://www.cvtisr.sk/itlib/itlib111/hrbekova.htm.

[13] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode).

Služby informačnej spoločnosti zahŕňajú celú škálu ekonomických činností, ku ktorým dochádza on-line; tieto služby môžu pozostávať najmä z predaja tovaru on-line; nepatria sem činnosti ako je dodávka tovaru alebo poskytovanie služieb off-line; služby informačnej spoločnosti nie sú výlučne obmedzené na služby, ktoré vedú k vzniku zmluvného vzťahu on-line, ale sa rozširujú aj na služby, ktoré nie sú platené ich príjemcami, pokiaľ predstavujú ekonomickú činnosť, ako sú napríklad služby poskytujúce on-line informácie alebo komerčnú komunikáciu alebo tie, ktoré poskytujú nástroje umožňujúce vyhľadávanie, prístup a získavanie údajov; služby informačnej spoločnosti taktiež zahŕňajú služby pozostávajúce z prenosu informácií prostredníctvom komunikačnej siete, v poskytovaní prístupu do komunikačnej siete alebo v ukladaní informácií poskytnutých príjemcom služby na hosťovskom počítači; televízne vysielanie v zmysle smernice EHS/89/552 a rozhlasové vysielanie nie sú službami informačnej spoločnosti, pretože nie sú poskytované na žiadosť jednotlivca; naproti tomu služby, ktoré sú prenášané z bodu do bodu, ako napríklad video na požiadanie alebo poskytovanie komerčnej komunikácie prostredníctvom elektronickej pošty sú službami informačnej spoločnosti; použitie elektronickej pošty alebo rovnocennej individuálnej komunikácie, napríklad fyzickými osobami, ktoré konajú mimo svojho obchodu, podnikania alebo povolania, vrátane ich využitia na uzatváranie zmlúv medzi takýmito osobami, nie je službou informačnej spoločnosti; zmluvný vzťah medzi zamestnancom a zamestnávateľom nie je službou informačnej spoločnosti; činnosti, ktoré kvôli svojej povahe nemôžu byť vykonávané na diaľku a elektronicky, ako napríklad zákonný audit účtov spoločnosti alebo lekárske poradenstvo, ktoré si vyžaduje fyzické vyšetrenie pacienta, nie sú službami informačnej spoločnosti.

Napriek globálnej povahe elektronickej komunikácie je nevyhnutná koordinácia vnútroštátnych regulačných opatrení na úrovni Európskej únie, s cieľom vyvarovať sa rozdeleniu vnútorného trhu a ustanovenia vhodného európskeho regulačného rámca; takáto koordinácia by mala taktiež prispieť k vytvoreniu spoločnej a silnejšej rokovacej pozícii na medzinárodných fórach. S cieľom umožniť ničím nerušený rozvoj elektronického obchodu, musí byť právny rámec jasný a jednoduchý, predvídateľný a v súlade s pravidlami uplatniteľnými na medzinárodnej úrovni, aby nemal nepriaznivý vplyv na konkurencieschopnosť európskeho priemyslu, alebo aby nebránil inovácii v tomto sektore. Ak má trh skutočne fungovať elektronickým spôsobom v kontexte globalizácie, musia sa Európska únia a hlavné neeurópske oblasti navzájom poradiť, aby ich zákony a postupy boli navzájom zosúladené. V oblasti elektronického obchodu by sa mala posilniť spolupráca s tretími krajinami, najmä so žiadateľskými krajinami o vstup do EÚ, rozvojovými krajinami a ostatnými obchodnými partnermi Európskej únie.

Záver

Úloha internetu v informačnej spoločnosti je nepochybne veľmi významná, nielen preto že internet sa stal globálnym zdrojom informácii, komunikácie a zábavy, ale aj zdrojom príjmu pre určitú skupinu ľudí. A aj to je jeden z dôvodov prečo vyvstala potreba regulovať používanie internetu aj na medzinárodnej úrovni, osobitne upravovať ochranu základných ľudských práv a slobôd v spojitosti s internetom.

Informačná spoločnosť v súčasnom MPV

Valéria Lásková

Úvod

Posledné desaťročia sú sprevádzané náhlym technologickým vývojom. Vďaka tomuto rapídnemu progresu máme náš každodenný život okorenený technickými aparátmi rôzneho druhu. Gramotnosť v tejto oblasti nezohráva žiadnu úlohu, keďže ich ovládateľnosť je poväčšine prispôsobená k užívaniu čo najpočetnejšej skupine ľudí. Či už hovoríme o mobilných telefónoch, alebo priemyselných robotoch, spektrum je široké. Práve jeho univerzálny charakter vystihuje podstatu informačnej spoločnosti vo všeobecnosti. Priestor, kde prebieha výmena, ukladanie a narábanie s informáciami sa nazýva kyberpriestor. Fyzické osoby majú ľahší prístup k informáciám hlavne kvôli internetu, ktorý v dnešnej dobe podľa internetového portálu InternetWorldStats.com využíva k decembru 2011 približne 32,7 % populácie. Toto percento nemá tendenciu klesať, naopak, zvyšuje sa. V súvislosti s medzinárodným právom a celkovo s právom je dôležité spomenúť, že aj na túto oblasť sa vzťahujú špecifické normy, ktoré ju regulujú. Našim cieľom je Vás oboznámiť vo všeobecnosti so spomínanou problematikou a vytvoriť ďalší priestor – priestor určený Vám na rozmýšľanie, či je tento nezastaviteľný fenomén informovanosti dostatočne právne upravený. Či je len nástrojom na uľahčenie mnohých úkonov, alebo aj hrozbou na vytvorenie nových konfliktov v relatívne novo vzniknutom priestore.

1. Kyber priestor

Na začiatok tejto práce je potrebné si vymedziť, čo pojem „kyber priestor" vlastne znamená. Autorom je americko-kanadský spisovateľ William F. Gibson, zakladateľ tzv. *cyberpunku*. Je trochu mätúce, že pojem vysvetľujem pojmom, ale cyberpunk je podžáner science-fiction. Gibson tento pojem použil vo svojich viacerých dielach a jeho definícia znela nasledovne: „kyberpriestor (v origináli *„cybercpace"*) je konsenzuálna dátová halucinácia, vizualizovaná v podobe imaginárneho priestoru, tvoreného počítačovo spracovanými dátami a prístupného len vedomiu (a nie fyzickej telesnosti) užívateľov." Pojem sa tak javí ako protipól skutočnému priestoru, ktorý je naopak založený na hmotnej existencii.[1]

Kyberpriestor je elektronický priestor, miesto, ktoré je v súlade s naším chápaním skutočného sveta, avšak má vlastné priestory, ako sú webové stránky, e- mailové účty a rôzne iné siete, ktoré spájajú verejnosť sieťovým prepojením. Okrem toho, kyberpriestor je virtuálny no existuje v ňom prevádzka na internete, sieť počítačov, ktoré zdieľajú informácie medzi sebou navzájom a so všetkými inými elektronickými obdobnými zariadeniami, ako družice a mobilné telefóny, ktoré môžu byť prepojené. To vytvára ďalšiu formu globalizácie, ba dokonca máme za to, že tú najefektívnejšiu, prístupnú pre nespočetné množstvo ľudí, ktorí používajú elektronické zariadenia na celej Zemi. Tu sa vynárajú otázky typu, či vôbec štáty majú ešte nejakú suverenitu. Tento typ globalizácie je

---

1 ŠVANDA, M.: *Vybrané otázky pôsobnosti práva na internete*, Diplomová práca, Právnická fakulta Masarykovej univerzity, 2008/2009, [online], dostupná na: http://is.muni.cz/th/134654/pravf_m/Diplomova_praca_final.txt.

vnímaný ako nezvyčajný druh teritoriality.[2] V tomto virtuálnom svete už nie je podstatná separácia štátov na dosiahnutie väčšej efektivity informovanosti cieľovej skupiny – fyzické osoby každej generácie. Interakcia prebieha v rámci odlišných nadnárodných sietí. Slovo „suverenita" tu nadobúda iný význam. Je mnoho významov prislúchajúcich tomuto slovu. V Kyber priestore sa pod suverenitou rozumie „totalita medzinárodných práv a povinností uznaných medzinárodným právom" s územnou jednotkou národ – štát.[3] Neznie to zároveň protichodne? Je suverenita štátov a nárastom vplyvu kyber sveta ohrozená? V medzinárodnom práve je chápaná ako nezávislosť štátnej moci od akejkoľvek inej moci, či vo vnútri štátu (vnútorná suverenita) alebo mimo hraníc daného štátu (vonkajšia suverenita). Metafora kybernetického priestoru navráva, že internet je autonómny svet. A odtiaľ je už blízko k protestom proti každému pokusu regulovať internet napríklad uplatňovaním autorských práv, či obmedzovaním extrémizmu. Nie je to celkom tak. Namiesto odlišovania medzi naším reálny svetom a kybernetickým priestorom by sme mali skôr vnímať ich prepojenosť a ovplyvňovanie. Jedinci sediaci za počítačmi nie sú občanmi žiadneho paralelného, autonómneho kyberpriestoru či nejakého univerza mimo nášho sveta. Štát má svoje zákony a právomoci vo vzťahu k tomu, čo sa deje vnútri medzinárodne uznaných hraníc. A z toho sa nemôže vymknúť ani poskytovanie internetových služieb, ktoré tiež nemôže byť v príkrom rozpore s tým, čo nazývame verejným záujmom. Štát má v prípade internetu rovnaké práva i povinnosti kontroly a regulácie ako pri iných moderných informačných a komunikačných technológiách, tvrdí americký publicista Michael Lind v magazíne Salon.[4] Nemá právo zneužiť osobné údaje ani obmedziť slobodu prejavu. Ani toto sa však nevzťahuje len na kybernetický priestor.

1.1. Internet ako súčasť kybernetického priestoru

Internet je otvorená sieť sietí. Zo všetkých sietí na internete by mali užívatelia byť schopní komunikovať s ľubovoľného počítača pripojeného na ktorúkoľvek internetovú sieť.[5] V prvej časti sme sa venovali kyberpriestoru zo všeobecného hľadiska. Načrtli sme tam aj, že internet je jeho súčasťou, akousi pomyselnou podmnožinou. Informovanosť je zabezpečená v rámci kyberpriestoru hlavne vďaka internetu, ktorý je riadený a kontrolovaný z mnoho strán. Existuje veľa inštitútov zriadených na národnej úrovni, ako aj na nadnárodnej, ktoré sa zaoberajú globálnym riadením v tejto oblasti. Spomeniem dva, ktoré zaraďujeme medzi hlavnejšie. Prvým z nich je the Internet Corporation of Assigned Names and Numbers (ICANN)[6] a druhým Global Business Dialogue on Electronic Commerce (GBDe).[7] V nasledujúcich riadkoch sa budeme venovať v stručnosti obidvom spomínaným organizáciám.

---

2 Georgios I. Zekos BS in Economics, JD, LLM, PhD, University of Peloponnesus, Advocate and Economist.

3 ZEKOS, G. I.: Cyber -Territority and jurisdiction of nations, Journal of internet law, June 2012.

4 ZEKOS, G. I.: Journal of internet law, Cyber territority and jurisdiction of nations, june 2012.

5 CLARKE, R.: Cyber War (Harper Collins, 2010), chapter 3; dostupné online: http://www.richardaclarke.net/cyber_war.php#excerpts.

6 http://www.icann.org, o ICANN vo všeobecnosti, FROOMKIN, M.: 'Wrong Turn in Cyberspace: Using ICANN to Route Around the Constitution and the APA', (2000) 50 Duke Law Journal 17–186; J. Weinberg, 'ICANN and the Problem of legitimacy', (2000) 50 Duke Law Journal 187–258; M. Mueller, ICANN and Internet Governance - Sorting through the debris of self-regulation', info Vol 1, No. 6, December 1999, 497–520.

7 http://www.gbde.org.

1.1.1. ICANN

„*Internet Corporation of Assigned Names and Numbers*." Na prvý pohľad zhluk nič nehovoriacich písmen. Avšak ICANN vo voľnom preklade do slovenčiny znamená Internetová organizácia (združenie) zapísaných mien a čísel. Na akom princípe funguje? Ak ste sa rozhodli nájsť inú osobu prostredníctvom ICANN, musíte do svojho počítača zadať adresu – meno alebo číslo. Táto adresa musí byť unikátna, aby počítač vedel, kde nájsť hľadaný počítač. ICANN koordinuje tieto jedinečné informácie po celom svete. Bez tejto koordinácie by sme nemali jeden globálny Internet. Z viac technického hľadiska by sme Internetové združenie pre prideľovanie mien a čísel (ICANN) definovali pojmom koordinácia. Koordinuje Domain Name System (DNS) - doménový systém, IP (Internet Protocol) a s ním súvisiace IP adresy, alokácie, henerické kódy a kódy krajiny, a koreňový server funkcie pre správu systému. Tieto služby boli pôvodne vykonané na základe zmluvy vlády Spojených štátov o Internet Assigned Numbers Authority (IANA) a ďalšími subjektmi. ICANN teraz vykonáva funkciu IANA.

Podobné organizácie, ktoré vzájomne participujú medzi sebou za rovnakým účelom sú napríklad:

- Address Supporting Organization (ASO),
- At-Large Advisory Committee (ALAC),
- Country Code Domain Name Supporting Organization (ccNSO),
- Generic Names Supporting Organization (GNSO),
- Governmental Advisory Committee (GAC),
- Root Server System Advisory Committee (RSSAC),
- Security and Stability Advisory Committee (SSAC).[8]

1.1.2. GBDe

„*Global Business and Eletronic commerce*" - stále narastajúca globalizácia vytvára priestor na potrebu ďalšej regulácie pomocou zriaďovania nových inštitútov. V minulosti bola postačujúca iná úprava, jednoduchšia. Je potrebné odstrániť paradigmy z minulosti a to bol aj jeden z dôvodov vzniku GBDe.[9] Obsahom tejto organizácie je právna regulácia rôznych oblastí kybernetického priestoru. Každá firma používa počítače, spravuje sa pri tom zákonmi, ktoré regulujú danú oblasť. Do ich interných zákonov vstupujú aj iné, nadradené jurisdikcie. Cieľom je zabezpečiť, aby tieto prístroje boli v súlade s právnou úpravou. Ich vzájomná prepojenosť je nevyhnutná a súlad samozrejmý. Jedným z príkladov zavedenia zákona platného nadnárodne bol v roku 1990 the Computer Misure Act schválený vo Veľkej Británii. Zahŕňa mnoho rôznych právnych aspektov používania počítačov alebo iných sietí v súlade s právom. Dôraz sa kladie hlavne na bezpečnosť uloženia informácii v počítačoch a zároveň aby k týmto informáciám mali prístup len spoločnosti, ktorým počítače patria. Keďže táto oblasť vývoja napreduje závratným tempom, už pár rokov na to bolo potrebné uviesť to platnosti ďalšie zákony. Nie je pravidlom, že zákon prijatý v jednej krajine bude platným napriek svojej univerzalite v iných krajinách. Faktom však je, že krajiny sa inšpirujú a vďaka informovanosti sa podieľajú v konečnom dôsledku na tom, že ich úprava je často krát podobná. Tu je na mieste uviesť aj ďalšie krajiny, ktoré zaviedli zákony, ktorými sa riadi internet, podnikanie v kyber priestore. India v roku 2000 priniesla svoj

---

8 http://www.icann.org/en/about/welcome.

9 http://www.gbde.org/promoting-your-business-legally/.

India´s Technology Act, jednotlivé štáty USA priniesli do sveta informačných technológii niekoľko zákonov, na príklad the Florida Electronic Security Act. Illinois a Texas sa podieľajú na zákonoch súvisiacich s bezpečnosťou elektronického obchodovania (Electronic Security Act). Niektoré krajiny sa rozhodli pre takú právnu úpravu, ktorá sa nepriamo týka aj iných krajín a to je zavedenie internetovej cenzúry. Informácie sú dostupné len na počítačoch, ktoré sídlia v danej krajine. Je niekoľko krajín, ktoré to považujú za nevyhnutné pre vlastné jedinečné dôvody.[10] Medzi najznámejšie patrí Rusko, kde je prenikavá cenzúra. To znamená, že pod cenzúru spadá veľké množstvo informácii rôznych kategórii. Naopak, takmer žiadna cenzúra nie je v štátoch USA, západnej Európe a na juhu Afriky. Ani táto oblasť nie je čierno biela a klasifikácia cenzúry je obšírnejšia.[11] V jednoduchosti a v skratke by sme mohli povedať, že firma sa riadi zákonmi tej krajiny, v ktorej sídli.

Na tomto príklade sme chceli v krátkosti vysvetliť, čím sa GBDe zaoberá. Je to organizácia, ktorá poskytuje kvantum informácii, ktoré sú dostupné aj bežnému používateľovi internetu. Zámerne sme vybrali pre objasnenie príklady legálneho používania počítačov, no GBDe poskytuje informácie z rôznych oblastí kyber priestoru.

2. Komunikácia v rámci informačných systémov - Interoperabilita

V tejto časti len okrajovo spomenieme túto problematiku, z dôvodu jej obšírnosti. Keď sa zameriame na informačné systémy ako také, samostatná ich existencia by nebola až taká efektívna nebyť ich vzájomného prepojenia. Interoperabilita je schopnosť informačného systému používať informácie a funkcie iného systému používaním spoločných štandardov.[12]

Schopnosť vymieňať si údaje a zdieľať informácie a vedomosti. Na nadnárodnej úrovni sa problematikou interoperability zaoberá Európska komisia v rámci skupiny IDA (Interchange of Data between Administrations), ktorá v roku 2004 publikovala návrh rámca interoperability EIF (European Interoperability Framework), ktorý má podporovať poskytovanie celoeurópskych služieb elektronickej správy e-governmentu.[13]

Na základe dokumentu „Európsky rámec interoperability pre paneurópske e-Government služby“ rozlišujeme sa tri aspekty (úrovne) interoperability:

- **organizačná** - definovanie podobných cieľov biznisu, modelovanie biznis procesov, zavádzanie spolupráce administratív a zohľadnenie používateľských požiadaviek,
- **sémantická** - porozumenie vymieňanej / poskytovanej informácii nezávisle od zariadenia a cieľa,
- **technická** - technologické prepojenie systémov a IT technológií.[14]

2.1. SIS

Možno sa po prečítaní prvých strán môže zdať, že dnešná miera informovanosti je až nekomfortne obšírna, hlavne čo sa týka možnosti vystopovať osobu, a teda aj Vás práve tam, kde čítate tento príspevok. Tu Vám však demonštrujeme, že vďaka informačným systémom je možné vypátrať osobu, ktorá je medzinárodne hľadaná. „Schenhenský informačný

---

10 http://www.gbde.org/legal-use-of-computers/.
11 http://en.wikipedia.org/wiki/Internet_censorship_by_country.
12 http://portal.gov.sk/Portal/sk/Default.aspx?CatID=89.
13 http://www.informatizacia.sk/interoperabilita/3481s.
14 http://www.informatizacia.sk/interoperabilita/3481s.

systém" (SIS) je databázou, ktorá pomáha členským krajinám v pátraní po osobách a veciach. Na zhrnutie činnosti SIS je namieste uviesť prehľadne, čím sa zaoberá:

- osobami, na ktoré sa vzťahuje požiadavka na ich zatknutie či odovzdanie na základe európskeho zatýkacieho rozkazu, alebo osobami, na ktoré sa vzťahuje požiadavka na vzatie do predbežnej väzby za účelom ich vydania;
- štátnymi príslušníkmi tretích krajín, ktorým je nutné odoprieť vstup na územie schengenských krajín;
- nezvestnými osobami, ktoré v záujme svojej vlastnej ochrany, alebo predídeniu nebezpečia musia byť dočasne pod policajnou ochranou;
- osobami, u ktorých je potrebné zistiť pobyt za účelom trestného konania;
- osobami a predmetmi, ktoré sú predmetom skrytej kontroly alebo špecifickej kontroly;
- stratenými alebo ukradnutými predmetmi, alebo predmetmi hľadaných za účelom zaistenia dôkazov v trestnom konaní (napr. ukradnuté, neoprávnene používané alebo zmiznuté motorové vozidla, strelné zbrane, nevyplnené úradné doklady, bankovky, ukradnuté kreditné karty, atď.).[15]

Do SIS prispievajú členské krajiny Schengenu priamo zo svojich národných pátracích databáz. SIS má aj zoznam nežiaducich osôb, má ho však aj Interpol. S týmto zoznam prichádza do styku veľmi málo ľudí. Krajiny Schengenu: 22 členských krajín EÚ, ktoré sa dohodli medzi sebou na zrušení hraničných kontrol. Do tohto priestoru patrí aj územie pridružených krajín Európskeho hospodárskeho spoločenstva (EHP) a od 12. decembra 2008 aj územie Švajčiarska. Spolu je to teda územie 25 európskych krajín.[16]

3. Prístup k internetu – ponímané ako ľudské právo?

Vynálezca internetu Sir Tim Berners-Lee John povedal: "Prístup na web je teraz ľudské právo. Je možné žiť bez internetu, no nie je možné žiť bez vody. Ale ak máš vodu, potom rozdiel medzi niekým kto je pripojený k internetu a súčasťou informačnej spoločnosti a niekým kto nie, je stále väčší a väčší".[17] V nadväznosti na tento výrok sme poukázali aj na fakt, že aj keď je tu internet od roku 1960, až dnes sa stal súčasťou prakticky všetkých aspektov moderného ľudského života. Stal sa nenahraditeľným nástrojom na realizáciu celej rady ľudských práv, v boji proti nerovnosti a je prostriedkom na urýchlenia ľudského pokroku. Práve pre to by mala byť čo najväčšia snaha štátov o zabezpečenie jeho univerzálneho prístupu. Osobitný spravodajca OSN Frank La Rue je názoru, že internet je jedným z najmocnejších nástrojov 21. storočia na zvýšenie transparentnosti v správaní mocných, prístupu k informáciám, ako aj na uľahčenie aktívnej účasti občanov pri budovaní demokratickej spoločnosti. Dodal, že nedávna vlna demonštrácií v krajinách Blízkeho východu a severnej Afriky ukázala, že internet môže zohrať kľúčovú úlohu pri mobilizácii populácie a jej hlasu po spravodlivosti, rovnosti, zodpovednosti a lepšieho dodržiavanie ľudských práv.[18] My zdieľame jeho názor, keďže je isté, že rast používateľov internetu sa nedá spochybniť a tým je priamočiara aj rastúca krivka informovanosti jeho používateľov, čo

---

15 http://www.euroinfo.gov.sk/schengensky-informacny-system-sis-mozog-schengenu/.

16 http://www.euroinfo.gov.sk/co-je-schengensky-priestor/.

17 OSN deklarovalo prístup na internet ako základné ľudské právo, inet.sk, 14.06.2011, dostupné online: http://archiv.inet.sk/11668-komentar-osn-deklarovalo-pristup-na-internet-ako-zakladne-ludske-pravo.html.

18 Tamtiež.

v neposlednom rade prospieva k mobilizácii populácie a k ďalším spomínaným aspektom. Touto problematikou sa zaoberá viac dohovorov, namieste je však spomenúť Medzinárodný pakt o občianskych a politických práv, ktorého článok 19 ods. 3 znie nasledovne: „Užívanie práv uvedených v odseku 2 tohto článku nesie so sebou osobitné povinnosti a zodpovednosť. Môže preto podliehať určitým obmedzeniam, tieto obmedzenia však budú len také, aké ustanovuje zákon a ktoré sú nevyhnutné:

a) na rešpektovanie práv alebo povesti iných;

b) na ochranu národnej bezpečnosti alebo verejného poriadku alebo verejného zdravia alebo morálky.“[19]

Tu sme preukázali, že prístup na internet má už aj inštitucionálny rámec a odrezanie používateľov od prístupu k internetu je porušením citovaného odseku.

3.1. Sloboda prejavu a sloboda protestovania na internete

Európsky dohovor o ochrane ľudských práv a základných slobodách zakotvuje vo svojich štrnástich článkoch aj slobodu prejavu (čl. 10). Týka sa aj internetu. No ako je to vlastne so slobodou protestovania? V nedávnej minulosti sme mali možnosť sledovať aktuálne dianie v kyber priestore týkajúce sa Slovenskej republiky. Aktivisti z hnutia Anonymous odstavili a znefunkčnili stránku generálnej prokuratúry. Cieľom útoku bola podpora protestu proti vývoju v kauze Gorila.[20] Podobných Tu sa vynára ďalšia otázka, či je to vôbec legálny spôsob protestu, ktorý neodporuje súčasnej legislatíve. V Amerike žiadajú aktivisti Anonymouse prezidenta Obamu o uznanie DDoS (Distributed dential-of-service) útoku ako legálnu formu online protestu.[21] Svoju petíciu odôvodňujú tým, že s rozvojom technológii a internetu prichádzajú nové možnosti na protest. Nepovažujú to za formu hackingu, ale ako ekvivalent k protestom konajúcim sa v reálnom svete. My sa s ich názorom nestotožňujeme úplne, keďže nabúranie na sa cudziu stránku je nelegálne ale zároveň súhlasíme s časťou, ktorá pojednáva o proteste. Aj v reálnom živote môžeme protestovať, avšak zákonom vymedzeným spôsobom. Tu sa žiada, aby sme v krátkosti priblížili činnosť hackera. Samotný pojem má neutrálny charakter, o jeho náboji sa rozhodne v závislosti od toho, do akej sféry sa hacker nabúra a ako ďalej využíva informácie, ktoré svojimi zručnosťami v IT svete získal. Ak sa činnosť hackera dostane až na súd, vyrieknutie trestu bude znamenať, že virtuálne kroky majú dohru v reálnom svete. Clemens Kurtenbach, špecialista na boj s počítačovou kriminalitou zo španielskej Pamplony tvrdí, že v tom prípade ich činnosť nenazývame hackovaním, ale cybekriminalitou.[22] Dvadsiatka expertov na vojenské a internetové právo zverejnila dokument *Tallinský manuál o medzinárodnom práve aplikovateľnom na kybervojnu*, ktorý má pre NATO odporúčací charakter. Zaoberali sa v ňom aj otázkami kyberútokov a ochranou ľudí, ktorí takéto útoky páchajú či sú ich obeťami. Výsledkom je, až ak sú následkom kyberútoku značné hospodárske škody, verejné ohrozenie či dokonca obete, je takýto útok považovaný za vojnový akt. Obzvlášť, ak sa ho dopustí jeden

---

[19] Medzinárodný pakt o občianskych a politických právach. Uverejnený pod číslom 120/1976 Zb.

[20] Anonymous odstavili web Generálnej prokuratúry kvôli podpore protestu Gorila, Živé.sk, 09.09.2012, dostupné online: http://www.zive.sk/anonymous-odstavili-web-generalnej-prokuratury-kvoli-podpore-protestu-gorila/sc-4-a-303595/default.aspx.

[21] Anonymouse žiadajú Obamu aby uznal DDoS útoky ako legálnu formu online protestu, Svet IT, 10.01.2013, dostupné online: http://www.svet-it.sk/2013/01/anonymouse-ziadaju-obamu-aby-uznal-ddos-utoky-ako-legalnu-formu-online-protestu/.

[22] LASZLÓOVA, K.: Hackeri, iŽurnál, 09.09.2009, dostupné online: http://www.izurnal.sk/index.php?option=com_content&task=view&id=3336.

štát voči inému.[23] Hackeri sú zväčša civilisti a tak majú právo na ochranu, akú v konfliktoch majú podľa Ženevskej konvencie civilní obyvatelia. To znamená, že ak niekto hackera za podmienok stanovených v tomto dokumente a teda, ak kyberútok možno považovať za vojnový akt, nemôže byť súdený za vojnové zločiny.

Naša legislatívna úprava online protesty výslovne nezakazuje, avšak nie je úplne jasná ani definícia pojmu „zhromažďavanie" podľa zákona 84/1990 Zb. o zhromažďovacom práve. Otázka teda podľa nášho názoru nestojí tak či je možné v kyberpriestore vôbec protestovať, ale skôr či je možné ešte považovať DDoS útoky za súčasť *práva pokojne sa zhromažďovať*. Naša ústava v čl. 28 na túto otázku priamo neodpovedá, odkazuje nás však na spomínaný zákon. Naša podústavná úprava zhromažďovacieho práva pamätá predovšetkým na fyzické protesty a nie online protesty. Niektoré ustanovenia sú teda zjavne neaplikovateľné na protest v kyberpriestore (§ 4 ods. 2, § 7 ods. 3 a pod.).[24] Stručným zhrnutím by sme mohli konštatovať, že to, do akej miery je protest protizákonný a do akej mieri ešte spadá pod slobodu zhromažďovania, možno zistiť až *ex post* po vznesení prvých obvinení a uložení prvých pokút.

---

[23] Poradcovia NATO: Hackerov môžete zabiť, Sme, 22.03.2013, dostupné online: http://tech.sme.sk/c/6743302/poradcovia-nato-hackerov-mozete-zabit.html.

[24] HUSOVEC, M.: Ako je to vlastne so slobodou protestovania na internete, MicroBlog Priateľov EISI, 10.09.2012, dostupné online: http://blog.eisionline.org/2012/09/10/ako-je-to-so-slobodou-protestovania-onlin/.

Regulácia internetu na medzinárodnej úrovni – spôsoby, minulosť a budúcnosť, obsah právnej úpravy, regulované vzťahy

Dominika Becková

Internet a jeho právna úprava je témou, ktorá je aj v súčasnosti veľmi živou, keďže sa začala rozoberať len v nedávnej minulosti. To je jedným z dôvodov prečo sa právne odvetvie internetového práva neustále vyvíja a zdokonaľuje. Dnes si už nevieme život a svet bez internetu predstaviť, ale nie vždy tomu tak bolo. Internet pre nás predstavuje zdroj nových informácií, myšlienok a prostredníctvom neho sú ľudia informovaní o dianí vo svete. Teda internet pre spoločnosť plní veľmi významnú funkciu. Spolu s rozpínaním sa pôsobnosti internetu do jednotlivých sfér spoločenského, ale aj politického života sa do popredia dostávali otázky, či nie je potrebné zaviesť pravidlá užívania internetu a prostredníctvom nich obmedziť jeho obsah. Jednotlivé štáty sa spočiatku prikláňali k regulovaniu internetu na regionálnej úrovni, prostredníctvom prijímania právnych úprav záväzných len pre danú krajinu, poprípade oblasť. Takáto regulácia sa spočiatku ukazovala ako účelná, ale konflikty medzi štátmi, ohľadom toho čo môže a nemôže byť zverejňované na internete a taktiež aj viacero sporov medzi nimi, presvedčili spoločenstvo že bude účelnejšie ak sa pre priestor internetu vytvorí jednotná právna úprava. Tu sa otvoril priestor pre medzinárodné právo, aby prostredníctvom svojich nástrojov začalo regulovať internet.

1. Minulosť a internet

Vznik internetu v druhej polovici 20. storočia a jeho pozoruhodné sa rozšírenie do mnohých krajín sveta vyvolalo veľký údiv. V tomto období si ľudia začínali uvedomovať silu internetu a hlavne jeho prospech pre ľudstvo. Informácie sa stali prístupné každému, bez ohľadu na to kde sa nachádza. Internet sa stal nástrojom demokratizácie spoločnosti. Predstavoval samostatný priestor, ktorý bol úplne odlišný od reálneho sveta, a práve to ho robilo výnimočný a preto bolo veľmi ťažké, ba dokonca sa zdalo až nemožné ho v danom období právne regulovať.[1]

1.1. Etapa „otvoreného“ internetu

V počiatku tohto obdobia pre štáty nebola dominantná otázka právnej regulácie internetu. Tá vyvstala až neskôr, keď sa začalo diskutovať o tom, či internet možno vôbec považovať za priestor. V histórii vývoja internetu a jeho právnej regulácie sa vyvinulo viacero problémov a myšlienkových smerov. Ľudstvo sa ocitlo na rozhraní 2 budúcich možností, ktoré internet so sebou prináša. Na jednej strane stála budúcnosť plná privatizácie a vlastníctva majetku duševnej činnosti, na strane druhej budúcnosť, kde záujmy spoločnosti presahovali vo veľkom záujmy jednotlivcov a kde bude internet ako nový priestor prístupný pre všetkých.[2]

Táto problematika sa spája aj so sférou práv duševného vlastníctva, ako autorské právo a patenty. Tieto práva sa stali najohrozenejšími v dôsledku toho, že ich bolo možné veľmi rýchlo rozšíriť na internete a tým mohlo dôjsť a napokon aj došlo k ich masívnemu zneužívaniu. Išlo o priestor, hoci len abstraktný, ktorý bol prístupný pre všetkých, na ktorom mohol každý komunikovať, kde si každý našiel to čo ho zaujíma a mohol sa obohacovať

---

1 SEGURA – SARRENO, A.: Internet regulation and the role of International law.

2 PALFREY, J.: Four Phases of Internet Regulation.

o nové poznatky. Ľudia si na internete začali postupne vytvárať malé komunity (zoskupenia) v rámci, ktorých si začali formovať vlastné pravidlá, ktoré im vyhovovali. Išlo o nekonečný priestor: otvorený, voľný a naplnený možnosťami. Dominovala predstava o internete ako o priestore, ktorý je ohraničený len nárokmi jeho používateľov. Internetový priestor sa pomaly začal rozdeľovať na časti, ktoré si ale neboli veľmi vzdialené. Začal vznikať spor o to či internet možno označovať pojmom priestor, keďže nemá stanovené hranice svojej pôsobnosti. V prvých rokoch jeho existencie bol považovaný za priestor v pravom zmysle slova. Hlavným argumentom tejto teórie bolo to, že ide o priestor samostatný a taký, ktoré je možné právne regulovať. Tento názor bol v priebehu nasledujúcich rokoch prekonaný, keď sa koncom 20. storočia dospelo k názoru, že argumentovať tým že ide o priestor v pravom slova zmysle bolo nelogické. Internet ako reálny priestor vlastne neexistuje, pretože nie je nijako ohraničený, nemá vlastných obyvateľov.

Uvažovanie o kyberpriestore ako abstraktnom priestore podnietilo sudcov, tvorcov zákonov a predovšetkým právnych vedcov k uvažovaniu či naše „fyzické" predpoklady môžu byť do tohto priestoru premietnuté. Vlastníci internetových zdrojov začali rozmýšľať nad www stránkami a e-mailovými systémami ako ich vlastnými nárokmi v tomto novovznikajúcom priestore, ktoré musia byť chránené pred zásahmi ostatných ľudí. To viedlo k sérií prípadov a myšlienok týkajúcich sa súkromného sektora v kyber oblasti.

Tento efekt spôsobil, roztrieštenosť internetového priestoru do mnohých častí. Súkromné záujmy boli a aj sú dominantnou formou alokácie zdrojov v tomto svete. Išlo o premenu práva jednotlivca na právo ktoré nemá nikto, teda nikto nemá efektívnu moc na jeho používanie.

Chápanie internetu ako priestoru a následky dovtedajšej právnej úpravy viedli spoločenstvo smerom vytvárania mnohých roztrúsených práv v rámci jedného odvetvia, ktoré ničili prvotnú myšlienku internetu ako spoločného priestoru otvoreného pre všetkých. Tieto práva ničili taktiež zvyky ako povaha internetu, ktorá predtým viedla k veľmi neobyčajnej inovácií a poskytovala nové možnosti.

1.2. Debata o regulácií internetu

Vzhľadom k virtuálnej povahe existencie internetu sa prvá dôležitá právna diskusia o internete zamerala na prirodzený odpor regulácie tohto priestoru. Napriek tomuto počiatočnému odporu vnútroštátneho práva boli postavené po celú dobu vo svete cieľu a efektu podriadenia internetu skutočnej, to znamená reálne existujúcej regulácii. Vzhľadom na globálny charakter, ktorý internet má, sa ukázalo že medzinárodné právo bude v niektorých oblastiach vhodnejším nástrojom na jeho reguláciu.

Od počiatku rozvoja internetu, existovala debata či je vhodnejšie regulovať alebo neregulovať toto nové pole aktivity. Či je to vôbec možné a žiaduce regulovať internet alebo či naopak internet je v podstate voľným miestom, virtuálne terra nullius? Pozícia liberálov bola ovplyvnená pár akademikmi, predovšetkým z USA, počas 90. rokov, kedy sa internet rozširoval z malých komunít k veľkej populácii. Podľa liberálov internetový priestor nemôže a navyše ani nesmie byť regulovaný. Nielenže, je to nemožné pre štát regulovať internet, ale je tiež žiaduce, aby bol internet bez štátnej regulácie. Štáty stáli oproti reálnym problémom voči tomu, ako pokryť a zabezpečiť právnymi pravidlami ochranu internetu a riadiť činnosti na ňom vykonávané. Kyber priestor sám o sebe, ako neobmedzený priestor predstavuje realizáciu liberálnych a demokratických myšlienok.[3]

---

[3] SEGURA – SARRENO, A.: Internet regulation and the role of International law.

V rámci tejto debaty sa vykryštalizovali 2 popredné názory, respektíve dve veľké skupiny:

a.) Samoregulácia – vytváranie pravidiel samostatnými používateľmi internetu v procese jeho využívania a objavovania všetkých jeho prvkov
b.) Štátna regulácia – vytváranie pravidiel samotnými štátmi, ktoré nepripúšťali myšlienku, aby internet ostal bez zásahov vnútroštátnej právnej úpravy.

Liberáli sa snažili o vytvorenie miesta pre *netcitizens* – teda obyvateľov internetu, ktoré bolo prebraté z tradičných národných, teda štátnych pravidiel. Po opisnej stránke liberáli tvrdili, že keďže niet hraníc v kyberpriestore, žiadne snahy teritoriálnych suverenít ho nemôžu regulovať. Internet je všade a nikde, teda je mimo jurisdikčnej sféry, pretože žiadna zo suverenít štátov nemá žiaducejší cieľ ako iný subjekt, teda nemôže byť regulované jedným štátom tak, aby zároveň neoprávnene nezasahovalo do jurisdikcie iného štátu a ovplyvňovalo výber inej krajiny. Taktiež by to bolo problematické pre netcitizens orientovať sa, podľa ktorého práva používajú internet. Z pohľadu zástancov tohto názoru bolo najrozumnejšie namiesto štátnej regulácie, poskytnúť samoreguláciu, založenú na myšlienke delegácie, tzv. neformálne pravidlá nazývane „*Netiquette internet etiquette*", sformované vo vývoji používania internetu jeho samotnými užívateľmi a akceptované bussiness ľuďmi a ľuďmi, ktorí dáta na internete sprostredkuvávajú. Tieto pravidlá viac sedia potrebám internetového priestoru ako novej virtuálnej komunity, pretože boli vytvorené v praxi. Netcitizens sú skutoční a legitímni tvorcovia tohto nového sociálneho priestoru, tzv. ľudskí právnici – ideologický trend spoločnosti najmä v USA.[4]

Jedným z problémov samoregulácie bolo ako ďaleko môže zájsť, teda vynárala sa otázka či každá oblasť existujúca v rámci internetového priestoru bude podliehať pravidlám samoregulácie alebo či budú existovať aj oblasti, do ktorých bude zasahovať jurisdikcia štátov.

Internet v ponímaní voľného a nezávislého priestoru teda nemohol podliehať suverénnej jurisdikcii štátu tiež preto, že bol vzdialený akejkoľvek doterajšej úprave. Štáty si nevedeli stanoviť ciele, ktoré by prostredníctvom tohto nového média chceli dosiahnuť. Jedným z ďalších teoretických problémov bolo, v čom je internet rozličný, v tom aký je a aký by mal byť, to znamená či predstava o tom aký internet bude a načo sa bude využívať sa skutočne stotožňuje s tým, aký internet v skutočnosti je. Niektorí teoretici prišli s možnosťou právnej úpravy internetu na základe kombinácie princípu samoregulácie a štátnej regulácie, táto možnosť by zabezpečila určite legitímnosť, flexibilitu a vymáhateľnosť požiadaviek na internetovú reguláciu tak aby sa stala fungujúcim právnym systémom.

Ukazovalo sa, že najlepším regulátorom internetového práva by malo byť práve spojenie národného práva s prvkami samoregulácie a medzinárodného práva. Na národnej úrovni boli prijaté viaceré akty – napr. *National Commerce act, Computer Crime Enforcement act*, atď. Úlohou medzinárodného práva sa stalo dopĺňanie medzier národných úprav prostredníctvom jeho nástrojov.

2. Súčasnosť a internet

Štáty samotné spolu s medzinárodnými organizáciami, začali rozmýšľať o potrebe blokovania a obmedzovania aktivít a vyjadrení na internete. Dôvody, ktoré ich k tomu viedli boli rôzne, ale prevažujúcim bolo zabránenie porušovania práv jednotlivcov. Nie všetky štáty tak ale robili z tohto dôvodu, niektoré sa snažili o túto reguláciu predovšetkým preto, aby

---

4 DE VEY MESTDAGH, C N J. and RIJGERSBERG, R W.: Internet governance and global self regulation: Theoretical and empirical building blocks for a general theory of self regulation.

zabránili obyvateľom v prístupe k určitým informáciám. Najprísnejšie to bolo v Číne, kde došlo k zakázaniu prístupu k obsahom mnohých článkov. Vzhľadom na rýchlo meniaci sa obsah na internete, ktorý sa rozširuje a ktorý často krát porušuje základné práva jednotlivcov, štáty museli túto otázku vyriešiť čím skôr.

2.1. Možnosti regulácie používania internetu

V pomerne krátkom čase internet začal zasahovať do našich životov rýchlo a to v každej oblasti ľudských možností. Prostredníctvom neho majú ľudia prístup k novým myšlienkam, neobmedzeným možnostiam a k celému radu svetových komunít. To ako veľmi rýchlo sa internet rozmáhal a vyvíjal ovplyvnilo to, ako ľudia konajú, ako si dohadujú biznis, ako sa učia a ako máme postupovať v reálnom živote deň čo deň. Vzhľadom na to ako menil životy jeho používateľov (teda takmer celého ľudstva), v priebehu jeho vývoja sa aj on sám menil a zdokonaľoval.

Možnosť existencie predpisov, ktorých cieľom je nariadiť neutralitu internetu bola predmetom búrlivej diskusie po celom svete. Internetová regulácia vo svojej podstate predstavuje obmedzenie alebo kontrolu prístupu k niektorým aspektom alebo informáciám.

Internetová regulácia sa skladá z viacerých častí, ale medzi tie hlavné je možné zaradiť cenzúru údajov a kontrolných aspektov internetu, ako aj kontroly jednotlivých internetových stránok, IP adries a podobne.[5]

Ako internet v súčasnosti funguje? Funguje vďaka tomu, že je možné sa pripojiť z jednej siete na akúkoľvek inú sieť, a to je dôvod, ktorý umožňuje každému vytvoriť si vlastný účet, stránku, ponúkať služby a predávať produkty bez nutnosti povolenia centrálneho orgánu. Teda ide o priestor, ktorý je prístupný každému z nás. Internet pozostáva z desiatok tisíc poprepájaných sietí spravovaných servisnými správcami, súkromnými spoločnosťami, univerzitami, vládami a mnohými inými. Technická koordinácia internetu má niekoľko zvyčajných charakteristík, medzi ktoré zaraďujeme: otvorenosť, nezávislosť a to, že je prevádzkovaný neziskovými organizáciami, ktoré spolupracujú, aby zjednotili potreby všetkých. Takáto samoregulácia internetu bola kľúčom k úspešnému rozvoju internetu a je taktiež dostatočne flexibilná pre prispôsobovanie sa zmenám v budúcnosti.[6]

2.2. Súčasná úloha medzinárodného práva v oblasti internetovej regulácie

V rámci internetovej regulácie možno hovoriť o 3 pomerne širokých okruhoch problémov, ktoré medzinárodne právo rieši prioritne, pretože predstavujú najväčší zdroj problémov medzi štátmi.[7]

a.) Ochota časti štátov (prevažne európskych krajín) kontrolovať a odstraňovať škodlivý obsah nachádzajúci sa na internete a zároveň ochraňovať právo na slobodu prejavu (záujem USA). Otázky jurisdikcie a výberu medzi suverénnymi právami jednotlivých štátov.
b.) Ochrana práv duševného vlastníctva – autorské právo a ostatné práva sú vo veľkej miere zneužívané, predovšetkým kvôli existencii softvéru, ktorý umožňuje voľnú distribú-

---

5 What is the Internet? Dostupné online: http://www.internetsociety.org/internet/what-internet.
6 http://www.internetsociety.org/internet/how-it-works.
7 SEGURA – SARRENO. A: Internet regulation and the role of International law.

ciu materiálov. V tomto prípade, sú nástroje medzinárodného práva využívané na zabránenie rozširovania tejto aktivity.

c.) Ochrana osobných údajov proti ich ilegálnemu používaniu niektorými organizáciami operujúcimi na internete, čo dospelo k dohovoru medzi hlavnými aktérmi v boji proti tomuto problému a to USA a Európskou úniou.

Ad. 1.) Konflikt medzi slobodou prejavu a škodlivým obsahom

Jedným z najzávažnejších problémov medzinárodnej regulácie internetu je konflikt medzi slobodou prejavu a škodlivým obsahom dokumentov nachádzajúcich sa na internete. Silným zástancom slobody prejavu je USA, kde je toto právo ústavne chránené v prvom dodatku americkej ústavy.[8] Európske krajiny a Austrália majú viac záujem na kontrolovaní materiálov na internete a odstránenia tých, ktoré majú škodlivý obsah. Medzi štáty, ktoré vyvíjajú najväčšie úsilie patrí predovšetkým Nemecko a Francúzsko. Problémy týkajúce sa právnej regulácie vyplývajú predovšetkým z tohto konfliktu, teda sú veľmi často spájané s bojom medzi svetovo dostupnou možnosťou nájdenia a publikovania dát na internete, ktoré sú proti základným princípom toho ktorého štátu a ústavnou ochranou slobody prejavu, ako výrazu prostriedku v mnohých štátoch, kde sú dáta prístupné. Jedným z najznámejších prípadov týkajúci sa tejto otázky je prípad CompuServe, ktorý sa odohral v Nemecku. Súvisel so zverejňovaním násilia a detskej pornografie. Obsah bol publikovaný na amerických serveroch. Potom čo bol celosvetovo zakázaný obsah týchto materiálov, CompuServe vykonal kontroly a sprístupnil tento portál znova. Súd v Mníchove, ktorý o tejto otázke rozhodoval vyriekol: „Tvrdenie o slobode prejavu v krajine, kde sa nachádzajú zdroje sa dostalo do rozporu s prísnejšou legislatívou v krajine, kde sa tieto dáta ocitli. Ochraňovať také hodnoty ako je právo na súkromie, obmedziť by sa mali nenávistné výroky, urážka na cti a zakázať obscéznosť a pornografiu. Voľnosť v prístupe k týmto informáciám naráža na negatívne právo dostávajúceho štátu chrániť sa proti vonkajším vplyvom."[9] Tento konflikt možno poukázať aj na spore Yahoo!, ktorý vznikol medzi USA a Francúzskom. Francúzsko sa v tomto spore rozhodlo uplatňovať svoje právo, proti škodlivým zdrojom pochádzajúcim zo zahraničia na svojom území. Prípad tiež potvrdil, že v cezhraničných sporoch, v ktorých môže vzniknúť problematika slobody prejavu, nie je rozhodujúca právna regulácia v krajine poskytovateľa informácií, ale právne úprava v krajine príjemcu.[10]

Nemecko, Francúzsko a Austrália ako demokratické krajiny si vybrali pravidlá pre slobodu vyjadrovania, ktoré sú obsiahnuté v medzinárodnom dohovore o ľudských právach, ale ten nezodpovedá ochrane poskytnutej prvým dodatkom americkej ústavy. Je možné povedať, že takéto rozhodnutie ide proti základným princípom slobody vyjadrovania a slobody na prístup k informáciám na internete. Internet bol vybudovaný ako voľný priestor a nehovorí o tom, ako by mal vyzerať. Technická inovácia poveruje suverénne štáty, aby vytvorili pravidlá smerujúce k usmerňovaniu aktivity na internete. Exteritoriálna regulácia

---

8 *„Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."* V slovenskom preklade: „Kongres neschváli žiadny zákon ohľadom zavádzania náboženstva alebo zakazujúci jeho slobodný výkon; taktiež neschváli žiadny zákon obmedzujúci slobodu slova alebo tlače; neschváli ani žiadny zákon obmedzujúci právo ľudí pokojne sa zhromažďovať a právo odovzdávať štátnym orgánom žiadosti o nápravu krívd."

9 KUNER, Ch.: Judgment of the Munich Court in the „CompuServe Case" (Somm Case), commentary, dostupné online: http://www.kuner.com/data/reg/somm.html.

10 SEGURA – SARRENO, A.: Internet regulation and the role of International law.

na internete je teda ponechaná na úpravu v jednotlivých štátoch do doby, kým sa nevytvorí medzinárodný systém jej regulácie.

Ad. 2.) Ochrana práv duševného vlastníctva

Spolu s nástupom internetu, ochrana práv duševného vlastníctva (predovšetkým autorského práva), bola zmenená novými technológiami a softvérmi, ktoré povoľovali distribúciu digitálnych prác chránených vlastníckym právom. Takáto situácia dovoľovala ľuďom používajúcim internet sťahovať perfektné kópie pesničiek, filmov alebo iných prác, predtým chránených existujúcim štátnym právom a medzinárodnými dohodami. Teda dochádzalo k vzniku masívneho pirátstva na internete. Po prvých takýchto neoprávnených zásahoch do práv okamžite nasledovala odpoveď štátov v podobe hľadania nových pravidiel národného práva, ktoré by ochraňovali tradičné hodnoty práv duševného vlastníctva. Ako príklady možno uviesť No Electronic Theft act (NET Act) v USA alebo DMCA. V rámci európskych krajín to bol Copyright Directive. Súdy pri svojom rozhodovaní vynaložili veľmi veľa úsilia zaoberajúc sa otázkou ochrany autorského práva tak, aby na jednej strane nebolo obmedzené právo na prístup k informáciám, ale na strane druhej, aby sa poskytovala náležitá ochrana aj autorskému právu. Hranica medzi týmito právami je ale veľmi tenká a preto je veľmi problematické ju upraviť tak, aby nedošlo k porušeniu ani jedného z nich. Popri tomto probléme sa vynorila aj otázka technická, ktorá spočívala v tom, ako sa táto právna ochrana bude realizovať, čo predstavovalo v praxi veľmi veľký problém. Úsilie medzinárodných organizácií v oblastí práv duševného vlastníctva sa premietlo do uzavretia WIPO Copyright Treaties. Prostredníctvom týchto dohovorov došlo k právnej úprave používania internetu, ktorých nosnou myšlienkou bolo ochraňovanie práv duševného vlastníctva. WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) bol zlomovým pre medzinárodno-právnu reguláciu a ochranu autorského práva, pretože ochranu tohto práva zaviedol celosvetovo. TRIPS – Dohoda o obchodných aspektoch práv duševného vlastníctva je medzinárodnou dohodou navrhnutou Svetovou obchodnou organizáciou (WTO), ktorá stanovuje minimálne štandardy pre rôzne formy práv duševného vlastníctva.[11] Táto dohoda premietla práva duševného vlastníctva do oblasti medzinárodného obchodu po prvý krát a do súčasnosti je ich najkomplexnejšou úpravou, aj napriek tomu že do platnosti vstúpila 1.1.1995. Táto dohoda je zatiaľ jedinou multilaterálnou obchodnou dohodou, ktorá sa venuje výlučne právam duševného vlastníctva v 3 oblastiach: medzinárodné štandardy, vymožiteľnosť týchto práv a riešeniu sporov. Pokrýva predovšetkým oblasť autorského práva, ochranných známok, zemepisného označenia, priemyselných vzorov, patentov, topografie polovodičových výrobkov. V rámci WTO bola vytvorená osobitná Rada pre TRIPS[12] a WTO spolupracuje v oblasti duševných práv predovšetkým so Svetovou organizáciou pre duševné vlastníctvo a Svetovou zdravotníckou organizáciou.[13] Jednotlivé dohovory boli veľkým prínosom pre oblasť práv duševného vlastníctva a slúžia ako štandardy a minimá jeho ochrany v jednotlivých štátoch.

---

11 http://en.wikipedia.org/wiki/TRIPS_Agreement.

12 Rada pre TRIPS. Je orgánom, ktorý sa zaoberá oblasťou práv duševného vlastníctva v rámci WTO. Je tvorená zástupcami členských štátov WTO. Primárnou úlohou tejto rady je dohliadať na implementáciou Dohody TRIPS a viesť rokovania o nových skutočnostiach a navrhovaných úpravách v rámci tejto oblasti. Za Slovenskú republiky sa zasadnutí zúčastňuje predstaviteľ Ministerstva hospodárstva SR a ak je to potrebné tiež zástupca Úradu priemyselného vlastníctva SR.

13 http://www.economy.gov.sk/dusevne-vlastnictvo-trips-6618/128303s.

Ad.3.) Oblasť ochrany osobných údajov

V súčasnosti nie je neobvyklé, že dochádza k častému zneužívaniu osobných údajov, ktoré tvoria identitu človeka. Osobné údaje sú publikované v centrálne registrovanej databáze. Po dobu, kým internet neexistoval, nebolo ich ohrozenie až také nebezpečné a riziko ich zneužitie tak vysoké. Spolu s rozvojom internetu sa zmenila situácia aj v tejto oblasti a v súčasnosti omnoho viac subjektov využíva tieto osobné údaje, čo ohrozuje právo na súkromie a ochranu týchto informácií, preto ochrana osobných údajov sa stala jednou z dominantných tém v oblasti internetového práva. Svetový summit informačnej spoločnosti len potvrdil, že táto otázka je stále živá a jej právna regulácia je čoraz viac žiaduca. Oblasť ochrana osobných údajov, tak ako aj iné oblasti, nie je právne regulovaná, v národných právach jednotlivých štátov, na tej istej úrovni. Ako príklad je možné uviesť právnu reguláciu ochrany osobných údajov v USA a ich ochranu v rámci Európskej únie.

- USA bolo jednou z prvých krajín, ktoré začali právne regulovať súkromie, ale nie až vo veľmi vysokej miere pretože kladú veľký dôraz na prvý dodatok americkej ústavy, ktorý hovorí o slobode prístupu a získavania informácií, teda úloha štátov je tu limitovaná.
- V rámci Európskej únie je ochrana osobných práv upravená omnoho striktnejšie ako to je v USA. Existuje tu legislatíva, ktorá zakladá mnoho práv a povinností v procese používania osobných údajov iných osôb, ktorá je založená aj na myšlienke, že používatelia nie sú konzumentmi ale sú obyvateľmi. Striktné právne regulácie ochrany osobných údajov vyplývajú z Európskeho dohovoru o ľudských právach a ostatných medzinárodných dohovorov, ktoré hovoria že štáty európskeho regiónu sú zaviazané rešpektovať súkromie, rodinný život a domov.

Medzinárodné právo hralo významnú úlohu vo vzťahoch medzi štátmi, riešilo problémy ktoré vznikali vo vývoji, zaoberalo sa otázkou úpravy regulácie, riešilo konflikty medzi slobodou prejavu a obsahovou reguláciou, medzinárodné zmluvy a dohovory na ochranu práv duševného vlastníctva a osobných údajov. Teraz má medzinárodné právo ale omnoho významnejšiu úlohu a to reguláciu internetu. Jeho nástroje a inštitúty sa snažia reagovať na to, čo tu doposiaľ nebolo. Ide o otázky, ktoré majú nesporne charakter medzinárodného práva a preto je práve ono povolané na ich riešenie. Vynárajú sa otázky sebaobrany pri kybernetických útokoch, úprava internetu ako spoločného dedičstva celého ľudstva a možnosť, že sa právo prístupu na internet stane medzinárodným ľudským právom.

Ako už z predchádzajúceho textu vyplýva, snaha štátov o reguláciu internetu sa stávala prioritnou aj na medzinárodnej úrovni. Organizácia spojených národov v roku 2012 usporiadala konferenciu, na ktorej predstavila zmluvu týkajúcu sa regulácie internetu. Jej podstatou bolo obmedzenie obsahu nachádzajúceho sa na internete prostredníctvom cenzúry, ktorú budú vykonávať jednotlivé vlády. Túto zmluvu podpísalo 89 členských štátov medzinárodnej telekomunikačnej únie. Túto zmluvu nepodpísalo 55 členských štátov, k popredným odporcom patrili USA. Táto konferencia mala predstavovať určitú „aktualizáciu" medzinárodných telekomunikačných regulácií (ITRs) z roku 1988. USA ale tiež aj Google sa stali jej odporcami, vzhľadom na to, že negatívne zasahovala do činnosti internetu a nesúhlasili s vládnou kontrolou a obmedzovaním. Cieľom tejto konferencie a zmluvy bolo docieliť to, aby štáty a ich vlády, každý mali rovnakú zodpovednosť a rolu pri regulácií internetu, a aby spoločným úsilím dosiahli jeho medzinárodné regulovanie.[14]

---

[14] The UN Approved A Treaty Said To Let Governments Censor The Internet, Bussines Insider, 14.12.2012, dostupné online: http://www.businessinsider.com/un-signs-internet-regulation-treaty-2012-12.

3. Budúcnosť a internet

Je veľmi ťažké predpovedať budúcnosť niečoho tak dynamického ako je internet. Ale je možné s istotou povedať, že bude pokračovať v uplatňovaní doterajších nástrojov a hľadania nových tak, aby sa internet stal bezpečným. Už teraz sa uvažuje o ochrane podnikania na internete a jeho zvýšenej kontrole, vzhľadom na rapídnu rýchlosť jeho rastu a bohatej evolúcie nových produktov a ponúk. Možno veriť tomu, že internet dopomôže rozvoju vzdelávania, aktivít, ekonomike a mnohým ďalším oblastiam. Medzinárodné právo by svoju úlohu chcelo v tejto oblasti zvýšiť predovšetkým tak, že sa na neho nebude pozerať iba ako na nástroj, ktorý vypĺňa medzery národného práva, ale ako na nástroj ktorý bude komplexne upravovať problematiku internetového práva.

Internet a právo Európskej únie

Michaela Fabiánová

Úvod

Internet je v dnešnej dobe natoľko rozšírený, že si mnohí existenciu bez neho nedokážu predstaviť. Informačné a komunikačné technológie sú nenahraditeľnými pomocníkmi. Čím je však ich význam väčší a čím viac sme od nich závislí, tým väčšie problémy vznikajú pri ich neopatrnom používaní alebo zneužívaní. Právny poriadok sa len veľmi ťažko vysporadúva s takým fenoménom, akým je internet a technológiami, ktoré pracujú na jeho báze. Je to zapríčinené, predovšetkým, rýchlym tempom vývoja technológií, v porovnaní s pomalým tempom tvorby zákonov, globálnym rozmerom internetu a v konečnom dôsledku aj faktom, že internet ako taký nie je právnym subjektom. Jedna z najkomplikovanejších právnych situácií, ktorá vzniká s používaním internetu, je princíp teritoriality pri poskytovaní služieb, ktorá sa riadi konkrétnym právom krajiny, v ktorej sa daná služba poskytuje. V súvislosti s prebiehajúcou európskou integráciou, sa do popredia dostáva európske právo.

1. Právo Európskej únie

Európske právo označuje súhrn právnych noriem súvisiacich s činnosťou a existenciou Európskej únie. Tieto normy môžu byť vyjadrené v rôznych právnych formách, či už v medzinárodných zmluvách, ktoré sú výsledkom činnosti členských štátov, ale aj Európskej únie a Európskych spoločenstiev, alebo môžu byť vyjadrené v právnych aktoch orgánov Európskej únie, prípadne môžu mať podobu medzinárodnej obyčaje.[1]

Európska únia odvodzuje všetky svoje činnosti zo zakladajúcich zmlúv, ktoré sú dobrovoľne a demokraticky dohodované so všetkými členskými krajinami a ktoré tvoria tzv. *„primárne právo“.* Na ďalšie rozpracovanie primárnych prameňov práva je zamerané *„sekundárne právo EÚ“,* využívajúc pri tom atypické (biele a zelené knihy) a typické právne nástroje, ktoré sa ďalej členia na právne nezáväzné (odporúčania a stanoviská) a právne záväzné nástroje (smernice a nariadenia) – a práve prostredníctvom týchto právnych nástrojov sekundárneho práva, vychádzajúc z práva primárneho, reguluje EÚ aj kyberpriestor.

V Európe začala regulácia internetového priestoru získavať dôležitosť koncom 90-tych rokov 20. storočia. V súčasnosti je veľmi rozšírená. Európska únia podporuje spôsob samoregulácie on-line priestoru, ktorá je obsiahnutá v rozličných politických dokumentoch.[2]

Smernica stanovuje ciele, ktoré majú dosiahnuť členské štáty a na ktorých dosiahnutie si môžu zvoliť vlastné prostriedky, pričom môže byť určená členskému štátu, viacerým alebo všetkým členským štátom. Používa na zosúladenie vnútroštátnych právnych predpisov jednotlivých štátov. Na rozdiel od smerníc, ktoré sú určené členským štátom, **nariadenie** je určené všetkým. Je priamo uplatniteľným, všeobecne záväzným právnym aktom, ktorý prijíma Rada Európskej únie spolu s Európskym parlamentom alebo Európska komisia. Dnešná európska regulácia internetu predstavuje akúsi mozaiku rôznych právnych predpisov, ktoré upravujú niektoré časti spoločenského života v tomto priestore, počnúc právom na prístup k sieťam a službám poskytovaným on-line, či ochranou osobných údajov

---

1 MAZÁK, J., JÁNOŠÍKOVÁ, M.: *Základy práva Európskej únie.* Bratislava: IURA EDITION, 2009. Str. 211.

2 SAVIN, A.: *EU internet law.* Elgar European Law series, 2013. str. 14.

a bezpečnosti. Významným aspektom regulácie je elektronický obchod, v ktorom sa premietajú princípy voľného pohybu tovarov a služieb, ochrany spotrebiteľa, poskytovania finančných služieb na diaľku. Internet vo svojich širších súvislostiach presahuje aj do oblastí ako je hospodárska súťaž, e-government, vrátane elektronického verejného obstarávania, elektronického podpisu a opakovaného použitia informácií verejného sektora, až po ochranu duševného vlastníctva.

Problémy európskej regulácie súvisiacej s internetom však obsahujú oveľa širšie spektrum otázok patriacich k on-line priestoru a preto sa ani nedajú presne načrtnúť a zosumarizovať.

2. Prístup k sieťam a službám poskytovaným on-line

V súčasnosti približne 60% populácie v celej Európe používa internet pravidelne a 48% na dennej báze.[3] Užívatelia však každým dňom pribúdajú. Tento narastajúci trend súvisí, okrem iného, s neustálym napredovaním a modernizáciou informačných a telekomunikačných zariadení, ako aj s možným rozšírením základných ľudských práv o nové právo, ktorým by sa malo stať právo na slobodný prístup na internet.

Za uznanie tohto práva sa, 10. júna 2011, pridalo 41 krajín sveta k stanovisku, ktoré vzniklo na základe správy špeciálneho spravodajcu OSN pre podporu a ochranu práva na slobodu názoru a vyjadrovania pre Výbor OSN pre ľudské práva, Franka La Rue, podľa ktorého sa *"internet stal nenahraditeľným nástrojom boja za ľudské práva, proti nerovnoprávnosti, urýchľujúci vývoj a napredovanie ľudstva, a preto by malo byť zabezpečenie prístupu na internet prioritou každého štátu."*[4]

Vychádzajúc z poznatku, že Európska únia je zoskupením štátov, ktoré sa v jej prospech vzdávajú časti svojich národných suverenít, zabezpečenie prístupu na internet stalo prioritou práve tohto nadnárodného zväzku. Občania EÚ majú v súčasnosti k dispozícii základný súbor práv v oblasti prístupu a používania on-line sietí a služieb. Tieto práva podrobne opisuje *Kódex EÚ práv v on-line prostredí*. Tento kódex je kompiláciou základného súboru práv a zásad ukotvených v právnych predpisoch EÚ, ktoré chránia občanov EÚ pri prístupe k on-line sieťam a službám a ich využívaní.[5]

Každý v EÚ má nárok na základné a cenovo dostupné on-line služby dobrej kvality, ktoré môže využívať vo svojom domove.[6] Znamená to, že v každom členskom štáte EÚ musí pôsobiť aspoň jeden operátor schopný tieto služby poskytovať. V právnych predpisoch EÚ sa takýto prevádzkovateľ označuje ako *„poskytovateľ univerzálnej služby"*.[7] V súlade s princípom rovnosti a zákazom diskriminácie, má nárok vybrať si z dostupných poskytovateľov a služieb, ktoré využíva väčšina spotrebiteľov aj osoba so zdravotným postihnutím. Ak má používateľ zhoršený zrak, má nárok aj na osobitné zariadenia na zabezpečenie

---

3 Digital Agenda: investment in digital economy holds key to Europe's future prosperity, says Commission report, Communiqués de presse rapid, Brussels 17 May 2010, Dostupné na internete: http://europa.eu/rapid/press-release_IP-10-571_en.htm?locale=FR.

4 Freedom of Expression on the Internet Cross-regional Statement, speech of Carl Bildt, Minister of foreign affairs, Kingdom of Sweden, Human Rights Council, 17th session, 10 June 2011, Dostupné na internete: http://www.government.se/sb/d/14194/a/170566.

5 Európska Komisia: Kódex EÚ práv v on-line prostredí, Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2012. str. 2.

6 Smernica Európskeho parlamentu a Rady 2002/22/ES zo 7. marca 2009 o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (smernica o univerzálnej službe) v znení zmien a doplnení smernice 2009/136/ES, článok 1.

7 Tamtiež, článok 3.

dostupnosti k on-line službám, akými sú napríklad softvér na zväčšenie textu alebo čítač obrazovky.[8] Každý v EÚ musí mať možnosť prístupu k akýmkoľvek informáciám, možnosť šíriť akékoľvek informácie a využívať akékoľvek aplikácie a služby podľa vlastného výberu prostredníctvom sietí elektronických komunikácií. V tejto súvislosti sa dodržiavajú základné práva a slobody fyzických osôb, ktoré zaručuje Charta základných práv Európskej únie, Európsky dohovor o ochrane ľudských práv a základných slobôd a všeobecné zásady právnych predpisov EÚ.[9] V nadväznosti na spomínanú možnosť slobodného využívania aplikácií a služieb sa však naskytuje otázka porušovania autorských práv. Podľa údajov Medzinárodnej Federácie Hudobného Priemyslu, si šestnásť percent užívateľov internetu v Európe pravidelne sťahuje nelegálne šírenú hudbu, pričom 95 percent z toho, sú sťahované nelegálne. Boj proti užívateľom internetu, ktorí si nelegálne sťahujú filmy alebo hudbu však nabral po novembri 2009 v Európskej únii nový smer.

V Európe sa boj proti internetovým pirátom doposiaľ nesústreďoval priamo na žaloby vlastníkov autorských práv proti fyzickým osobám, „zneužívateľom" internetu, ale v snahe zabrániť tomuto javu, žaloby smerovali buď priamo proti serverom, ktoré ponúkali sťahovanie hudby či filmov, alebo sa vlastníci autorských práv spojili s legislatívcami a za ich pomoci presadili zákony, na základe ktorých prinútili providerov[10] internetu, aby vyhľadávali „pirátov", posielali im varovania a v prípade neuposlúchnutia a za uplatnenia zásady „trikrát a dosť" ich odpájali z internetu. Kým prvá cesta sa ukázala ako málo účinná, z dôvodu, že aj v prípade „víťazstva hudby" nad pirátstvom, keď súd nariadil uzavretie toho ktorého servera, dopyt spôsobil, že na uvoľnené miesto prišiel nový portál, druhý spôsob bol v novembri 2009 zablokovaný priamo Európskym parlamentom.

Smernica Európskeho parlamentu a Európsky Rady č. 2009/140/EC,[11] ktorá je súčasťou tzv. *telekomunikačného balíčku*, prvýkrát reguluje prístup k internetu na úrovni práva Európskej únie. Dosiaľ bola táto oblasť výlučne v oblasti národnej regulácie členských štátov, z čoho vyplývala aj rozličná právna úprava v jednotlivých členských štátoch EÚ. Nová úprava prístupu na internet zaviedla do tejto oblasti tzv. *due process clause*, a teda osoby podozrivé z porušenia zákona už nemôžu byť odpojené od internetu bez náležitého procesu (due process). Obmedzenia v prístupe užívateľov internetu môžu „byť uložené iba vtedy, ak sú opodstatnené, primerané a nevyhnutné v rámci demokratickej spoločnosti."[12] Takého opatrenia môžu byť prijaté iba „s náležitým zohľadnením zásady prezumpcie neviny a práva na súkromie. Zaručí sa predchádzajúce spravodlivé a nestranné konanie, vrátane práva na vypočutie dotknutej osoby alebo osôb, podliehajúce potrebe primeraných podmienok a procesných úprav náležite v opodstatnených naliehavých prípadoch v súlade s Európskym dohovorom o ochrane ľudských práv a základných slobôd. Zaručí sa právo na účinné a včasné súdne preskúmanie."[13]

---

8 Smernica Európskeho parlamentu a Rady 2002/22/ES zo 7. marca 2009 o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (smernica o univerzálnej službe) v znení zmien a doplnení smernice 2009/136/ES, článok 7.

9 Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica), článok 1 ods. 3a.

10 Sprostredkovateľ trvalého alebo dočasného pripojenia ku komunikačnej sieti, napr. internetu.

11 Smernica Európskeho parlamentu a Rady 2009/140/ES z 25. novembra 2009, ktorou sa menia a dopĺňajú smernice 2002/21/ES o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby, 2002/19/ES o prístupe a prepojení elektronických komunikačných sietí a príslušných zariadení a 2002/20/ES o povolení na elektronické komunikačné sieťové systémy a služby.

12 Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica), článok 1 ods. 3a.

13 Tamtiež.

Táto legislatívna úprava telekomunikačného balíčka sa rodila ťažko, jedným z dôvodov bolo, že internet ako celosvetová sieť je v súčasnosti považovaný za jeden zo základných nástrojov pri uplatňovaní základných práv občanov EÚ, akými sú právo na súkromie, na vzdelávanie, slobodu prejavu a prístup k informáciám. Prvýkrát bol pozmeňovací návrh Európskemu parlamentu predložený už v roku 2007, spornou však bola otázka týkajúca sa práve oblasti ochrany práva na prístup na internet a tým aj práva na informácie a slobodu prejavu, ktorá sa v pôvodnom legislatívnom návrhu vôbec nenachádzala. Rada EÚ dvakrát odmietla tento pozmeňovací návrh, čím spôsobila tretie, a teda posledné štádium legislatívneho procesu EÚ, známe ako zmierovacie konanie. Tento návrh bol preto po mesiacoch rokovaní v EP doplnený o ochranné záruky proti neoprávnenému obmedzeniu užívateľov v prístupe na internet v podobe požiadavky predchádzajúceho rozhodnutia súdu.

Parlament presadením tohto pozmeňujúceho návrhu dosiahol, že v prípade, že chce národný súd alebo správny orgán obmedziť prístup používateľa internetu, používateľ má právo ešte pred prijatím rozhodnutia brániť sa obvineniam za náležitého zohľadnenia zásady prezumpcie neviny, ako aj práva na účinné a včasné preskúmanie súdom. „Telekomunikačný balíček“ je od 18.decembra 2009 účinný v Európskej únii a členské štáty boli povinné ho transponovať do svojich národných legislatív do júna 2011.

3. Riešenie sporov vzniknutých v on-line prostredí

Charta základných práv Európskej únie stanovuje: „Každý, koho práva a slobody zaručené právom Únie sú porušené, má za podmienok ustanovených v tomto článku právo na účinný prostriedok nápravy pred súdom, každý má právo na to, aby jeho záležitosť bola spravodlivo, verejne a v primeranej lehote prejednaná nezávislým a nestranným súdom zriadeným zákonom a každý musí mať možnosť poradiť sa, obhajovať sa a nechať sa zastupovať. Právna pomoc sa poskytuje osobám, ktoré nemajú dostatočné prostriedky v prípade, ak je táto pomoc potrebná na zabezpečenie efektívneho prístupu k spravodlivosti.“[14] Tieto ustanovenia sa vzťahujú aj na spotrebiteľov, ktorí získavajú prístup k on-line službám a využívajú ich.

Užívateľ, ktorý má podozrenie, že jeho práva boli porušené poskytovateľom služieb alebo bol podvedený internetovým predajcom, má niekoľko možností ako môže danú situáciu riešiť:

1. kontaktovanie priamo poskytovateľa služieb resp. predajcu;
2. kontaktovanie vnútroštátneho regulačného orgánu (pre poskytovateľov internetových služieb);
3. mimosúdne riešenie sporov;
4. súdna žaloba.

3.1. Kontaktovanie priamo poskytovateľa služieb resp. predajcu

Prvým krokom riešenia sporu je možnosť obrátiť sa na poskytovateľa služieb alebo predajcu. Je potrebné oboznámiť ho, že konal v rozpore s právnymi predpismi EÚ a daného členského štátu a požiadať ho, aby problém vyriešil. Ak poskytovateľ služieb alebo predajca neposkytne súčinnosť, poškodenému nezostáva nič iné, ako podniknúť ďalšie kroky v tejto veci.

---

[14] Charta základných práv Európskej únie, článok 47.

3.2. Kontaktovanie vnútroštátneho regulačného orgánu

Ďalším krokom v prípade, že poskytovateľ služieb alebo predajca sťažnosť zamietne, je možnosť obrátenia sa na *Vnútroštátny regulačný úrad pre odvetvie elektronickej komunikácie,* ktoré zahŕňa aj internetové služby. Tento úrad môže vyriešiť spory medzi sťažovateľom a poskytovateľom internetových služieb. Vďaka osobitným postupom pre poskytovateľov internetových služieb často dokáže spravodlivo a rýchlo vyriešiť spotrebiteľské spory týkajúce sa napríklad zmluvných podmienok, kvality služieb, prístupu k sieťam a službám.

3.3. Mimosúdne riešenie sporov

Spotrebitelia majú takisto možnosť vyriešiť spor súvisiaci s on-line transakciou mimosúdnou cestu prostredníctvom subjektov poskytujúcich alternatívne riešenia sporov, keď takéto subjekty existujú. Nie všetky členské štáty EÚ však majú takéto subjekty ARS, ktoré by zastrešovali všetky druhy sporov medzi spotrebiteľmi a obchodníkmi. Európska komisia preto prijala návrh smernice o alternatívnom riešení sporov (ARS) a o riešení sporov on-line (ORS) s cieľom zabezpečiť, aby subjekty ARS boli k dispozícii v prípade akýchkoľvek sporov o zmluve medzi obchodníkmi a spotrebiteľmi, ktoré vznikajú vzhľadom na predaj tovaru alebo poskytovanie služieb na jednotnom trhu.

Výraz **alternatívne riešenie sporov** pokrýva mimosúdne postupy, ako je zmierenie, mediácia, arbitráž, rada pre sťažnosti. Na účely tohto posúdenia vplyvu sa ARS vzťahuje na riešenie sporov medzi spotrebiteľmi a obchodníkmi súvisiacich s predajom tovaru a poskytovaním služieb zo strany obchodníkov. Cieľom systémov ARS je urovnanie sporov medzi stranami zapojením príslušného subjektu (napr. zmierovacieho vyjednávača, mediátora, ombudsmana, rady pre sťažnosti atď.). Systémy ARS zamerané na riešenie sporov medzi spotrebiteľmi a obchodníkmi uplatnením online postupu sa volajú systémy **riešenia sporov online** a mohli by byť účinným nástrojom najmä pri riešení sporov súvisiacich s transakciami online.[15]

Výhodou týchto mechanizmov je zvyčajne ich rýchlejšie, lacnejšie a jednoduchšie využitie ako súdne konanie. O väčšine sporov postúpených na alternatívne riešenie sporov sa rozhodne do 90 dní, pričom veľká väčšina konaní je pre spotrebiteľov bezplatná alebo je spojená iba s nízkymi nákladmi (menej ako 50 EUR).

Opatrenia vo vzťahu k subjektom ARS by mali začať platiť v roku 2014, spustenie platformy riešenia sporov on-line a dobudovanie pokrytia ARS v súlade s ustanoveniami o ARS sa plánuje v roku 2015. Po uvedení návrhu do praxe, budú mať **spotrebitelia** možnosť vyriešiť spory s obchodníkmi týkajúce sa tovarov a služieb rýchlo, jednoducho, efektívne a mimosúdne bez ohľadu na to, či nakupujú on-line alebo tradične, doma či v zahraničí a **podnikatelia** budú mať možnosť ukončiť spory so spotrebiteľmi rýchlo, jednoducho, efektívne a mimosúdne, čím sa vyhnú vysokým dodatočným nákladom a poškodeniu svojej reputácie. Aj keď smernica o alternatívnom riešení sporov a riešení sporov on-line nie je v súčasnosti účinná, to neznamená, že spotrebitelia nemajú právo na vyriešenie svojich sporov mimosúdnou cestou. Toto právo im zaručuje *smernica o platobných službách*, ktorá obsahuje obdobné ustanovenie, v ktorom je zakotvený nárok na osobitné mimosúdne vy-

---

15 Summary of the Impact Assessment. Dostupné na internete: http://ec.europa.eu/consumers/redress_cons/adr_policy_work_en.htm.

rovnanie, ktoré majú on-line spotrebitelia k dispozícii na riešenie sporov týkajúcich sa predovšetkým platobných transakcií.[16]

Pokiaľ ide o poskytovanie elektronických komunikačných sietí a služieb, spotrebitelia musia mať prístup k transparentným, nediskriminačným, jednoduchým mimosúdnym vyrovnaniam spojeným s nízkymi nákladmi, ktoré im zabezpečujú členské štáty na vyriešenie nedoriešených sporov s poskytovateľmi služieb, ktoré sa týkajú zmluvných podmienok alebo vykonávania zmluvy.[17] V cezhraničných prípadoch sa on-line spotrebiteľom odporúča využiť mediačný postup, ktorý zostane dôverný a v rámci ktorého strany môžu požiadať, aby obsah ich dohody o urovnaní bol vyhlásený za vynútiteľný. Ak pokus o vyrovnanie sporu mediáciou zlyhá, spotrebiteľovi nič nebráni iniciovať súdne konanie z dôvodu premlčacích a prekluzívnych dôb.[18]

3.4. Súdna žaloba

Poslednou možnosťou riešenia sporu je súd. Každý má právo podať žalobu a byť žalovaní vo veciach týkajúcich sa spotrebiteľskej zmluvy na súde v mieste bydliska spotrebiteľa, v prípade, že spoločnosť je obchodne alebo pracovne činná v členskom štáte bydliska spotrebiteľa alebo tieto jej aktivity smerujú do predmetného členského štátu.[19]

V niektorých prípadoch, vrátane on-line transakcií do 2 000 EUR, majú spotrebitelia možnosť využiť európske konanie vo veciach s nízkou hodnotou sporu, ktoré je rýchlou a z finančného hľadiska výhodnou alternatívou k tradičnému súdnemu konaniu. Na začatie takéhoto konania stačí podať štandardný formulár pre konanie vo veciach s nízkou hodnotu sporu.

V konaní pred súdom sa obom stranám zaručujú práva vyplývajúce z práva na súdnu a inú právnu ochranu stanovené v Charte základných práv a slobôd Európskej únie, ako aj iných právnych aktov, ktoré zakotvujú základné ľudské práva a slobody.

Záver

Informačné a komunikačné technológie sú v súčasnosti jednými z najrýchlejšie sa rozvíjajúcich odvetví vôbec. Na druhej strane, tvorba práva je oveľa komplexnejší proces ako by sa na prvý pohľad mohlo zdať. Právo samo o sebe netvorí len konečná forma ako je napríklad zákon, či smernica. Tvoriť právo v širšom ponímaní znamená aj zásah do už vzniknutého právneho poriadku, systému práva, a do právnych noriem. A to je, hádam, jednou z najpodstatnejších príčin, prečo má právo Európskej únie v istých oblastiach regulácie medzery. Informačná spoločnosť síce neustále napreduje, no „inštitucionálny trojuholník" troch hlavných inštitúcií (Európsky parlament, Rada Európskej únie a Európska komisia) zúčastňujúcich sa legislatívneho procesu svojou činnosťou postupne reaguje na prebiehajúce zmeny týkajúce sa nielen oblastí elektronického obchodu a ochrany spotrebiteľa, kto-

---

16 Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES, článok 80 a 83.

17 Smernica Európskeho parlamentu a Rady 2002/22/ES zo 7. marca 2009 o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (smernica o univerzálnej službe) v znení zmien a doplnení smernice 2009/136/ES, článo 34.

18 Smernica Európskeho parlamentu a Rady 2008/52/ES z 21. mája 2008 o určitých aspektoch mediácie v občianskych a obchodných veciach.

19 Nariadenie Rady (ES) č. 44/2001 z 22. decembra 2000 o právomoci a o uznávaní a výkone rozsudkov v občianskych a obchodných veciach, článok 16.

ré tvoria najdôležitejšiu súčasť európskej on-line regulácie, ale aj ostatných častí „mozaiky“ spoločenského života na internete.

Soft law a iné mimoprávne regulácie a ich význam pre internet

František Lipták

Úvod

Technologický prokrok spôsobený rozšírením Internetu má za následok vznik nových situácií, s ktorými dovtedajšie právne poriadky nepočítali. Nové rozmery spoločenských vzťahov, ktoré používanie Internetu prináša prinášajú so sebou otázky, ktoré je potrebné riešiť. Otázky, ktoré sa dotýkajú práva Internetu sú prierezové, súvisia s otázkami ako sloboda prejavu a cenzúra, doménové mená, autorské právo, kyberbezpečnosť, riešenie sporov online a mnohé ďalšie.[1]

Tým, že Internet nie je geografický vymedzený, ale predstavuje nový druh priestoru, vstáva otázka, ktor by mal určiť, kým a ako bude Internet regulovaný. Preto je na mieste položiť si otázku, či by mal byť Internet upravený multilateralnou zmluvou medzi štátmi, fragmentovanou právnou úpravou založenou na právnych poriadkoch štátov alebo normách neštátnej povahy – soft law. Pochopiteľne, do úvahy prichádza aj kombinácia predchádzajúcich prístupov. Tento pohľad závisí najmä od toho, ako sa dívame na jurisdikciu kyberpriestoru, mala by byť samostatná alebo podliehať moci suverénov? Jedná sa o úplne nové prostredie, ktoré by malo byť regulované silovými prostriedkami štátnej moci alebo je efektívnejšia viac flexibilná soft law úprava? Aké úskalia nám prináša hard law a aké soft law a naopak aké benefity prinášajú uvedené dva prístupy? Je lepšie sa spoliehať na reguláciu alebo umožniť samoreguláciu? V ktorých prípadoch je samoregulácia efektívnejšia? A v ktorých regulácia?

V našom príspevku sa budeme zaoberať prístupom soft law pre reguláciu Internetu, právnou povahou fungovaním príkladov súčasnej právnej regulácie soft law, analýzou výhod a nevýhod soft law regulácie a ďalšími aspektmi tohto fenoménu. Závere zhrnieme demokratickosť uvádzaného prístupu a tiež rozlíšenie oblastí, pre soft a pre hard law založených na predchádzajúcej analýze. Samotnú otázku právnej povahy komplikuje aj fakt klasickej reflexie právneho princípu teritoriality[2] právnymi poriadkami na rozdiel od Internetu pôsobiaceho prakticky bez geografických obmedzení. Otázka budúcnosti regulácie Internetu je tak živou otázkou.[3]

Geografická delokalizácia kyberpriestoru sa vyznačuje tým, že vzhľadom na technologicky možné prekonanie vzdialenosti, dochádza k stretu rôznych účastníkov, kultúr, záujmov, vzniku cezhraničných transakcií, šíreniu myšlienok a konfrontácii názorov. Takto môžu mať politiky alebo konania iných účastníkov dopad na dianie v krajinách, kde nevznikli alebo kde tieto konania nie sú povolené, majú iný status právnej ochrany alebo nie sú regulované vôbec, poprípade sa vyznačujú iným faktickým dopadom. Existuje teda množstvo

---

1 SOLUM, LAWRENCE B.: Models of Internet Governance (September 3, 2008). Illinois Public Law Research Paper No. 07-25; U Illinois Law & Economics Research Paper No. LE08-027. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825.

2 CARREIRA, M.-A.: Soft Law in Cyberspace: Exploring the Role of Codes of Conduct as Legal Instruments of Web Regulation, dostupné online: http://effectius.com/yahoo_site_admin/assets/docs/Soft_law_in_cyberspace_by_Marc_Antoine_Carreira_da_Cruz.20774859.pdf.

3 WEISER, P.: The Future of Internet Regulation (February 16, 2009). University of Colorado Law Legal Studies Research Paper No. 09-02. Available at SSRN: http://ssrn.com/abstract=1344757 or http://dx.doi.org/10.2139/ssrn.134475.

problémov, pri ktorých bude potrebné aplikovať niektoré zo známych druhov regulácie alebo ich neregulovať vôbec alebo v rôznom rozsahu.

Emergentná povaha soft law, spoliehajúca sa na neštátne prostriedky tvorby právnych pravidiel a donútenia poprípade reputačných mechanizmov, je analogická princípom fungovania. Lex mercatoria ako stredoveké právo kupcov sa spoliehala na autonómnu tvorbu práva, riešenie sporov založené na kupeckých súdoch, kde si strany sporu dobrovoľne vyberali spomedzi seba sudcov, ktorí požívali dôveru strán a rozhodovlai podľa obyčají obchodníckej komunity, rozhodovali podľa zásad dobrého a spravodlivého (*ex aequo et bono*). Tento systém fungoval na báze právnych obyčají charakteristických pre medzinárodnú komunitu kupcov a ich vlastných pravidiel a zvyklostí. Ako ukážeme ďalej, viacero z týchto aspektov je charakteristických aj pre právnu reguláciu Internetu. Lex informatica alebo lex mercatoria ako pravidlá neštátnej povahy majú v uvádzaných otázkach esenciálne postavenie, a len kvôli prvotnej percepcii povahy nižšieho stupňa právnej záväznosti by nemali byť podceňované, práve naopak, zastávajú významené miesto v rámci súčasnej úpravy pravidiel fungovania Internetu.

1. Charakteristika soft law

Soft law je možné voľnou definíciou vymedziť ako súbor pravidiel, ktoré sú pôvodom svojho vzniku pravidlami neštátnej povahy. Prvým definičným znakom je teda tvorba týchto noriem subjektmi, ktoré sú odlišné od štátu. Druhým definičným znakom je predovšetkým ich nižší stupeň právnej záväznosti.

Aj keď je otázne, či táto nižší stupeň právnej záväznosti má nejaké opodstatnenie ak je často krát efektívna vykonateľnosť porovnateľná (uživateľov porušujúcich podmienky používania je možné odpojiť zo servra). Je treba povedať, že nižší stupeň právnej záväznosti vyplýva najmä z porovnania s tým, čo rozumieme pod pojmom „hard law“. V tomto kontexte treba treba chápať rozlíšenie na soft law a hard law, nakoľko donucovacia autorita je spätá so suverénom – štátom. Tiež je otázne, ktoré porušenia pravidiel správania onlin sú detekovateľné.

Soft law nástroje fungujú na báze „*opt in*“, čo znamená, že subjekty si zvolia súbor noriem, ktoré sa budú na nich aplikovať. Soft law nie je iba teoretickým konceptom, ale aj aj prístpom, ktorý je známy svojim empirickým fungovaním a praktickou aplikáciou. Jedná sa o kváziprávne prostriedky alebo nástroje. Existuje otázka, či soft law je vôbec law, teda či sa jedná o právo vo vlastnom zmysle slova. Soft law, či už vo forme guidelines, standards of practice, best practice, codes of conduct, modelové zákony a súborov v rozdmedzí iných pomenovaní je používaná aj v iných prostrediach, v rámci regulácie spoločenských vzťahov v EU medzinárodných organizáciách a tiež súkromných entitách. Keďže právne poriadky sa prispôsobujú novým situáciám s oneskorením, soft law normy spontánne vznikali na dobrovoľnej báze bez ingenerecie štátu, aby sa pravidlami upravilo fungovanie otázok, ktoré bolo potrebné riešiť. Väčšinou sa jedná o súbory pravidiel, ktoré vypracovali rôzne technické a inžinierske organizácie, s potrebou riešiť vzniknuté situácie súvisiace s používaním technológií.[4]

ICANN, Internet Corporation of Assigned Names and Numbers, ktorá registruje domény a je fundamentálnou súčasťou internetovej infraštruktúry, má svoje vlastné súbory soft law pravidiel, a čo sa týka jej právnej formy je neziskovou organizáciou (non-profit). Jedná sa o súkromnú entitu, ktorá sa vyznačovala samoreguláciou. To isté platí aj pre Internet Engi-

---

4 POWER, A. and TOBIN, O.: Soft Law for the Internet, Lessons from International Law", 2011 8:1 Scripted page, online: http://www.law.ed.ac.uk/ahrc/script-ed/vol8-1/power.asp.

neering Task Force a mnohé ďalšie entity. Podobné organizácie sa v minulosti sústredili najmä na harmonizáciu technických štandardov, aby sa prekonávali technické bariery.

Okrem hmotnoprávnych oprávnení a povinností, soft law upravuje aj procesné ustanovenia, jedná sa o online dispute resolution methods. V podstate ide o alternatívne metódy riešenia sporov online. Riešenie doménových sporov, online arbitráž, online mediácia a online konciliácia, podávanie sťažností elektronicky v rámci poskytovanie online služieb, výkonu transakcií online atď. Tieto procesné mechanizmy majú za následok konštitutovanie procesnej stránky práva Internetu. Ďalším definičným znakom soft law je decentralizovaná tvorba soft law. Neexistuje centralizovaná autorita, ktorá by určila pravidlá, ktoré budú platiť pre celý Internet vo všetkých ohľadoch regulácie vo všetkých spoločenských vzťahoch, práve naopak, viac rozšírená je súkromná tvorba práva, ktorá je decentralizovaná. Ak si zoberieme napríklad Paypal, podmienky používania Paypal-u vrátane riešenia sporov sú založené na báze pravidiel vypracovaných súkromnou spoločnosťou, jedná sa teda o soft law.

Môžeme sa pozrieť aj na UDRP, politiku riešenia doménových sporov, ktoré sú tiež soft law. ICANN, ktorá registruje a priďeľuje IP adresy funguje na princípoch soft law úpravy, ako sme už uviedli, jedná sa o neziskovú organizáciu založenú na účely charitatívne a verejné podľa kalifornského práva. Bitcoin,[5] globálna elektronická mena fungujúca na privátnej báze je upravená výlučne podľa vlastných soft law noriem a na týchto princípoch funguje. Existujú aj ďalšie prípady soft law pravidiel, reputačný mechanizmus predajcov na eBay, kde sú hodnotení hviezdičkami podľa svojej kvality, a tak sa dosahuje ochrana zákazníkov na základe vyžiadania hodnotenia podľa ich spokojnosti. V zásade nie je nutné používať formálne právne postupy a aplikovať legislatívu danej jurisdikcie, pretože spoločná platforma umožňuje prostredníctvom svojich pravidiel odmeňovať poctivých predajcov na základe ich hodnotení, a poškodenie reputácie má ďalekosiahlejší vplyv ako zarobenie na nespokojnom zákazníkovi. Toto je výhodné najmä pri transakciách malej hodnoty, čo pôsobí ako motivačný mechanizmus na predajcov dodržiavať etický štandard, sledovať spokojnosť zákazníka a zabezpečovať dôveru v rámci spomenutej platformy.

K ďalšiemu znaku soft law patrí aj emergentnosť systému pravidiel. Pravidlá vznikajú spontánne, prirodzene, keďže subjekty spoločenských vzťahov túto úpravu vzťahvo požadujú pre svoje fungovanie a vymedzenie pravidiel, ktoré by transparentne určili ich povinnosti a práva, a tak vymedzili spôsob a princípy svojho fungovania, čím by eliminovali riziká plynúce z právnej neistoty, ktorá je charakteristická pre stav bez úpravy. Súkromné subjekty tak autonómne vytvárajú vlastné súbory pravidiel podľa potreby vzhľado mna vzniknuté situácie. Táto spontánna tvorba pravidiel je podobná hayekovskému modelu spontánneho poriadku, kde pravidlá vznikajú spontánne, prirodzene a na báze samoregulácie vznikajú pravidlá v spoločnosti a upravujú jej fungovanie.

Nastolenie soft law pravidiel znamená viacero vecí,[6] ide najmä o rešpekt pred hard law, snahy o nastolenie spolupráce pri štátoch, ktoré nemajú ochotu spolupracovať, prekonanie súvisiacej neistoty a ďalšie.

---

5 Living on Bitcoin for a Week: Birthday Bitcoiins, Forbes, 5 May 2013, dostupné online: http://www.forbes.com/sites/kashmirhill/2013/05/05/living-on-bitcoin-for-a-week-birthday-bittycoins/?utm_campaign=forbesfbsf&utm_source=facebook&utm_medium=social.

6 Segura-Serrano, A.: Internet Regulation: A Hard-Law Proposal, Jean Monnet Working Paper 10/06, 2006, dostupné online: http://centers.law.nyu.edu/jeanmonnet/papers/06/061001.pdf.

2. Soft law a hard law - porovnanie výhod a nevýhod

Učenie sa a evolúcia noriem

Medzi výhody soft law patrí – učenie sa[7] – soft law pravidlá umožňujú začleniť praktické riešenia vzniknutých situácií do svojich štandarov praktík, best practice, pravidiel používania, guidelinov a iných kódexov, pričom pravidlá su vzhľadom na flexibilitiu tohto prístupu ľahšie meniteľné a nevyžaduje sa komplikovaný a namáhavý legislatívny proces charakteristický pre striktné písané „hard law". Vzhľadom na nové vzniknuté situácie je možné adaptovať pravidlá poprípade ich meniť. Aj keď soft law pravidlá existujú samostatne, stále je otvorený priestor na reguláciu klasickými prostriedkami hard law, ak by sa tieto pravidlá neosvedčili alebo by bola z rôznych dôvodov táto úprava potrebná. Učenie, skúšanie a experimentovanie s rôznymi pravidlami umožňuje flexibilne sa adaptovať novým situáciám a vzhľadom na testovanie rôznych súborov pravidiel je tak možné vybrať tie najlepšie. Ich zmenu je možné uskutočniť rýchlo. Jedná sa teda o *learning by doing*. Skúšanie a testovanie nových pravidiel urýchľuje učenie a otvára cestu k lepším pravidlám s možnosťou rýchlych zmien a flexibilnej reakcie na vstávajúce a nepredvídané problémy.

Rozsah vzťahov, ktorý je potrebné upraviť a rozsah problémov štát vzhľadom na svoju obmedzenú právotvornú kapacitu nemôže poňať a ani obsiahnuť, a tiež ani často meniť. Na to sú lepšie súkromné organizácie, ktoré sa prispôsobujú rýchejšie ako právne prostriedky štátov. Ďalším dôvodom, prečo je lepšie regulovať prostredníctvom soft law je to, že soft law je rýchlejšie a jednoduchšie upraví obrovský rozsah vzťahova problémov na báze špecializácie organizácií, keďže tieto sa problémami zaoberajú, vidia riešenia a úskalia a sú rýchlejšie. Regulácia legislatívou nie je pre tieto prípady vhodná a ani očakávateľná vzhľadom na rapídny technologický rozvoj, je soft law lepším nástrojom regulácie.[8]

Špecializácia je typickým atribútom pre arbitrážne súdnictvo. Analógia z lex mercatoria, kde spory rozhodovali sudcovia – kupci, ktorí rozumeli obchodným zvyklostiam, je príznačná aj pre súčasnú samoreguláciu Internetu. Špecializácia má svoje opodstatnenie pretože sa jedná o konkrétnu oblasť, ktorej fungovanie ovplyvňujú odborníci, o ktorých sme už hovorili. To sa týka aj regulácie práv a povinností a aj procesu riešenia sporov, kde nemusí ísť vždy nutne o spory čisto právnej povahy, aj keď sa práva a povinnosti s týmito spormi spájajú.

Je treba povedať, že soft law môže slúžiť aj v zmysle opinio iuris, pri interpretácii zmlúv v medzinárodnom práve, poprípade aj ako inšpirácia pre právne úpravy hard law. Soft law ponúka vodítko pre štáty, aby reflektovali priania občanov, neziskové organizácie a aj ďalších stakeholderov, ktorí si vytvorili vlastné pravidlá pri formulácii právnych úprav. Vzhľadom na širšiu účasť súkromných entít a rôznych stakeholderov, je možné hovoriť o legitimizačnej funkcii, najmä v prípade ak sa sami aktéri internetových vzťahov podieľajú na tvorbe noriem. Toto prostredie teda môže slúžiť na zapojenie viacerých subjektov do diskusie o podobe pravidiel.

V každom prípade je lepšie mať prvotne úpravu soft law, ktorá sa môže meniť. Ak by táto právna úprava zlyhala, stále existuje priestor na reguláciu zo strany štátov.[9] Soft law je

---

7 POWER, A. and TOBIN, O.: Soft Law for the Internet, Lessons from International Law, SCRIPTed, Volume 8, Issue 1, April 2011, dostupné online: http://www.law.ed.ac.uk/ahrc/script-ed/vol8-1/power.asp.

8 Ibid.

9 POWER, A. and TOBIN, O.: Soft Law for the Internet, Lessons from International Law, SCRIPTed, Volume 8, Issue 1, April 2011, dostupné online: http://www.law.ed.ac.uk/ahrc/script-ed/vol8-1/power.asp.

teda dobrý mechanizmus, ktorý sa dokáže sám udržiavať a regulovať, a necháva priestor otvorený pre reguláciu v ďalšom čase.

Je to dôležité najmä v tých prípadoch, keď štáty nechcú spolupracovať pri prijímaní hard law úprav. Prijatie globálnej medzinárodnej zmluvy o regulácii Internetu sa javí nereálne, vzhľadom na širokú diverzitu účastníkov tohto procesu, s rôznymi a často krát protichodnými záujmami. Je treba povedať, že soft law dokáže prekonať právnu neistotu spojenú s neexistujúcou úpravou, poskytnúť priestor a zmenu a vyjednávanie pri riešení problémov, vzhľadom na nižší stupeň právnej záväznosti štáty nebudú mať čo ľutovať, ak sa do tohto procesu tvorby pravidiel zapoja, naproti situácii ak by sme hovorili o prijatí medzinárodnej zmluvy regulujúcej Internet, pretože táto môže mať dopad na rozloženie práv a povinností a záujmy štátov bez jednoduchej možnosti opt out alebo rýchlej zmeny v prípade nevyhovujúcej úpravy. Je to tvrdé právo, ktoré platí. Tiež je potrebné povedať, že predčasné riešenie problémov spätých s Internetom môže mať ďalekosiahly dopad na jeho ďalšie fungovanie a môžu nastať situácie, ktoré sme nepredvídali. Zvyšuje to riziko toho, že to ovplvní štáty s rôznymi záujami tak, že im táto úprava môže prestať v budúcnosti vyhovovať. Soft law tak dokáže svojou evolučnou charakteristikou rýchlo, neformálne a pružne reagovať na meniace sa potreby a otvára priestor pre vyjednávaneei a zapojenie rôznych stakeholderov, čo by malo robiť proces demokratickejším, vzhľadom na rešpektovanie a zohľadňovanie rôznych názorov. Je treba povedať, že s demokratickosťou tvorby rôznych praivdiel to nie je vždy úplne jednoduché, vzhľadom na niektoré problémy známe z histórie. Politika budujúca na úprave soft law sa zakladá na „*adaptive*" atribúte uvádzanej úpravy.[10]

Vzhľadom na uvedené argumenty, tento nástroj je vhodné najmä pre situácie, keď štáty nechcú spolupracovať.[11] Tento prístup môže tak uľahčiť spoluprácu na menej formálnej, menej záväznej a viac flexibilnej báze.

Ak chceme hovoriť o nevýhodach soft law úpravy alebo o sitácii, kedy je lepšie použiť hard law, jedná sa o nasledovné situácie:[12] 1. Ak ide o situáciu, keď benefity zo spolupráce sú vysoké, a náklady z porušenia sú tiež vysoké. 2. Ak je ťažké detekovať „non compliance", teda nedodržanie alebo nezosúladenie sa s právnymi pravidlami. Ide teda o klasický prípad *free ridingu*.

3. Keď sa štáty snažia získať dôveru v medzinárodnej komunite 4. keď majú domáce agentúry s malou kontrolou od exekutívy právo uzatvárať zmluvy. Tiež sme toho názoru, že aj keď konkurencia a učenie sa prostredníctvom rôznych súborov pravidiel a ich skúšania prináša svoje benefity, štadnardizácia a jednotná úprava eliminuje právne riziká a neznalosť lokálnych alebo špecifických noriem soft law u každého subjektu (napríklad rôzne podmienky u každého prevádzkovateľa servra). Na druhej strane, výhody zo štandardizácie nezohľadnia vždy technologický pokrok, ak máme na mysli ich uniformitu. Na druhej strane, aj soft law dokáže priniesť štandardizáciu, vzhľadom na inžinierske organizácie, ktoré vytvárajú pravidlá ako ICANN alebo Internet Engineering Task Force, ktoré plati v podstate pre celý Internet. Ide o to, či ide o subjekty, ktoré tvoria vlastné pravidlá, a či ide o viacero subjektov, ktoré tvoria pravidlá regulujúce tie isté vzťahy alebo o pravidlá, ktoré regulujú celú Internetovú štruktúru alebo architektúru a fundamentálne aspekty jeho fungovania. Či ide o centralizovanú tvorbu soft law alebo o decentralizovanú tvorbu soft law. Aj keď je decentralizovaná tvorba pravidiel frekventovanejšia a charakteristická, existujú aj soft law normy s extenzívnejším dopadom.

---

10 Ibid.
11 Ibid.
12 Ibid.

Demokratickosť súčasného mechanizmu správy Internetu bola vo viacerých prípadoch spochybňovaná. Existovalo viacero kontroverzných rozhodnutí o správe ICANN.[13]

Tiež existuje viacero kontroverzných rozhodnutí UDRP procesu. V tomto prípade ide najmä o favorizáciu držiteľov ochranných známok, ktorým podľa viacerých skutočností UDRP ako politika nadržiava[14]. Existujú teda kritické názory týkajúce sa nezávislosti a nestrannosti rozhodovania týchto sporov.

Záver

Ak máme na mysli otázky, ktoré majú tendenciu byť upravené medzinárodným právom verejným alebo právnou úpravou štátov môžeme povedať, že medzi tieto oblasti patria tie, ktoré sú charakteristické verejným záujmom alebo späté s oblasťami trestného práva, otázky týkajúce sa národnej bezpečnosti atď, je vhodné regulovať prostriedkami hard law. Niektoré je vhodnejšie zahrnúť pod doménu hard law úpravy. Soft law umožňuje demokraticky zapojiť viac stakeholderov, na druhej strane, neexistuje dokonalé fungovanie spoločenských vzťahov a ani v tomto prípade soft law nie je *panacea*. V budúcnosti môžeme očakávať pretrvávanie kombinácie soft law a hard law úpravy fungovania Internetu.

---

13 ORAM, A.: ICANN without restraints: the difficulties of coordinating stakeholders, Oct. 2, 2009, dostupné online:
http://radar.oreilly.com/2009/10/icann-without-restraints-the-d.html;
ICANN at the center of a controversial challenge, again, 20.06.2012, dostupné online: http://www.hightechnewstoday.com/jun-2011-high-tech-news-archives/102-jun-20-2011-high-tech-news.shtml;
ICANN't Believe What They're Doing, 17.6.1999, dostupné online: http://cyber.law.harvard.edu/pil-99/icannt.txt;
E.U., U.S. call for ICANN Internet governance reforms, Computerworld, 13.05.2013, dostupné online:
http://www.computerworld.com/s/article/9216687/E.U._U.S._call_for_ICANN_Internet_governance_reforms;

14 KELLEY, P.: Emerging Patterns in Arbitration Under the Uniform Domain-Name Dispute-Resolution Policy, dostupné online:
http://www.law.berkeley.edu/files/bclt_AnnualReview_Emerging_Final.pdf.

Ochrana diplomatickej komunikácie a internet

Helena Hlaváčková

Úvod

V medzinárodnom spoločenstve štáty vykonávajú funkcie prostredníctvom svojich orgánov, ktoré sa tradične členia na zákonodarné, výkonné a súdne.[1] Okrem svojich vnútroštátnych úloh plnia štátne orgány aj medzinárodné záväzky, ktoré štátom vyplývajú z medzinárodného práva a platných medzinárodných zmlúv, ktorých sú zmluvnými stranami. Rozvoj zahraničných vzťahov zabezpečujú štátne orgány v rôznej miere. Podľa miesta výkonu sa štátne orgány štátu členia na vnútroštátne orgány a vonkajšie (zahraničné orgány). Už iba z daných názvov orgánov je zrejmé, že vnútroštátne orgány pôsobia v rámci územia štátu a na druhej strane vonkajšie orgány plnia svoje funkcie na pôde iného štátu alebo medzinárodnej organizácie. Vnútroštátne orgány štátu takisto môžu zastupovať štát pri uskutočňovaní zahraničnej politiky, vtedy hovoríme o špecializovaných vnútroštátnych orgánoch, ktorými sú ministerstvá zahraničných vecí, na čele stojí minister zahraničných vecí. Štátne úrady v oblasti zahraničnej politiky možno rozdeliť do dvoch skupín, na zastupiteľské úrady, ktoré zastupujú vysielajúci štát v prijímajúcej krajine a na strane druhej štátne úrady, ktoré zastupujú štát v rámci vymedzeného konzulárneho obvodu, kde patria konzulárne úrady alebo v rámci medzinárodných organizácií, kde zaraďujeme stále misie a delegácie pri medzinárodných organizáciách (OSN, Rada Európy, NATO, EÚ, OBSE). So súčasným rozvojom a pokrokom vo svete sa tradičné inštitúty prispôsobujú novým formám výkonu ich činnosti, s čím sa spájajú výhody ako aj nevýhody pokroku, ktoré majú priaznivý alebo negatívny vplyv v oblasti udržiavania medzinárodných vzťahov.

1. Diplomacia,diplomatické styky a diplomatická komunikácia

So vznikom každého štátu je spätý vznik jeho práv a povinností v medzinárodnom spoločenstve. Jedným z nich je právo poverovať a teda vysielať a prijímať diplomatických zástupcov (*ius legationis*),ktoré štát nadobúda svojím vznikom a predstavuje tradičný prejav jeho suverenity.[2] V dôsledku toho, že nejde o oprávnenie jednostranného charakteru, prax si vyžaduje realizáciu tohto vzťahu na základe vzájomnej dohody štátov o vyslaní a prijatí diplomatického zástupcu podľa článku 2 VCDR.[3] Pod pojmom diplomacia rozumieme metódu uskutočňovania zahraničnej politiky štátov, ktorá sa usiluje dosiahnuť zamýšľané ciele vyjednávaním medzi štátmi. Daný inštitút zohráva významnú úlohu v procese tvorby medzinárodného zmluvného a súčasne aj obyčajového práva. Proces tvorby medzinárodného zmluvného práva sa uskutočňuje prevažne vždy prostredníctvom inštitútu diplomatických rokovaní. V súčasnom ponímaní sa diplomaciou chápe činnosť diplomatov upravujúca medzinárodné pomery a takisto prípadné riešenie medzinárodných konfliktov. Komplexne činnosť diplomatických misií a teda diplomatických zástupcov upravuje článok 3 VDCR.

Medzinárodné právo ako aj vnútroštátne právo jednotlivých krajín upravujú spôsoby a formy diplomatických stykov ako aj spôsoby styku diplomatických zástupcov s orgánmi

---

1 PALUŠ, I. - SOMOROVÁ, Ľ.: Štátne právo Slovenskej republiky. Košice, UPJŠ 2002, s. 204 a nasl.

2 KLUČKA, J.: Medzinárodné právo verejné.Košice, Iura edition 2011, s. 362.

3 Viedenský dohovor o diplomatických stykoch, uverejnený pod číslom, 157/1964 Zb., článok 2: *Nadviazanie diplomatických stykov medzi štátmi a zriadenie stálych diplomatických misií sa uskutočňuje vzájomnou dohodou*.

štátu,v ktorej plnia svoju misiu a takisto aj formy, spôsoby a pravidlá stykov spojenia s vysielajúcim štátom. Je samozrejmé, že diplomatické styky sa riadia určitými pravidlami, ktorých vývoj bol podmienený vývojom spoločnosti a techniky. Samotné diplomatické styky sa uskutočňujú v dvojakej forme a teda konkrétne ústnou formou alebo písomnou formou, ktorá sa nazýva diplomatická korešpondencia.

1.1. Status quo a internetová revolúcia

S vývojom spoločnosti je úzko spätý aj technologický vývoj. Najstaršie diplomatické misie sa vyznačovali zdĺhavými prípravami na rokovania, spájané nielen s časovou ale aj finančnou náročnosťou. Je potrebné si uvedomiť, že školenia diplomatických zástupcov ako aj vymieňanie si diplomatickej korešpondencie boli na dnešné pomery takisto zdĺhavé. Technický vývoj v súčasnosti umožňuje rýchlejší a efektívnejší spôsob komunikácie medzi štátmi, čo má nemalý vplyv na rýchlejšie a často aj efektívnejšie riešenie problémov medzinárodnej politiky. Rozmáhajúcim trendom je využívanie moderných technológii komunikácie a to nielen telefonicky, no čoraz častejšie faxom a emailom. Ďalším významným inštitútom sú takzvané on-line školenia diplomatických zástupcov. V súčasnej dobe však inovácie zápasia s mnohými problémami a obmedzenia. Tu vzniká otázka, do akej miery sa má diplomacia otvárať a prijímať nové pozmeňujúce formy komunikácie. Netreba zabúdať, že diplomacia je veľmi tradičná, hierarchická a uzavretá profesia. Jej kultúra je postavená na snahe vyhnúť sa chybám a byť opatrná čo sa týka zmien. V mnohých prípadoch je kľúčom k úspechu inovačného projektu riešenie týchto aspektov diplomatickej profesionálnej kultúry.[4] Na druhej strane inovácie sú podstatné pre rozvoj modernej diplomacie, a je teda nevyhnutné aby moderný diplomat bol schopný sa rýchlo a efektívne prispôsobiť sa meniacemu sa medzinárodnému prostrediu.

S rozmáhaním internetu je spojené vytváranie rôznych sociálnych sietí, pri ktorých je na mieste položiť si otázku, či vytvorenie si účtu na danej sociálnej sieti je v súlade s jeho oprávneniami a kompetenciami. Neexistuje žiaden zákaz alebo obmedzenie, ktoré by sa týkalo vytvorenia účtu na sociálnej sieti príslušníkmi zastupiteľských úradov, takisto ako neexistuje žiadne obmedzenie, ktoré informácie by nemali zverejňovať. Diplomatický post je však veľaváženým a profesionálnym postom a preto, by si mali dávať pozor, čo na danej sociálnej sieti zverejňujú. V súčasnej dobe je trendom aj u diplomatov ako aj u iných vedúcich funkcionárov zakladať si funpage-e ako aj účty na sociálnych sieťach, z dôvodov spopularizovania sa ako aj na podporu záujmov ich krajiny, či ako súčasť verejnej diplomacie. Sociálne siete ako napríklad Twitter, umožňujú poskytovať diplomatom a iným zástupcom štátov verejné vyhlásenia, prípadne im uľahčujú zverejňovať odpovede na otázky týmto spôsobom namiesto verejných vyhlásení do médií. Týmto vyhláseniam do médií totižto predchádzajú plánovania a realizovania rôznych tlačových konferencií. Diplomati, konzuli ako aj ostatní členovia zastupiteľských úradov sú však takisto ľudia a teda majú záujem sa podeliť o svoje názory a myšlienky, postoje. Vzhľadom k ich funkcii by nemali zabúdať nato, že niektoré ich stanoviská by zverejňované byť nemali a to nielen z politických a etických dôvodov.

1.2. E-diplomacia verzus tradičná diplomacia, verejná diplomacia

Rozvoj spoločnosti, prostriedkov masovej komunikácie, globalizácia a informačné technológie sa začali prejavovať pri vytváraní zahraničnej politiky ako aj na jej prijímaní širšou

---

4 Innovation in Diplomacy. (Conference, 19th November 2012), Diplo, Dostupné na: http://www.diplomacy.edu/conferences/innovation.

verejnosťou. Hlavnými aktérmi medzinárodných vzťahov ostávajú štáty, reprezentované svojimi orgánmi, treba si všimnúť tendenciu vstupovania ďalších subjektov, ktoré napriek tomu, že nemajú štátnu povahu majú veľký vplyv v rámci medzinárodných vzťahov. Táto infiltrácia tretích sektorov má vplyv na charakter diplomacie. Z tohto dôvodu, už nie je možné diplomaciu redukovať iba na činnosť štátnych orgánov a na vzájomné prepojenia výlučne medzi vládnymi predstaviteľmi. Nutná potreba predefinovať klasický prístup k diplomacii vyplýva zo zmien, ktoré pre vnímanie a interpretáciu rôznych udalostí vo svete znamená čím ďalej tým väčšiu nadväznosť s politickou scénou na domácom území. Vplyv daných aktérov môže byť nielen kritický ale v prevažujúcej miere pozitívny až žiadúci. Mimovládne organizácie a média často omnoho efektívnejšie upriamujú pozornosť na problémy, na ktoré by vlády jednotlivých krajín neprihliadali, prípadne im dávali malý dôraz.

Termínom „verejná diplomacia" sa vo všeobecnosti rozumie komunikácia vlády s verejnosťou v zahraničí a teda *„verejná diplomacia označuje vládou sponzorované relácie určené pre informovanie alebo ovplyvňovanie verejnej mienky v iných krajinách, jej hlavnými nástrojmi sú publikácie, videosekvencie, kultúrne výmeny, rozhlas a televízia."*[5] Verejná diplomacia však svojou povahou nenahrádza postavenie tradičnej diplomacie. Ako som už spomínala, pre Verejnú diplomaciu je charakteristická komunikácia vytvorenými zastupiteľskými úradmi zriadených v krajine so zahraničnou verejnosťou.

Tradičná diplomacia sa snaží ovplyvňovať a presviedčať zahraničných vládnych zástupcov, verejná diplomacia má celkom odlišné ciele, a z tohto dôvodu používa aj rozdielne prostriedky a zameriava sa na inú cieľovú skupinu. Na druhej strane tradičná diplomacia stále zosobňuje komunikáciu medzi vládami jednotlivých štátov, a to už vo forme bilaterálnej diplomacie alebo diplomacie multilaterálnej. Ciele Verejnej Diplomacie je možné vyjadriť v dvoch oblastiach. Prvou oblasťou a teda cieľom je zviditeľnenie krajiny v medzinárodnom spoločenstve, prípadne cieľových krajinách s cieľom dosiahnuť štatút rešpektovaného a vplyvného aktéra na medzinárodnej scéne. Druhou oblasťou je pritiahnutie pozornosti a získanie si sympatií zahraničnej verejnosti s cieľom dosiahnuť, aby zahraničné vlády nemohli ignorovať záujmy alebo postoje krajiny.[6]

S rozvojom počítačovej techniky sa objavilo v diplomacii nové odvetvie diplomacie nazývané *E-diplomacy, digital diplomacy, online diplomacy* alebo *cyber diplomacy*. Presná a legálna definícia neexistuje, no z jej osobitých znakov môžeme usúdiť, že ide o novú formu diplomacie, ktorá reaguje na rozvoj internetovej spoločnosti a komunikácie. Čo sa týka jej odlíšenia od tradičnej diplomacie môžeme rozoznávať 3 hlavné rozdiely. Prvým je to, že e-diplomacia poskytuje viacej informácií ako tradičná diplomacia, stačí vedieť kde hľadať. Druhým rozdielom je to, že na rozdiel od tradičnej diplomacie poskytuje väčšiu interakciu s použitím digitálnych komunikačných prostriedkov, ktoré umožňujú efektívnejšiu komunikáciu pri väčšom počte zaangažovaných subjektov a teda mení spôsob, akým sa stýkať a komunikovať s jednotlivcom i organizáciami. Tretím hlavným rozdielom je to, že zabezpečuje väčšiu transparentnosť a to v dôsledku už spomínanej väčšej miery informovanosti, interakcie, čoho výsledkom je, že mnohé verejné inštitúcie sú teraz omnoho otvorenejšie a ochotnejšie zverejňovať informácie občanom.[7] Prínosom e-diplomacie je aj zmena diplomatickej aplikačnej praxe, keďže umožnila a uľahčila komunikáciu medzi jednotlivými

---

5 Pozri: http://publicdiplomacy.org/pages/index.php?page=about-public-diplomacy.

6 SLÁVIKOVÁ, E., BILČÍK, V., DULEBA, A.: Strednodobá koncepcia rozvoja verejnej diplomacie v podmienkach Ministerstva zahraničných vecí SR, Analýzy. Bratislava, Výskumné centrum Slovenskej spoločnosti pre zahraničnú politiku 2009, s. 13.

7 Definition of digital diplomacy, EU Digital Diplomacy, 21 August 2011, dostupné online: http://www.digitaldiplomacy.eu/a-definition-of-digital-diplomacy/.

štátmi. Ďalším prínosom je to, že je menej nákladná ako aj na čas tak aj na financie. S rastúcim fenoménom e-diplomacie sa dokonca uvažuje o zriadení virtuálneho ministerstva, ktoré by ju malo na starosť.

1.3. Dopad informačnej revolúcie na diplomatické styky

Vznik internetu a šírenie informácií spôsobilo revolúciu aj v diplomatických a vojenských záležitostiach. Nespornou výhodou globálnej komunikácie prostredníctvom internetu je to, že pomáha a uľahčuje získavanie informácií vládam krajín vo väčšom množstve a pomáha im pri analýze a pri zaujatí stanovísk. Keďže informovanosť je výsledkom získavania informácií z databáz a archívov, tak môže získanie týchto informácii podliehať aj elektronickej špionáži. Diplomatická pošta je šifrovaná a posielaná cez osobitný satelit, no napriek tomu je podstatne ľahšie sa dostať k diplomatickým depešiam z mailových adries, diskiet, CD nosičov, externých diskov ako keby boli ručne spísané a uložené v sejfoch.
Príkladom na danú situáciu je aj kauza „Wikileaks", ktorej podstatou bolo zverejnenie tajných diplomatických depeší, ktoré boli v rámci modernej technológie uložené v počítači a nie v osobitnom sejfe. Podstatou kauzy bola penetrácia do šifrového systému, odkiaľ boli tajné diplomatické informácie skopírované a následne predané hlavnému predstaviteľovi internetovej komunity wikileaks Julianovi Assagnovi. Pri danej kauze vyvstáva otázka, či Assagne porušil nedotknuteľnosť diplomatickej komunikácie alebo nie. Viedenský dohovor o diplomatických stykoch z roku 1961, v článku 24 ustanovuje: *„Archívy a písomnosti misie sú nedotknuteľné kedykoľvek a kdekoľvek sa nachádzajú*."[8] Konvencia však nekonkretizuje o aké archívy a o aký typ písomnosti má ísť. V tomto prípade treba analogicky vykladať daný článok a predpokladať, že sa jedná aj o iné moderné média. Článok 10 Európskeho Dohovoru o ľudských právach pojednáva o slobode prejavu. Konkrétne článok 10 hovorí v odseku 1: *„Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice.*" Z daného ustanovenia vyplýva, že zverejnením aj keď utajených depeší sa môže javiť, že nebolo porušené žiadne právo, článok však neudeľuje právo nikomu zverejňovať utajované informácie. Druhá časť daného článku hovorí, že: *„Tento článok nebráni štátom, aby vyžadovali udeľovanie povolení rozhlasovým, televíznym alebo filmovým spoločnostiam*." Teda ide tu aj o osobitnú právnu úpravu každého štátu. Osoba, ktorá by aktívne a s cieľom poškodiť určitý štát, získala dané informácie kúpou od informátora by bola žalovateľná. Keby bol J. Assagne americkým občanom, tak by bol stíhateľný z dôvodu vlastizrady. Vlastizradou sa rozumie konanie občana s cieľom poškodiť vlastný štát v rámci kontrarozviedky inej krajiny. Článok 10 odsek 2 Európskeho dohovoru o ľudských právach hovorí: *„Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci*." Z tohto výroku možno takisto usúdiť, že zodpovednosť za vyzradenie tajných informácií sa posudzuje podľa zákona, a v takom rozmedzí ako si určujú štáty samé. Z tohto pohľadu J. Assagne neporušil žiadne právo, aj keď jeho počínanie má nepriaznivý vplyv na medzinárodnú politiku.
V súvislosti takýmto okrajovým javom viaceré štáty začali s úpravou a aktualizáciou svojich trestných zákonov, alebo iných zákonov. Príkladom je Rusko, ktoré vo svojom trestnom zákonníku vymedzilo pojem zrady štátu-vlastizrady v kapitole 29, konkrétne v článku

---

8 Viedenský dohovor o diplomatických stykoch, uverejnený pod číslom 157/1964 Zb., článok 24.

275 ruského trestného zákonníka.[9] Podľa novej úpravy z vlastizrady môže byť obvinený aj ten kto priamo pracuje pre cudzie rozviedky. Za vlastizradu je zodpovedný aj občan, ktorý pôsobí v rámci medzinárodnej organizácie, ktorej činnosť je nasmerovaná voči bezpečnosti štátu. Žalovateľná bude aj akákoľvek forma pomoci týmto organizáciám. Obžalované budú aj konzultácie, finančná a materiálno-technická ako aj iná pomoc pre dané subjekty, pretože každá z týchto činností je považovaná za protištátnu. Dokonca aj oficiálna práca na kontrakt so zahraničnými organizáciami môže byť považovaná za trestnú, ak vyšetrovanie preukáže, že tieto štruktúry konali proti štátu. Do trestného zákona sa okrem toho zavádza osobitný článok *„Nezákonné získanie informácií obsahujúcich štátne tajomstvo".*
Nový článok spomína aj občana, ktorý štátne tajomstvo zmení na objekt kúpy a predaja, teda nový článok predpokladá nielen úmysel ale aj vedomé a cielené vyzradenie štátneho tajomstva s cieľom zisku. Významným kapitolou v ruskom trestnom zákonníku je kapitola 28, ktorá spomína protiprávny prístup k informáciám v počítači, v počítačovom systéme, v sieti a na pamäťových médiách ako aj ich zneužitie.[10] Vzhľadom na osobitnú povahu internetu je nevyhnutná jeho osobitná a jedinečná úprava, ktorá by mala zahŕňať jednak medzinárodné a jednak vnútroštátne prvky. Daná koncepcia pre rozsiahle internetové komunikácie by mala byť upravená medzinárodnými právnymi nástrojmi, ktoré majú význam na riadenie internetu a to menovite prostredníctvom zmlúv, dohovorov, obyčajového práva, *ius cogens* a prostredníctvom nezáväzných právnych predpisov. Problémom pri vytvorení tejto koncepcie sú značné rozdiely v názoroch týkajúcich sa hlavných zásadách riadenia internetu a v rozdieloch týkajúcich sa návrhov právnych noriem, ktoré by internetovú oblasť mali zahŕňať. Ďalšou možnosťou by bolo zavedenie protokolu[11] prípadne zákona o užívaní internetu, no ich zavedenie by mohlo byť zdĺhavé a problematické.

2. Ochrana diplomatickej komunikácie

„Úradná korešpondencia misie je nedotknuteľná. Pod úradnou korešpondenciou sa rozumie všetka korešpondencia majúca vzťah k misii a jej funkciám."[12] Tento článok 27 odsek 2 Viedenského dohovoru, hovorí o tom, že danú korešpondenciu nemožno zadržať ani otvoriť. Toto ustanovenie je prísnejšie ako v prípade korešpondencie konzulov. Súčasťou diplomatickej pošty môžu byť aj listy osobného charakteru aj ľahšie zásielky ak to interné predpisy ministerstva zahraničných vecí nezakazujú. Diplomatická pošta musí byť zreteľne označená, najbežnejšie znakom CD[13] aby mohla požívať diplomatickú ochranu. Šifrovaná ako aj bežná diplomatická pošta sú prísne evidované a monitorované. Musia spĺňať predpísané formálne aj obsahové náležitosti. E-maily na rozdiel od diplomatickej písomnej pošty nie sú označované prostredníctvom diplomatických značiek.[14] Ich označenie nie je možné, ich ochrana spočíva tým, že sú prenášané cez **WPN** linku. Úradné e-maily sú v špeciálnych režimoch, z čoho vyplýva, že aj prístup do nich je zložitejší. Sú prenášané satelitným systémom do ktorého nemá prijímajúci štát prístup. Všetka diplomatická korešpondencia je *in*

---

9 Trestný zákonník Ruskej federácie, Hlava 29 (Ugolovnij kodeks – Glava 29. Prestuplenja protiv osnov konstytucyjonnogo stroja i bezopasnosti gosudarstv), dostupné online: http://www.ug-kodeks.ru/ug/ug-kodeks.ru/ugolovnij_kodeks_-_glava_29.html.

10 Trestný zákonník Ruskej federácie Hlava 28, článok 272, (Ugolovnij kodeks – Glava 28, Prestuplenja v sfere kompjuternoj informacii) dostupné online: http://www.ug-kodeks.ru/ug/ug-kodeks.ru/ugolovnij_kodeks_-_glava_28.html.

11 Sada pravidiel.

12 Viedenský dohovor o diplomatických stykoch, uverejnený pod číslom, 157/1964 Zb., článok 27.

13 Colis diplomatique.

14 Diplomatic bag, valise diplomatique, colis diplomatique.

claris[15] a jej predmetom nie sú utajované skutočnosti podľa zákona o utajovaných skutočnostiach. Utajené materiály nemôžu byť posielané obyčajnou poštou ako ani zabezpečeným poštovým transferom. Utajené materiály v šifrách sa prenášajú cez spojenie internetu a to buď satelitom alebo prostredníctvom providera internetu v mieste. Utajované materiály sa spravidla dopravujú do rúk komunikačného pracovníka, ktorý daný materiál následne poskytne diplomatovi na nahliadnutie. Ministerstvá majú svoje interné predpisy o diplomatickej pošte ako aj o šifrovej službe. Dané predpisy sa považujú za utajené materiály. Technická a administratívna ochrana spadá pod správu a úpravu každého štátu.

2.1. Nedotknuteľnosť archívov a dokumentov

Viedenský dohovor o diplomatických stykoch ako aj Viedenský dohovor o konzulárnych stykoch vo svojich ustanoveniach konštatujú, že dokumenty a archívy misie sú nedotknuteľné kedykoľvek a kdekoľvek. Termín archív nie je obsiahnutý vo VCDR, na rozdiel od VCCR kde daný termín obsiahnutý je. Analógiou sa pojem archív uvedený vo VCCR aplikuje aj na diplomatický archív. Takisto analógiou sa pripúšťajú aj moderné formy skladovania ako sú počítačové súbory, diskety a CD nosiče, aj keď to v daných dohovoroch nie je uvedené. Nedotknuteľnosťou sa rozumie to, že korešpondencia nesmie byť otvorená, vyhľadaná, zhabaná bez súhlasu a použitá ako dôkaz. Na zvýšenie bezpečnosti a tajnosti diplomatickej korešpondencie sa používajú šifry. Do akej miery môže byť zaručená ochrana korešpondencie závisí od použitých komunikačných prostriedkov. Na výmenu veľmi citlivých informácií sa využíva diplomatická batožina a odosielanie kuriérom, ktorý nemôže byť zadržaný a nesmie mu byť zásielka odobratá.

2.2. Diplomatická a konzulárna batožina

Diplomatická a konzulárna batožina sú chránené špeciálnym označením. Rozdiel medzi ochranou pri diplomatickej batožine a konzulárnej diplomacie je obsiahnutý v Dohovoroch. Podľa VCCR možno zo závažných dôvodov konzulárnu batožinu otvoriť. Podľa VCDR diplomatickú batožinu otvoriť nemožno. Tým, že VCDR neumožňuje otvorenie batožiny, tak umožňuje potenciálne zneužitie, akými sú napríklad drogy alebo zbrane. Voči danému ustanoveniu majú niektoré štáty výhrady a žiadajú obmedzenie diplomatickej pošty tak ako je to u konzulov. V súčasnej dobe sa však všetka batožina podrobuje skenom, v dôsledku negatívnych skúseností. Je všeobecne uznávanou praxou pre letecké úrady skenovať diplomatické batožiny a dokonca odmietnuť ich dopravu, kde sa predpokladá, že sú potenciálnou hrozbou pre bezpečnosť lietadla. Ak odoprie skenovanie batožiny leteckým úradom, tak bude nútený použiť inú formu dopravy svojej diplomatickej batožiny, napríklad kuriérom.

3. Dohovory VCDR a VCCR, ich analógia a potreba prepracovania

Z dôvodu rozvoja technického pokroku ako aj rozvoja foriem komunikácie je nutné zaoberať sa otázkou a potrebou výkladov Viedenských konvencií o diplomatických ako aj konzulárnych stykoch, konkrétne ustanovení, ktoré sa týkajú foriem a ochrany komunikácie. Viedenský dohovor o diplomatických stykoch bol prijatý roku 1961 a Viedenský dohovor o konzulárnych stykoch pochádza z roku 1969, je teda evidentné, že v dobe kedy boli prijaté sa nepredpokladala potenciálna forma komunikácie prostredníctvom internetu, mailu a podobne. Dohovory takisto nekonkretizujú formu archívov v akých majú byť písomnosti

---

15 V otvorenej reči.

uložené, teda nespomínajú ani nepredpokladajú moderné formy uskladňovania dokumentov ako sú diskety, CD nosiče, externé disky. Vyvstáva teda otázka, či na výklad ustanovení obsiahnutých v konvenciách bude stačiť analógia alebo či by nebolo adekvátnejšie prijatie noviel daných dohovorov.

Záver

V súčasnom svete a modernej dobe panuje technologický pokrok a s ním spájaný rozvoj elektronickej komunikácie. Modernú komunikáciu využívajú nielen bežní ľudia, ale aj predstavitelia štátov, príslušníci zastupiteľských úradov a teda aj každý jedinec. S modernou komunikáciou sa nám spájajú mnohé výhody ako sú aj ušetrenie času, prípadne menšie finančné výdavky. No často s mnohými pozitívami sa spájajú aj mnohé nevýhody. Internet ako nový fenomén doby nemá podrobne určené pravidlá používania ani presne stanovené možnosti ochrany obsahu komunikácie, ktorá sa jeho prostredníctvom prenáša. Z tohto dôvodu pri posielaní citlivých informácií je predsa len bezpečnejšie využívať tradičnejšie metódy.

Význam internetu v medzinárodnom obchode

Marián Seman

„The Internet is becoming the town square for the global village of tommorow."
Bill Gates

Úvod

V dnešnom svete 21. storočia je medzinárodný obchod nevyhnutnou podmienkou hospodárskeho rastu každej krajiny. Prešiel dlhú cestu, od cezhraničných obchodných začiatkov medzi gréckymi mestskými štátmi, cez výrazne obchodné styky talianskych štátov ako Benátky, či Janov, až po súčasné globálne obchodné aktivity Číny či USA. Import a export sa prostredníctvom medzinárodnej deľby práce stali základným stavebným kameňom fungovania modernej civilizovanej spoločnosti. Výmena tovarov a služieb medzi národnými ekonomickými celkami dlhé roky prebiehala klasickými formami obchodovania, poznamenanými rôznymi ekonomickými teóriami.[1] Tento spôsob je finančne a administratívne náročný, čo do značnej miery bránilo rozvoju takéhoto podnikania najmä pre malé a stredné podniky.

Nedá nám nesúhlasiť s výrokom Billa Gatesa, jedného z najbohatších ľudí na planéte a zakladateľa Microsoftu,[2] kde nadnesene označil internet za námestie svetového mesta budúcnosti. Internet zaujal v živote človeka nenahraditeľné miesto. Jeho vplyv na spoločnosť ako takú je nepopierateľný a postupne začal zohrávať dôležitú úlohu aj v rámci medzinárodného obchodu. Dovolíme si tvrdiť, že tak, ako v predchádzajúcich storočiach do obchodu zasiahla priemyselná revolúcia a natrvalo zmenila jeho tvár, to isté sa v tejto dobe pred našimi očami odohráva prostredníctvom internetu. Výmena tovarov a služieb cez internet nepochybne veľmi rýchlo napomáha k rozvoju medzinárodného obchodu. Myslíme si, že potenciál, ktorý tkvie v elektronickom obchode, či možno povedať on-line službách nie je ešte ani zďaleka vyčerpaný a do budúcna môže znamenať základný prostriedok na cezhraničné obchodovanie.

Ak sa štáty dokážu popasovať s výzvou, ktorá pred nimi stojí v podobe obchodovania prostredníctvom internetu, urobia všetko pre to, aby podporili jeho ďalší progres a rozvoj, a zároveň dokážu ochrániť najmä spotrebiteľov, ale taktiež podniky pred jeho nástrahami, môže sa internet stať budúcim „Wall Street" medzinárodného obchodu.

1. Využívanie internetu v medzinárodnom obchode

V krajinách OECD (The Organisation for Economic Co-operation and Development) malo celkové širokopásmové pripojenie v prepočte na 100 obyvateľov v roku 2009 približne 23,10 %.[3] Ak by sme sa pozreli na domácnosti v Európskej Únii (ďalej len EÚ), v roku 2010 malo podľa Európskej Komisie (výsledky prieskumu Eurostat) prístup k internetu 70% z nich, pričom viac než polovica (56%) jednotlivcov v krajinách EÚ v roku 2010 ho využívalo na vyhľadávanie informácii o tovare alebo službách. Dve pätiny (40%) ľudí v týchto štá-

---

1 Od merkantilizmu, cez klasickú a neoklasickú teóriu medzinárodného obchodu, až po peňažnú teóriu medzinárodného obchodu.

2 Spoločnosť Microsoft Corporation je jednou z najvýznamnejších svetových firiem v oblasti softvéru, služieb a internetových technológií pre osobné aj obchodné využitie. (Viac pozri: Microsoft, Profil spoločnosť Microsoft Corporation. Dostupné na online: http://www.microsoft.com/slovakia/mic/onas/mscorp_profil.aspx).

3 OECD, Statistics, Dostupné na internete: http://dx.doi.org/10.1787/888932398081.

toch si prostredníctvom internetu objednali tovar alebo služby na súkromnú potrebu.[4] Ten istý prieskum nás informuje, že v roku 2010 nemalo v krajinách EÚ prístup k internetu len asi 5% podnikov, pričom takmer dve tretiny z nich malo vlastnú webovú stránku (pri veľkých podnikoch to bolo podľa štatistík až 92%). Treba dodať, že výsledky štatistiky znižovali údaje z menej rozvinutých krajín v oblasti informačných a komunikačných technológii (ďalej len IKT) ako Rumunsko či Bulharsko. Dôležitým údajom je, že internetový obchod v roku 2009 tvoril asi 14% obratu v rámci podnikov, ktoré zamestnávajú aspoň 10 zamestnancov (tento podiel bol od 1% na Cypre po približne 24% v Írsku).[5]

Tak, ako sa internet stal dôležitým nástrojom nášho každodenného súkromného života, tomuto trendu sa postupne začínajú prispôsobovať aj firmy a svoje pôsobenie rozširujú aj do tejto sféry. V značnej miere sa aktivita v medzinárodnom obchode začína presúvať na internetový trh prostredníctvom on-line služieb. Pod pojmom „on-line služby" tu chápeme *„služby poskytované na diaľku elektronickým spôsobom, na žiadosť príjemcu služby a za platbu. Zahŕňajú elektronický obchod s tovarom (vrátane kultúrnych hodnôt, liekov) a so službami (vrátane on-line hier), ale aj sociálne siete, diaľkové odborné vzdelávanie atď.*"[6] Treba však zdôrazniť, že existuje stále vysoký nepomer pripojenia spotrebiteľov k internetu a aktívnemu obchodovaniu prostredníctvom neho. Ďalším dôležitým faktorom je, že keď už sa spotrebiteľ odhodlá k využitiu on-line služieb, vo väčšine nejde o cezhraničný obchod, ale tuzemský podnik.[7] A napokon tiež fakt, že úroveň IKT je nie len v celosvetovom, ale taktiež v regionálnom meradle (EÚ, Východná Ázia, Južná či Latinská Amerika) nerovnomerne rozvinutá.[8] Preto je nevyhnutné, aby sa ďalej pracovalo na rozvíjaní IKT, informovaní a vzdelávaní predajcov a spotrebiteľov o možnostiach ich využitia na nákup a predaj tovarov a služieb, vzájomnom spolupôsobení štátov na základe bilaterálnych, no predovšetkým regionálnych multilaterálnych úrovniach pri rozvoji a podpore cezhraničného obchodu prostredníctvom internetu a dôslednej ochrane týchto subjektov obchodovania, čo zvýši dôveru a záujem v takýto obchod a v konečnom dôsledku zabezpečí ďalší nárast produktivity národných hospodárstiev.

2. Internetové obchodovanie v Európskej Únii

EÚ ako nástupca Európskeho hospodárskeho spoločenstva (EHS) je budovaná okrem iného predovšetkým na myšlienke jednotného spoločného trhu s voľným pohybom kapitálu a tovaru, upravovaným spoločnými jednotnými pravidlami. Tento trh dnes už vo výraznej miere zahŕňa tiež internetový priestor na ktorom sa odohrávajú dôležité obchodné aktivity. Ak hovoríme o jednotnom trhu EU, nesmieme opomenúť digitálny trh. Zmysel, účel a význam internetu v medzinárodnom obchode, nie len v rámci EÚ, ale aj s ostatnými re-

---

4 Štatistika informačnej spoločnosti, European Commission, Eurostat Dostupné na internete: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics/sk.

5 Tamtiež.

6 Pozri: Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a online služieb, str. 1, 2012.

7 *„Cezhraničný elektronický obchod v EÚ-27 využíva iba 9 % spotrebiteľov EÚ a 18 % maloobchodníkov EU; 48 % spotrebiteľov uviedlo, že pri nakupovaní on-line viac dôverujú nakupovaniu vnútroštátne ako cezhranične."* Pozri: Zelená kniha, Integrovaný trh s doručovaním balíkov s cieľom oživiť elektronickýý obchod v EÚ, Európska Komisia, Brusel, 29.11.2012, 2012, str. 5, dostupné online: http://ec.europa.eu/internal_market/consultations/docs/2012/parcel-delivery/121129_green-paper-parcel-delivery_sk.pdf.

8 Vyššie spomínané štatistiky krajín EU (str.4).

gióonmi sveta si inštitúcie EÚ prostredníctvom svojich zástupcov uvedomujú, čo je deklarované aj množstvom dokumentov prijatých v danej oblasti na ich pôde.[9] Pokiaľ sa im podarí podporiť dôveru v digitalizáciu trhu, odstrániť nedôveru voči formám obchodovania cez internet, znížiť administratívne nároky na takýto obchod a naopak zvýšiť ochranu dotknutých strán, môže byť hospodársky trh EÚ aj v budúcnosti vyrovnaným partnerom najväčších ekonomík.

Možnosti, ktoré nám jednotný digitálny trh ponúka, by pri ich plnom využití znamenali ďalekosiahle pozitívne následky v prospech celej spoločnosti, od podnikov, ich zamestnancov, cez spotrebiteľov až po životné prostredie. Medzi základnými výhodami takéhoto trhu vidíme nárast konkurencieschopnosti nie len medzi medzinárodnými korporáciami, ale najmä v prospech stredných a malých firiem, až po mikropodniky, ktorým sa otvorí šanca jednoduchšie sa dostať na trh mimo územia štátu, kde pôsobia. Práve obchodovanie medzi firmami navzájom sa prostredníctvom internetu dostalo na novú úroveň. Internet má práve na tieto vzťahy medzinárodného podnikania najvýraznejší vplyv. Pozitívne ho stimuluje a otvára nové možnosti. To sa pozitívne odrazí v prospech zamestnanosti v EÚ, pomôže zmazať demografické a geografické rozdiely,[10] vytvorí množstvo nových pracovných miest a sprístupní tieto pozície širokému spektru obyvateľstva.[11] Taktiež by to prinieslo nespochybniteľné výhody v podobe nižších cien a širšieho sortimentu tovaru a služieb pre spotrebiteľov, väčšiu pohodlnosť a voľnosť pri výbere produktov, zhodnotenie cenových ponúk a informácii o tovare a ich vzájomná komparácia. Netreba zabúdať na to, že jednotný digitálny trh by umožnil občanom lepšie využívať svoje práva, jednoduchšie sa s nimi oboznámiť a bezpečnejšie sa tak realizovať prostredníctvom internetu. Na neposlednom mieste, tiež patrí dopad elektronického obchodovania na životné prostredie. Takáto forma obchodu, výraznou mierou prispieva k budovaniu zelenej ekonomiky, teda pomáha obmedzovať zaťaženosť životného prostredia nežiaducimi vplyvmi.[12]

Dnes je takéto efektívne využívanie spomaľované najmä tým, že neexistuje jednotná právna úprava v rámci EÚ naprieč celým spektrom poskytovania on-line služieb.[13] To sa odzrkadľuje na jednej strane v zneužívaní medzier v nejednotnej legislatíve, a na strane druhej v strachu spotrebiteľov využívať takýto trh na uspokojovanie svojich potrieb a strachu predajcov vstupovať do tohto prostredia, kde neplatia jednotné pravidlá.[14] Nedôvera

---

9 Pozri nižšie.

10 Otvorí to nové príležitosti napríklad pre prácu z domu, a teda sa pracovný trh spružní a stane flexibilnejším, čo môže mať priaznivé dôsledky pre odľahlé kraje jednotlivých štátov, ľudí z vidieka, kde sú pracovné príležitosti značne obmedzenejšie ako v mestách, a tiež pri šanci uplatniť sa na pracovnom trhu pre starších ľudí alebo študentov.

11 Nie len priame pracovné miesta pri on-line obchodovaní, ale tiež nepriamo v doručovateľov tovarov, v IT (Information Technology) oblasti pri výrobe a výskume nových produktov, alebo pri budovaní infraštruktúry.

12 *„Doručovanie domov je v rámci optimalizovanej logistiky energeticky úspornejšie než viacnásobné individuálne premiestňovanie spotrebiteľov. Takisto dochádza k energetickým úsporám na samotnej výrobe tovarov, ktoré si teraz možno napríklad stiahnuť vo forme digitálnych údajov.*“ Pozri: Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a online služieb, 2012, str. 4, dostupný online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:sk:PDF.

13 Takáto úprava je riešená len čiastočne, alebo ponechaná na vnútroštátne právne predpisy.

14 *„Napríklad len 29 % obchodníkov vie, kde možno získať informácie alebo rady o právnych predpisoch týkajúcich sa ochrany spotrebiteľov platných v iných európskych krajinách. 72 % predajcov na diaľku nepozná presnú lehotu na odstúpenie od zmluvy pri predaji na diaľku vo svojej vlastnej krajine.*“ Pozri: Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a online služieb, 2012, str. 8, dostupný online:

v digitálny trh, najmä zo strany spotrebiteľov, značne spomaľuje napredovanie medzinárodného obchodu prostredníctvom IKT. Táto nedôvera je spôsobená nielen nejednotnou úpravou, ako sme to uviedli, ale tiež ťažkou vymožiteľnosťou práva vo viacerých krajinách tohto spoločenstva. Ďalším problémom môže byť slabá informovanosť a vzdelávanie v možnostiach realizácie sa vo svete obchodu prostredníctvom internetu. IKT sa vyvíjajú závratnou rýchlosťou, na čo samotné modely obchodovania nestíhajú promptne a včas reagovať. Smartphony a tablety posunuli on-line obchodovanie opäť o úroveň vyššie, čomu sa už snažia prispôsobiť aj poskytovatelia on-line služieb. Na ich plnohodnotné využívanie je však potreba osvety medzi spotrebiteľmi, ktorí často ešte pochybujú a majú strach z možností, ktoré nám tieto technológie poskytujú.

V tomto kontexte tiež netreba opomenúť potrebu posilnenia dôvery voči bezpečnosti elektronických platieb na diaľku a spoľahlivých systémov doručovania. Preto je dôležité, aby sa v rámci únie vytvoril jednotný bezpečný a spoľahlivý platobný priestor, kde by sa realizovali platby prostredníctvom platobných kariet, cez internet, či mobilné platby.[15] Približne 35 % používateľov internetu nenakupuje on-line, pretože pochybuje o bezpečnosti platieb.[16] Navyše, za hlavný jav, vplývajúci na mieru nedôvery v on-line nakupovanie sa na základe štatistík ukazuje, nepríjemná skúsenosť s doručovaním takto kúpeného tovaru. Či už sú to dlhé lehoty doručovania (28% spotrebiteľov), poškodenie výrobku (20%), celkové nedoručenie objednaného výrobku (17%), alebo doručenie iného tovaru (14%), ako aj to, že konečná cena s doručením bola vyššia ako cena uvedená pri nakupovaní (a teda nimi predpokladaná cena za tovar), čo uviedlo 7% spotrebiteľov.[17]

Množstvo z týchto problémov je viac či menej riešených v Smernici 2000/31/ES (smernica o elektronickom obchode). Podpora integrácie európskeho trhu takouto koordináciu právnych poriadkov výrazne prispieva ku zatraktívneniu podnikateľskej činnosti, čo pozitívne stimuluje hospodársky rast. V smernici sa jednotnou definíciou vyjasňujú niektoré pojmy a určujú zásade pre elektronický obchod. Rieši okrem iného tiež úpravu elektronických zmlúv, komerčnú komunikáciu, zodpovednosť sprostredkovateľov poskytovateľov služieb a iné.

3. Spôsoby obchodovania prostredníctvom internetu

Priemerný Európan si dnes už nedokáže predstaviť svoj život bez smartfónu, laptopu, či tabletu, kde si skontroluje mailovú poštu, urobí bankový prevod, prezrie účet na sociálnej sieti, prečíta noviny, objedná večeru a kúpi lístok na vlak. To všetko je priestor na obchodnú činnosť. Svet sa v oblasti ITK každodenne posúva míľovými krokmi dopredu a za posledné desaťročia značne pretvoril našu spoločnosť. Internet nepozná štátne hranice, na prezeranie zahraničných stránok nepotrebujete pasy ani víza, povolenia, ani sa za to neplatia žiadne špeciálne poplatky. Ak opomenieme isté formy regulácie v niektorých krajinách,

---

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:sk:PDF.

15 Základy takéhoto fungovania položila SETA (Single Euro Payments Area), ktorého základným cieľom je dá sa povedať zjednotenie platobných štandardov v EÚ (pozri: Národná Banka Slovenska, Platobné systémy, SEPA).

16 Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a online služieb, 2012, str. 11, dostupný online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:sk:PDF.

17 Pozri: Zelená kniha, Integrovaný trh s doručovaním balíkov s cieľom oživiť elektronický obchod v EÚ, Európska Komisia, Brusel, 29.11.2012, 2012, str. 10, dostupné online: http://ec.europa.eu/internal_market/consultations/docs/2012/parcel-delivery/121129_green-paper-parcel-delivery_sk.pdf.

tak si dovolíme tvrdiť, že internet spája celý svet na jednom mieste. To prinieslo firmám a spotrebiteľom dovtedy nevídané možnosti. Nikdy pred tým nebolo tak jednoduché rezervovať si hotel na druhom konci sveta, zabookovať si letenku, objednať si oblečenie z iného kontinentu, alebo si kúpiť album obľúbeného interpreta, ktorý vyšiel pred niekoľkými sekundami.

Z toho pramení množstvo foriem on-line obchodovania. Medzi základné členenie patrí obchodovanie bussiness to bussiness (B2B) a bussiness to customer (B2C).[18] B2B zahŕňa transakcie medzi firmami navzájom, ich obchodné styky a aktivity. B2C je už typický obchodný styk medzi firmou a spotrebiteľom, teda predaj koncovému užívateľovi. Okrem toho tu vznikajú tiež iné formy, ako napríklad customer to customer (C2C), kedy dochádza k obchodovaniu medzi spotrebiteľmi navzájom alebo obchod customer to bussiness (C2B), kedy je zákazníkom podnik a predávajúcim fyzická osoba.[19]

Práve tzv. „bussiness to bussiness" obchodovanie je formou, ktorá v elektronickom obchodovaní prevažuje a zároveň je aj najstarším spôsobom e-obchodovania.[20] Ako sme už uviedli, je to spôsob obchodných vzťahov medzi firmami navzájom (medzi výrobcami a veľkoobchodmi, alebo medzi veľkoobchodmi a predajcami). Takéto obchodovanie je prevažujúce najmä z dôvodu, že kým transakcia medzi predajcom a spotrebiteľom prebehne raz, transakcie pri tom istom tovare prebehnú niekoľkokrát viac medzi firmami.[21] Aj do tejto skupiny obchodovania zásadne zasiahol internet. Nadväzovanie vzťahov, komunikácia medzi obchodnými partnermi, dodávateľmi a odberateľmi, dopravcami a pod. nebola nikdy predtým taká rýchla a efektívna. Dojednávanie a uzatváranie zmlúv je už možné na diaľku, taktiež prostredníctvom IKT. Práve to je výhodou pre medzinárodné styky. Avšak, prináša aj množstvo rizík, ktoré sa pri obchodovaní medzi firmou a spotrebiteľom nejavia (tie si rozoberieme nižšie).

Za jednu z najsilnejších zbraní internetu z hľadiska obchodu (v rámci štátu, rovnako ako medzinárodného) považujeme reklamu. Reklama je istá forma propagácie tovaru alebo služby, firmy, alebo obchodnej značky.[22] Jednou z foriem reklamy je reklama internetová. Môžeme ju charakterizovať ako propagovanie nie len tovaru či služby, ale tiež webových stránok daného podniku, za účelom zvýšiť zisk. Takáto forma propagácie má mnoho výhod. Je rýchla a flexibilná (zmena v reklame sa dá urobiť behom sekundy), s dostupnou odozvou (zaznamenávajú sa počty návštev webovej stránky, či kúpených produktov), ale tiež lepšie zameraná na cieľovú kategóriu (zobrazuje sa pri zadaní kľúčových slov do vyhľadávača, alebo na sociálnej sieti užívateľovi, ktorý najčastejšie navštevuje tematický

---

18 Základné druhy elektronického obchodu, Dostupné na internete: http://blog.topshopping.sk/2009/11/02/typy-internetovych-obchodov-vyhody-a-nevyhody/#.UVT9SRxFWYE.

19 Tamtiež.

20 Legal Aspects of Electronic Commerce in International Trade, Prednáška José Angelo Estrella-Faria, Audiovisual library of international law, dostupné na internete: http://untreaty.un.org/cod/avl/ls/Estrella-Faria_IEL.html#.

21 Príkladom môže byť predaj mobilného telefónu. Keď si kúpite mobilný telefón v obchode s elektronikou, prebehne jedna transakcia. Ale kým sa mobil dostane do predaja v obchode, prebehne veľký počet transakcií medzi firmami. (výrobca nakupuje materiál a súčiastky na výrobu – následne predaj veľkoobchodníkovi – predaj do maloobchodu. Navyše sa na tom podieľa množstvo prepravcov a pod.).

22 *„Reklamou sa rozumie akékoľvek predvedenie súvisiace s obchodom, podnikaním, remeslom alebo povolaním, ktorého cieľom je podpora odbytu tovaru alebo služieb, vrátane nehnuteľností, práv a záväzkov."* Pozri: Smernica 2006/114/ES o klamlivej a porovnávacej reklame z 12 decembra 2006, str. 1.

podobné stránky). Navyše ako sme spomínali, internet nie je obmedzený štátnymi hranicami, a to je veľkou devízou aj pre reklamu na ňom.

Najčastejšou formou internetového predaja tovarov sú tzv. e-shopy. E-shop je opakom kamenného obchodu, teda klasického priestoru pre obchodovanie. Spravidla poskytuje katalógovú formu ponuky tovarov ktoré firma takto ponúka. Má prehľadnú štruktúru v ktorej sa dá dobre orientovať, a tovar je zoradený podľa ceny, farby, druhu, či iné. Pri konkrétnom tovare býva zvykom zobrazovať bližšie informácie o ňom, a jeho fotodokumentáciu. Takto sa dá nakupovať od oblečenia, cez domáce spotrebiče a počítačovú techniku, kozmetiku až po nábytok a autosúčiastky. Výnimkou nie je možnosť komunikácie s predajcom pri potrebe poradenstva vo výbere tovaru, alebo spresnení informácii o ňom. Formu platby si zvyčajne volí spotrebiteľ, alebo je určená predajcom.

Poskytovanie služieb podlieha spravidla tým istým pravidlám ako e-shopy, avšak ich režim býva v niektorých prípadoch osobitný. Príkladom je poskytovanie on-line hier a stávok, čo vo väčšine štátov podlieha potrebe licenčného práva na takéto služby. Iným príkladom je poskytovanie ubytovacích služieb, alebo zájazdov prostredníctvom internetu. To sa stáva najčastejšou formou cezhraničného obchodu, keďže internet uľahčil prístup k zahraničným hotelom a cestovným kanceláriám. Taktiež internetové služby, akými sú elektronická pošta (email), videokonferencia, internetové noviny, alebo rôzne druhy kanálov na zdieľanie videí či obrázkov sú najbežnejšie formou využívania internetu, pričom (aj keď si to mnohokrát neuvedomujeme) pri nej dochádza k obchodovaniu (a to často cezhraničnému).

Špecifickým druhom služieb, prostredníctvom internetu sú služby poskytované bankami a inými finančnými inštitúciami. Bankový sektor ako taký používa viaceré špecifiká a ináč tomu nie je ani pri využití internetu. Možnosť platby platobnou kartou, alebo výber hotovosti z bankomatu sa pre nás stali rutinou, keďže tieto inštitúcie už dávno spojili svoju činnosť s technickými vymoženosťami. Sledovanie bankového konta, manipulovanie s ním, či dokonca poskytnutie hypotéky sa už dnes dá vybaviť cez internet. Tzv. online-banking, alebo mobile-banking je častým spôsobom narábania s našimi financiami prostredníctvom internetu.

Napokon novým fenoménom internetu sa stalo obchodovanie medzi spotrebiteľmi. Prostredníctvom svetových serverov a aktívnych portálov, ako www.ebay.com dochádza k výmene tovarov priamo medzi spotrebiteľmi.[23] Spotrebiteľ zverejní na serveri produkt, ktorý už nepotrebuje a chce ho predať, aj svoje kontaktné údaje, na čo môžu záujemcovia reagovať a môže tak dôjsť k obchodnej transakcii. Takýto predaj sa často realizuje formou internetovej aukcie. Za obchodovanie medzi spotrebiteľmi môžeme označiť tiež vytvorenie veľkého množstva fór na internete, prípadne priestoru pre recenziu na internetových stránkach firiem, kde dochádza k výmene informácii a skúseností o tovaroch a službách priamo medzi spotrebiteľmi.

Napokon je v tomto kontexte tiež zaujímavé sa upriamiť na vznik, resp. existenciu samostatnej, nezávislej digitálnej meny, tzv. bitcoin. Dáva možnosť vykonať transakcie komukoľvek a kdekoľvek cez internet za minimálny poplatok, pričom sa využíva samostatná mena existujúca iba v digitálnej forme. Funguje na princípe peer-to-peer, teda programu vzájomne prepojených „užívateľov". Je označovaná tiež ako kryptomena, a funguje na absolútne decentralizovanom princípe. Teda nie je nikým ovládaná a ovplyvňovaná, a taktiež nie je ničím krytá. Za bitcoin sa dajú nakúpiť tovary a služby, no dá sa tiež vymeniť za inú

---

23 Alebo tiež www.amazon.com či u nás www.aukcie.sk.

menu.[24] Jej budúcnosť je nejasná, najmä z pohľadu legislatívnej regulácie a zásahov zo strany štátov, avšak jej vytvorenie a dnes reálne používanie dáva do budúcnosti obrovskú víziu pre on-line obchodovanie.[25]

4. Právna úprava a problémy obchodovania

Ako sme už vyššie spomenuli, na rozvoj medzinárodného internetového obchodovania je potrebné okrem iného zvýšiť dôveru v takéto podnikanie. Vyskytuje sa množstvo problémov, ktoré oslabujú dôveru a kladú prekážky v rozvoji internetovému podnikaniu. Za najzávažnejšie považujeme nejednotnosť právnej úpravy a nízku vymožiteľnosť práva,[26] čo vytvára množstvo ďalších problémov. Takými problémami je bezpečnosť nákupu cez internet, ochrana osobných údajov, ochrana platieb, zavádzajúce a klamlivé údaje. Taktiež dôležitý problémom sa stali „daňoví špekulanti".

Množstvo firiem zbiera a uchováva citlivé informácie o spotrebiteľoch, ako sú mená, adresy, čísla kreditných kariet či iných účtov a pod. Takáto firma musí zabezpečiť, aby nedochádzalo k úniku alebo inému zneužitiu týchto informácii. Dôsledná a efektívna ochrana osobných údajov zvýši dôveru spotrebiteľov v nákup on-line, a vyhne sa množstvu právnych problémov. Na tento účel je u nás vytvorený Úrad na ochranu osobných údajov, ktorý má na starosti prípravu legislatívy v tejto oblasti, kontrolu jej dodržiavania a dodržiavanie jej súladu s právom EÚ. Potrebné je však chrániť tiež firmy, resp. podnikateľov. Najmä ochrana autorských práv je prostredníctvom internetu narušaná. Je nutné chrániť autorov diel a vlastníkov značiek pred nenažitím ich obchodného mena, resp. nelegálnemu šíreniu ich produktov. U nás samozrejme na tento účel slúži autorský zákon 618/2003 Z.z., ale tiež napr. Smernica Európskeho parlamentu a Rady 2011/77/EU a ďalšie. Okrem toho ako už bolo spomínané, je potrebné ochrániť platby pri nakupovaní on-line. V tejto súvislosti je dôležitý Zákon č. 492/2009 Z.z. o platobných službách (alebo napr. na Európskej úrovni Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a on-line služieb). Internet sa stal taktiež širokým spektrom pre rôznych špekulantov z rád obchodníkov, ktorí zneužívajú nevedomosť spotrebiteľa. Je preto dôležité nie len nastaviť pravidlá na jeho ochranu, ale taktiež dostatočne informovať a vzdelávať ľudí v tejto oblasti.[27] V neposlednom rade je nevyhnutné nastaviť pravidlá v oblastí daní pri medzinárodnom obchode a mechanizmy pre ich dodržiavanie, alebo odstránenie zbytočných byrokratických opatrení a colných povinností, ktoré znižujú efektívnosť on-line predaja.[28]

Ako už bolo vysvetlené, najrozšírenejšou formou obchodovania cez internet je obchodovanie medzi firmami navzájom. To sa vystavuje v niektorých oblastiach ďaleko vyššiemu riziku, ako obchodovanie v klasickom ponímaní. Hlavným dôvodom sú omnoho väčšie investície do takého obchodovania. Najnebezpečnejšími sú kurzové, dodacie, ale tiež politické riziká, ktoré musí firma zvážiť a prípadne podstúpiť ak chce uspieť v konkurencii.

---

24 Jej kurz sa pohyboval v apríli 2013 na úrovni približne 159 USD za 1 BTC (bitcoin).

25 Pre viac pozri na http://bitcoin.org/en/.

26 Čiastočne je to riešené prostredníctvom možnosti riešenia sporov on-line. Teda aj takýmto spôsobom sa prispieva k zvyšovaniu dôveryhodnosti v on-line nakupovanie, a väčšej možnosti vymôcť svoje práva.

27 Častým javom je napr. zneužívanie nevedomosti zákazníkov o ich práve na bezplatné odstúpenie od zmluvy bez uvedenia dôvodu do 7 pracovných dní (pozri zákon č. 108/2000 Z. z.), čo predajcovia v niektorých prípadoch neakceptujú, neinformujú zákazníka o takejto možnosti, alebo si za to účtujú dodatočné poplatky. To všetko v rozpore so zákonom.

28 Pozri napr. Smernica Rady 2006/112/ES z 28. novembra 2006 o spoločnom systéme dane z pridanej hodnoty – tzv. smernica o DPH.

Aby takéto obchody mohli prebiehať v bezpečí, najmä na tento účel bol vytvorený inštitút zaručeného elektronického podpisu. Je to elektronický podpis, pri ktorom je možné overiť pravosť dokumentov a autentifikáciu podpísaného. Zabezpečuje sa prostredníctvom certifikovanej aplikácie, bezpečného zariadenia a kvalifikovaného certifikátu. Elektronický podpis je upravený Zákonom č. 215/2002 Z.z. o elektronickom podpise. V oblasti medzinárodného obchodovania prostredníctvom internetu medzi firmami sú funkčné najmä organizácie OSN vytvorené pre oblasť e-obchodovania, ktoré uvedieme v ďalšom texte (napr. UNCITRAL).

Právo sa snaží na tieto relatívne nové problémy reagovať čo možno najviac efektívne, pričom sa nevyhne moderným tendenciám v právnej úprave. Preto si dovolíme tvrdiť, že v tejto oblasti sa regulatívy primajú predovšetkým na medzinárodnej úrovni, v rámci rôznych spoločenstiev a regiónov. V tomto rozmere sú aktívne najmä inštitúcie EÚ, ktoré prijali mnoho smerníc, odporúčaní a uznesení viac že menej záväzných pre členské štáty. Takými sú napr. Smernica o elektronickom obchode 2000/31/ES, Smernica 2006/114/ES o klamlivej a porovnávacej reklame, Uznesenie Rady o stratégii spotrebiteľskej politiky EÚ, Koherentný rámec na posilnenie dôvery v jednotný digitálny trh elektronického obchodu a on-line služieb, Uznesenie Európskeho parlamentu o medzinárodnom obchode a internete (2008/2204(INI) a iné). Na tento účel si medzinárodné zoskupenia zároveň vytvárajú orgány, ktoré sa danej problematike venujú, riešia spomínané, aj iné problémy v danej oblasti a navrhujú legislatívnu úpravu pre ich riešenie, ako ja kroky na efektívne využívanie IKT. Takou je napríklad UNCITRAL. Je komisiou OSN pre medzinárodné obchodné právo, ktorá sa v značnej miere zaoberá aj elektronickému obchodovaniu (prostredníctvom samostatnej pracovnej skupiny pre elektronický obchod). Predmetom jej činnosti je harmonizácia a modernizácia pravidiel pre medzinárodný obchod. Vypracovala množstvo relevantných dokumentov, návrhov dohovorov a iné.[29] Ďalšou takouto organizáciou je ITU (Medzinárodná telekomunikačná únia). ITU je špecializovanou agentúrou OSN. Dalo by sa povedať, že jej cieľom je prepojiť prostredníctvom IKT celý svet navzájom. Jej činnosť je podstatná aj toho pohľadu, že okrem členstva štátov OSN, sú jej členmi aj vedúce akademické inštitúcie a niekoľko stovák súkromných spoločností. Samozrejme že jednou z oblastí jej činnosti je aj internet.[30] Ďalším dôležitým „hráčom" na tomto poli je tiež WTO (Svetová obchodná organizácia). Vyvíja v tejto oblastí množstvo aktivít – uskutočňuje rôzne semináre a workshopy, vydáva dohody, deklarácie a štúdie v tejto problematike a skúma rôzne aspekty elektronického obchodu po každej stránke. Významnou je napríklad Ministerská deklarácia Doha z roku 2001, ktorá zahŕňa celé spektrum internetového obchodovania, deklaruje zásady ktorými sa chce ďalej uberať a vyvára rámec pre realizáciu internetového obchodovania do praxe.[31]

Neznamená to, že by legislatívna činnosť na vnútroštátnej úrovni bola menej dôležitá. Významnými sú napríklad zákon č. 250/2007 Z.z. o ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov, alebo Zákon č. 108/2000 Z.z. o ochrane spotrebiteľa pri podomovom predaji a zásielkovom

---

29 Naposledy napr. Návrh ustanovenia o elektronických prevoditeľných záznamov z mája 2013(A/CN.9/WG.IV/WP.122), ale aj množstvo iných, ako napr. Právne aspekty elektronického obchodu – právne prekážky brániace rozvoju elektronického obchodu v medzinárodných nástrojoch týkajúcich sa medzinárodného obchodu: spôsob ich prekonania (A/CN.9/WG.IV/WP.89) a iné.

30 Viac pozri na: http://www.itu.int/en/Pages/default.aspx.

31 Pozri: Ministerial declaration, adopted on 14 November 2001, dostupné online: http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm#electronic.

predaji, Vyhláška Ministerstva životného prostredia SR č. 315/2010 o nakladaní s elektrozariadeniami a elektroodpadom a iné.

Záver

Pokrok vo vývoji IKT napreduje a pretvára našu spoločnosť. Internet sa stal súčasťou nášho každodenného života, čo sa prenieslo aj do medzinárodného obchodu. Pochopenie potenciálu, ktorý v sebe ukrýva nám otvára nevídane možnosti v oblasti obchodu rýchlejšou a flexibilnejšou formou ako kedykoľvek predtým.

Čaká nás ešte dlhá a ťažká práca k vytvoreniu jednotného digitálneho trhu, nie len na pôde EÚ, ale celosvetovo, na konci ktorej je internet miestom, kde prebieha výlučná väčšina obchodných aktivít. Pri odstránení negatív a hrozieb, ktoré v sebe takéto obchodovanie skrýva, pri správnom legislatívnom nastavení a podpore rozvoja sa môžeme dočkať toho, že obchodovanie cez internet bude hrať jednu z hlavných rolí hospodárstva krajín.

Bude potrebné dbať na to, aby sa odstránili prekážky v podobe nerovnomerného vývoja IKT medzi rôznymi regiónmi sveta. Aby ľudia a podniky vo väčšine krajín mali rovnakú možnosť na prístup k internetu, a tak mohli získavať informácie a vzájomne obchodovať. Taktiež je dôležité, aby právne úpravy krajín odrážali súčasnú situáciu a budúce ciele vo vývoji IKT, a tak nebránili jeho napredovaniu a rozmachu, aby sa cezhraničný obchod nezaťažoval zbytočnými povoleniami, poplatkami a inými obmedzeniami, ktoré by mohli odstrašovať podniky vstúpiť na takýto trh, aby sa legislatíva čo možno najviac vzájomne prispôsobila a tým sa zaručila právna istota pre všetky subjekty obchodovania. Nepochybne je dôležité, aby sa zaviedli účinné a efektívne mechanizmy ochrany týchto subjektov. Aby sa zohľadnili špecifiká takéhoto obchodovania a tomu sa tieto mechanizmy prispôsobili. Nech je spotrebiteľ dôsledne informovaný a chránený pred zlými úmyslami špekulantov zo strany firiem pri predaji na diaľku, nech nie sú zneužívané osobné údaje nevyhnutné pri takom predaji, a nech sú takisto chránené platby, ktoré sa takto uskutočňujú. Treba ochrániť pred nebezpečenstvom najmä niektoré osobitné subjekty (maloletí, chorí, a pod.) pred nástrahami na internete prostredníctvom dôslednej kontroly (pri on-line hrách, predaji liekov, prístup k porno stránkam a iné).

Ak dokážeme toto všetko splniť, popasujeme sa výzvami, ktoré pred nás takéto formy obchodu stavajú, veríme, že sa dočkáme sveta, kde spokojní spotrebitelia budú mať prístup k nevídanému sortimentu z najrozličnejších kútov sveta za výhodné ceny a spokojní podnikatelia budú prosperovať ako nikdy predtým, čo sa odrazí na spokojnosti všetkých vrstiev spoločnosti. Štátne hospodárstva dostanú nový impulz, zamestnanosť porastie a globalizácia sveta bude opäť o krok bližšie k spoločnosti, kde sme si všetci rovní v právach a povinnostiach. A takýmto právom je aj právo na informácie, právo podnikať alebo vykonávať inú zárobkovú činnosť, či právo na prístup k tovarom a službám.

Na záver ešte jeden citát od Napoleona Bonaparte - *„Slabí čakajú na príležitosť, silní ju vytvárajú.“* Buďme tými, čo aj formou obchodovania cez internet začnú budovať spoločnosť zajtrajška.

Právo na prístup na internet a iné odlesky používania internetu a ľudské práva

Katarína Kesselová

Úvod

Úlohou ľudských práv je ochrana jednotlivca pred zneužitím alebo neprimeraným uplatňovaním moci zo strany štátu. Potreba uznania ľudského práva vzniká vtedy, keď je ohrozená dôležitá hodnota. Ak sa diskutuje o nutnosti chrániť právo prístupu na internet, potom to znamená, že niečo nie je v poriadku.[1] V súvislosti s technologickými výdobytkami sa stretávame s novou sadou práv. Právo na online identitu, právo na (relatívnu) anonymitu, právo byť zabudnutý,[2] právo na online ochranu osobných údajov a samozrejme, samotné právo na prístup k internetu. Vyžaduje si digitálna evolúcia zavedenie nových práv alebo stačí tie existujúce aplikovať na nové technológie? V príspevku priblížime argumenty v prospech a v neprospech uznania prístupu na internet ako ľudského práva a poukážeme na ťažkosti s vyvažovaním ľudských práv na internete.

1. Argumenty v prospech vyhlásenia práva na prístup na internet za ľudské právo

Demonštrácie počas Arabskej jari sú prvým príkladom odôvodňujúcim význam prístupu na internet.[3] Informačné a komunikačné technológie počas tuniských a egyptských protestov ľuďom umožnili organizovanú mobilizáciu a okamžité informovanie o prebiehajúcich udalostiach. Otázka, či priznať používaniu internetu status ľudského práva vyvstala potom, čo vlády začali prístup na internet obmedzovať. V Tunisku boli zablokované konkrétne stránky a sociálne siete.[4] Vláda v Egypte zvolila tvrdší prístup a nariadila všetkým hlavným poskytovateľom telekomunikačných služieb prerušiť internetové pripojenie.[5] Atmosféra by sa dala zhrnúť do hesla: „Ak ťa vláda zhodí z internetu, je na čase zhodiť vládu."

Druhým argumentom je skutočnosť, že právo prístupu na internet je deklarované v právnych poriadkoch niektorých krajín, a to buď legislatívne alebo v rozhodnutiach ústavných súdov. Vo Fínsku je vyhláškou ministerstva[6] zaručené pripojenie k internetu s rýchlosťou 1 Mbit/s. Vyhláška však nespomína explicitné právo jednotlivca na prístup do sieťovej infraštruktúry, ale hovorí o prístupe k širokopásmovému internetu ako všeobecnej službe, podobnej iným verejným službám ako dodávka vody, elektriny, telefónnych služieb.[7] Taktiež v Estónsku bol zákonom prístup na internet deklarovaný za univerzálnu

---

1 DE HERT, P., KLOZA, D.: Internet (access) as a new fundamental right. Inflating the current rights framework, in: European Journal of Law and Technology, Vol. 3. No. 3, 2012.

2 KESSELOVÁ, K.: Právo byť zabudnutý. Dostupné na: http://www.najpravo.sk/clanky/pravo-byt-zabudnuty.html.

3 PENNEY, J.W.: Internet Access Rights: A Brief History and Intellectual Origins, in: William Mitchell Law Review, Vol. 38, No. 1, p. 12, 2011.

4 STEPANOVA, E.: The Role of Information Communication Technologies in the "Arab Spring".

5 Režimu odhodlanému zablokovať pripojenie v celej krajine uniklo niekoľko kanálov. Egypťania, ktorí ešte vlastnili modemy sa mohli pripojiť cez telefónny systém, i keď pripojenie bolo pomalé a drahé. Google a Twitter spustili službu "speak-to-tweet", ktorá Egypťanom umožnila zanechať hlasovú správu, ktorá bola skonvertovaná na text a zverejnená na webstránke.

6 Decree no. 732/2009 of the Ministry of Transport and Communications on the Minimum Rate of a Functional Internet Access as a Universal Service.

7 LUCCHI, N.: The Role of Internet Access in Enabling Individual's Rights and Freedom. p. 14.

službu. Podľa článku 5a (2) gréckej ústavy[8] má každý právo účasti v informačnej spoločnosti. V Taliansku bola navrhnutá obdobná zmena ústavy s cieľom zaviesť nové právo prístupu na internet.[9] Úvahy o práve na prístup na internet môžeme nájsť aj v judikatúre najvyšších súdov niektorých krajín. Najvyšší súd Kostariky v rozhodnutí, v ktorom konštatoval meškanie vlády s plnením záväzkov podľa CAFTA,[10] podľa ktorej mala vláda otvoriť monopolizovaný telekomunikačný trh novým poskytovateľom,[11] hovorí o *„základnom práve prístupu k týmto [informačno-komunikačným] technológiám, konkrétne o práve prístupu na internet*."[12]

Francúzska ústavná rada sa právu na prístup na internet venovala v rozhodnutí, ktorým zrušila časti zákona HADOPI, zameraného na predchádzanie nelegálnemu digitálnemu kopírovaniu. Podľa ústavnej rady je oprávnenie odpájať ľudí od internetu neústavným zásahom do slobody prejavu a práva na komunikáciu.[13] Štát ma naopak povinnosť uľahčovať produkciu, výmenu, rozširovanie a prístup k elektronicky prenášaným informáciám.

Správa spravodajcu Rady OSN pre ľudské práva[14] je tretím a najdiskutovanejším argumentom v prospech udelenia statusu ľudského práva internetovému pripojeniu. Osobitný spravodajca La Rue v správe OSN uvádza, že *„internet sa stal nevyhnutným nástrojom na uskutočňovanie celej škály ľudských práv*." Médiá túto správu interpretovali tak, že spravodajca vyhlásil samotný prístup na internet za ľudské právo. Rada OSN pre ľudské práva na valnom zhromaždení vzala túto správu na vedomie a rezolúciou[15] potvrdila, že práva, zvlášť právo slobody prejavu, ktoré majú ľudia offline, musia byť rovnako chránené online. Štáty vyzvala na podporovanie a uľahčovanie prístupu na internet. O prístupe na internet ako o ľudskom práve však nehovorí.

Právo prístupu na internet uznávajú rôzne súkromné deklarácie a nezáväzné akty. Internet Rights and Principles, koalícia jednotlivcov a organizácií, pripravuje Chartu ľudských práv a princípov na internete.[16] V článku 1 uvádza: *„Každý má právo na prístup a využívanie Internetu*." Kódex EÚ práv v online prostredí,[17] ktorý je kompiláciou základného súboru práv ukotvených v právnych predpisoch EÚ, uvádza, že: *„Všetci v EÚ musia mať možnosť prístupu k minimálnemu súboru služieb elektronických komunikácií dobrej kvality za finančne dostupnú cenu*."

---

8 Grécka ústava v anglickom preklade, dostupná online: http://www.nis.gr/npimages/docs/Constitution_EN.pdf.

9 Ibid 7 s. 15.

10 Central American Free Trade Agreement.

11 GUADAMUZ, A.: Costa Rican court declares the Internet as a fundamental right. Dostupné na: http://www.technollama.co.uk/costa-rican-court-declares-the-internet-as-a-fundamental-right.

12 DE HERT, P., KLOZA, D.: Internet (access) as a new fundamental right. Inflating the current rights framework?, in: European Journal of Law and Technology, Vol. 3. No. 3, 2012.

13 PENNEY, J.W.: Internet Access Rights: A Brief History and Intellectual Origins (September 1, 2011), in: William Mitchell Law Review, Vol. 38, No. 1, p. 14, 2011.

14 UN Human Rights Council: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. p. 22.

15 UN Human Rights Council, Resolution L13 – The Promotion, Protection and Enjoyment of Human Rights on the Internet – adopted by consensus on by the Human Rights Council (29. júl 2012).

16 Internet Rights.

17 Európska komisia: Kódex EÚ práv v online prostredí. Luxemburg: Úrad pre vydávanie publikácií Európskej únie. 2012. ISBN 978-92-79-26535-8.

2. Argumenty proti vyhláseniu práva na prístup na internet za ľudské právo

Vinton Cerf, tvorca TCP/IP protokolu, odmieta predstavu, že internet je ľudským právom. Tvrdí, že *„technológia umožňuje výkon práv ale nie je právom samotným.“*[18] Podľa Cerfa právo na internet nie je tak zvnútornené ako ľudské práva. Tie musia byť zaručené, aby sme mohli žiť zdravý a plnohodnotný život, ako napr. zákaz mučenia alebo sloboda svedomia. Internet je hodnotný len ako prostriedok na dosiahnutie účelu, nie účel samotný. *„Ak ste kedysi nemali koňa, bolo ťažké sa uživiť. Dôležité však bolo právo na živobytie, nie právo mať koňa. Ak by sme mali garantované právo na koňa, dnes by som nevedel, čo s ním*,“ píše Cerf.[19] Aj samotná správa OSN hovorí o internete ako o prostriedku,[20] nie o cieli samotnom. Rovnako ako telefón alebo cesta je internet len nástroj na dosiahnutie niečoho iného. Rozmieňaním ľudských práv na drobné môžeme dospieť až k „právu na koňa.“ Podobným príkladom je lobovanie leteckých spoločností, hotelov a cestovných kancelárií v OSN za vyhlásenie ľudského práva na turizmus.[21]

Predtým než možno bude právo na prístup na internet uznané za nové ľudské právo, je potrebné preskúmať, či už nie je chránené a ak áno, ako. Všeobecná deklarácia ľudských práv (čl. 19) obsahuje *„právo vyhľadávať, prijímať a rozširovať informácie a myšlienky akýmikoľvek prostriedkami a bez ohľadu na hranice*.“ Medzinárodný pakt o občianskych a politických právach (čl. 19) stanovuje, že: *„Každý má právo na slobodu prejavu; toto právo zahŕňa slobodu vyhľadávať, prijímať a rozširovať informácie a myšlienky každého druhu, bez ohľadu na hranice, či už ústne, písomne alebo tlačou, prostredníctvom umenia alebo akýmikoľvek inými prostriedkami podľa vlastnej voľby*.“ Obdobne Dohovor o ochrane ľudských práv a základných slobôd (čl. 10) uvádza, že *„Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice.“*

Všeobecná deklarácia a Medzinárodný pakt o občianskych a politických právach chránia spôsob komunikácie *„akýmikoľvek prostriedkami“ a* “*ústne, písomne alebo tlačou, prostredníctvom umenia alebo akýmikoľvek inými prostriedkami podľa vlastnej voľby*.“ Môžu preto zahrnúť aj nové technologické spôsoby komunikovania. Charta základných práv EÚ (čl. 11) a Dohovor o ochrane ľudských právach sa k spôsobu komunikácie nevyjadrujú, neobsahujú frázu „cez akékoľvek médium.“ Napriek tomu sa informácie prenášané cez internet nelíšia od iných foriem vyjadrenia, preto možno uzavrieť, že sloboda prejavu na internete je chránená aj týmito prameňmi práva.

3. Vyvažovanie práv v prostredí internetu

V súčasnosti sme v prostredí internetu svedkami vyvažovania dvoch základných práv, a to slobody slova a majetkových autorských práv. Odpájanie užívateľov od internetu po porušení práv duševného vlastníctva je založené na systéme „postupnej odpovede,“[22] kde poslednou „odpoveďou“ je prerušenie pripojenia. Takýto zákon zatiaľ prijalo Francúzsko a Veľká Británia.[23] V iných krajinách (Austrália, Nemecko, Holandsko, Nový Zéland, Južná

---

18 CERF V.: Internet Access Is Not a Human Right, New York Times, 4 January 2012, http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

19 CERF V.: Internet Access Is Not a Human Right, New York Times, 4 January 2012, http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html.

20 „Internet sa stal kľúčovým prostriedkom umožňujúcim vykonávanie slobody slova.“ p. 7.

21 BAXI, U.: Voices of Suffering and the Future of Human Rights. Transnational Law and Contemporary Problems, University of Iowa.

22 graduate response.

23 Digital Economy Act 2010.

Kórea, Švédsko) bol systém postupnej odpovede navrhovaný, ale nebol prijatý.[24] Možnosť odpojenia používateľov obsahoval aj pôvodný text Obchodnej dohody proti falšovaniu.[25]

3.1. Právo na spravodlivý proces v. právo na ochranu duševného vlastníctva

Francúzsky zákon z roku 2009[26] umožnil monitorovanie používania internetu s cieľom odhaliť ilegálne kopírovanie autorských diel. Zákon zriadil administratívny orgán s názvom „Vysoký úrad pre šírenie diel a ochranu práv na internete",[27] ktorého právomocou je monitorovať internet a odhaľovať tých, ktorý nelegálne sťahujú. Vysoký úrad môže vykonať nasledujúce postupné intervencie. Najprv zašle užívateľovi prostredníctvom jeho poskytovateľa internetu varovné e-maily. Prvý e-mail používateľa upozorní, že jeho internetové pripojenie bolo použité na sťahovanie nelegálneho obsahu. Ak Úrad zistí, že počas šiestich mesiacov používateľ v takomto konaní pokračuje, zašle druhý e-mail. Ak údajné porušovanie autorských práv pokračuje aj naďalej, Vysoký úrad mal v pôvodnej podobe zákona právomoc zablokovať internetové pripojenie používateľa na dva mesiace až rok, čím zákon vytvoril novú *„takmerpolicajnú autoritu, ktorá monitorovaním porušuje právo na súkromie a občianske slobody v elektronickej komunikácii*." [28]

Ústavná rada[29] časti zákona vyhlásila za protiústavné, ale v zmenenej podobe je zákon platný dodnes. Ústavná rada pri hodnotení ústavnosti zákona odhalila nasledujúce nedostatky. Po prvé, rozhodnutie prerušiť internetové pripojenie má byť v právomoci súdov, nie administratívnych orgánov. Iba sudca môže nariadiť prerušenie prístupu na internetové služby, keďže *právo slobody slova zahŕňa právo prístupu k týmto službám*.[30] Pôvodná verzia zákona zverila súdnu právomoc administratívnemu orgánu, ktorý v prípade „zjavného" porušenia autorských práv mohol prerušiť internetové pripojenie používateľa bez uplatnenia procesných princípov, ako je právo na spravodlivý proces, právo na obhajobu a prezumpcia neviny. Po druhé, legislatíva musí brať do úvahy, že *sloboda slova a komunikácie sú predpokladmi demokracie a akékoľvek obmedzenia preto musia byť nevyhnutné, efektívne a proporcionálne vzhľadom na svoj cieľ*.[31] Rozhodnutie Ústavnej rady treba vnímať tak, že prístup na internet nevyhlásila za základné právo, ale slobode komunikácie, ktorá už teraz má status chráneného práva, priznala zosilnenú ochranu v súvislosti s prístupom na internet.[32]

Treba si tiež uvedomiť, že porušenie autorského práva je pripísané osobe, ktorá uzavrela zmluvu s poskytovateľom pripojenia, nie skutočnému porušiteľovi autorského práva. Základom pre zaslanie upozorňujúcich e-mailov osobe, ktorá uzavrela zmluvu o poskytnutí pripojenia, bolo nové ustanovenie v Zákone o duševnom vlastníctve.[33] Článok jej určil zá-

---

24 LUCCHI, N.: Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression (February 6, 2011). Cardozo Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011. str. 654.

25 Anti-Counterfeiting Trade Agreement (ACTA).

26 Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

27 Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet.

28 LUCCHI, N.: Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression (February 6, 2011). Cardozo Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011. str. 659.

29 Conseil constitutionnel (Ústavná rada), rozhodnutie číslo 2009-580DC, z 10. júna 2009.

30 Ibid., článok 12.

31 Ibid., článok 15.

32 LUCCHI, N.: The Role of Internet Access in Enabling Individual's Rights and Freedom. p 13.

33 Art. L.336-3 Code de la Propriété Intellectuelle.

konnú povinnosť zabezpečiť, aby jej internetové pripojenie nebolo použité na rozmnožovanie, sprístupňovanie, zverejňovanie chránených diel verejnosti. Porušenie tejto novej „dohliadajúcej" povinnosti umožnilo zaslanie varovných e-mailov aj v prípade, že osoba, ktorá zmluvu o pripojení uzavrela, nie je priamo zodpovedná za porušovanie autorských práv (napr. univerzita).[34] Podľa Ústavnej rady zákon preniesol dôkazné bremeno na osobu, ktorá uzavrela zmluvu o pripojení, keďže ona bude musieť dokazovať, že k porušeniu došlo treťou osobou. Zákon u osoby, ktorá uzavrela zmluvu, zaviedol prezumpciu viny.[35] Pôvodný zákon neposkytoval možnosť podať námietky proti rozhodnutiu Úradu. Odvolanie bolo prípustné až po uložení sankcie.[36] Podľa súčasnej podoby zákona dostane užívateľ varovné e-maily, po ktorých nasleduje zrýchlené súdne konanie. Udeliť finančnú sankciu, ale aj odpojenie od internetu môže za súčasného stavu len súd.

4. Právo na slobodu podnikania v. právo na ochranu duševného vlastníctva

V iných krajinách (Belgicko, Írsko), ktoré nezaviedli systém postupnej odpovede, sa držitelia autorských práv v snahe vymôcť svoje práva online pokúšajú preniesť viac povinností na poskytovateľov internetového pripojenia. Jednej z týchto navrhovaných povinností, preventívnemu filtrovaniu obsahu, sa venoval Súdny dvor Európskej únie v konaniach Scarlet proti Sabam[37] a Sabam proti Netlog.[38] Prejudiciálna otázka znela, či vnútroštátny súd môže vydať súdny príkaz, ktorým by poskytovateľovi hostingových služieb (v tomto prípade prevádzkovateľovi internetovej sociálnej siete) uložil povinnosť zaviesť systém filtrovania informácií ukladaných na jeho serveroch používateľmi s cieľom predísť porušovaniu autorských práv.

Belgický zväz kolektívnej správy práv Sabam žiadal od spoločnosti Netlog, ktorá prevádzkuje sociálnu sieť, prostredníctvom ktorej používatelia tvoria a napĺňajú svoje osobné stránky, aby upustila od „*nepovoleného sprístupňovania hudobných audiovizuálnych diel na profiloch jej používateľov*".[39] Podľa Netlog by vyhovenie žalobe znamenalo, že jej bude uložená všeobecná monitorovacia povinnosť, ktorú vylučuje smernica o elektronickom obchode.[40] Spoločnosť poskytujúca hostingové služby patrí medzi poskytovateľov služieb informačnej spoločnosti (ISP),[41] ktorí nie sú povinní sledovať prenášané údaje a ani nezodpovedajú za informácie nahraté používateľmi služieb, ak sa o protiprávnom obsahu nedozvedia.

Súdny dvor skúmal, či požiadavka monitorovania komunikácie ISP je v súlade so základnými právami EÚ. Súd uznal, že ochrana duševného vlastníctva je základným právom,[42] no nie je právom absolútnym. Musí byť v rovnováhe s ochranou osobných údajov,[43] slobodou

---

34 STROWELL, A.: Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the "Graduated Response" a Good Reply? in: The WIPO Journal. 2009. Issue no1. p. 80.

35 Conseil constitutionnel (Ústavná rada), rozhodnutie číslo 2009-580DC z 10. júna 2009, článok 18.

36 LUCCHI, N., Access to Network Services and Protection of Constitutional Rights:. str. 660.

37 Rozhodnutie C-70/10 Scarlet Extended v Societe Belge des auteurs, compositeurs et editeurs (SABAM).

38 Rozhodnutie C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM)/ v Netlog NV.

39 Tlačové komuniké Súdneho dvora Európskej únie č. 11/12.

40 Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. 6. 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode, článok 15.

41 Information service provider.

42 Obsiahnutým v článku 17(2) Charty základných práv Európskej únie.

43 Článok 8 Charty základných práv Európskej únie.

prejavu a právom na informácie[44] a taktiež lobodou podnikania[45] ISP. Navrhovaný systém filtrovania by pre spoločnosť Netlog znamenal povinnosť skúmať všetky dáta uložené používateľmi na jeho serveroch a blokovať tie súbory, ktoré považuje za protiprávne. Filtrovanie by sa preventívne týkalo všetkých používateľov služby a prebiehalo neohraničenú dobu na náklady samotnej spoločnosti. Povinnosť inštalovať komplikovaný, nákladný a trvalý systém na vlastné náklady by podľa súdu porušil slobodu podnikania. Súdny príkaz by ďalej mohol ohroziť slobodu informácií, keďže systém by mohol nedostatočne rozlišovať medzi právnym a protiprávnym obsahom, čo by mohlo vyústiť do blokovania komunikácie neodporujúcej právu. V súvislosti s ochranou osobných údajov používateľov, súd odkázal na predchádzajúce rozhodnutie vo veci Promusicae.[46] V dôsledku toho Súdny dvor rozhodol, že vnútroštátny súd by vydaním súdneho príkazu, ktorým sa poskytovateľovi hostingových služieb ukladá povinnosť zaviesť takýto systém filtrovania, nerešpektoval požiadavku zabezpečiť náležitú rovnováhu medzi právom duševného vlastníctva na jednej strane a slobodou podnikania, právom na ochranu osobných údajov a slobodou prijímať a rozširovať informácie na druhej strane.[47] Rozhodnutie však neznamená úplné odmietnutie monitorovacích systémov slúžiacich na ochranu autorskoprávne chránených diel. Možno ich pripustiť, ak by dodržali podmienky v tomto rozhodnutí – proporcionalitu, vyváženie práv všetkých zúčastnených strán, prípadne zdieľanie nákladov slúžiacich na prevádzku takého systému.[48]

Belgická organizácia kolektívnej správy práv Sabam prednedávnom zvolila iný prístup, ako nahradiť unikajúce odmeny za diela na internete. Zažalovala troch najväčších poskytovateľov internetu v krajine s návrhom, aby platili autorskoprávne odmeny za samotné poskytovanie prístupu k autorských dielam online. Sabam žiada časť zisku ISP ako autorskú náhradu, ktorú ISP získavajú za poskytovanie internetového pripojenia umožňujúceho prístup k dielam.[49]

5. Právo na slobodu slova v. právo na ochranu duševného vlastníctva

Autorské práva nemusia vždy ustúpiť slobode prejavu. Jednotlivé štáty majú pomerne široké možnosti ich vzájomného vyvažovania, keďže žiaden súd či zákon nestanovil jednoznačné kritériá, ako postupovať pri ich strete. Viac jasnosti do problematiky prinesú až nové rozhodnutia, ak poskytnú všeobecnejší návod, nielen posúdenie veci v jednotlivom prípade. Jedným z posledných stretov týchto dvoch práv sa zaoberal Európsky súd pre ľudské práva, keď rozhodoval o sťažnosti dvoch zakladateľov najväčšej stránky na zdieľanie súborov The Pirate Bay, ktorí boli švédskym súdom uznaní vinnými za porušovanie práv duševného vlastníctva. [50]

---

44 Článok 11 Charty základných práv Európskej únie.

45 Článok 16 Charty základných práv Európskej únie.

46 Rozhodnutie Súdneho dvora EÚ vo veci Productores de Música de España (Promusicae) v Telefónica de España SAU. (C-275/06).

47 Tlačové komuniké Súdneho dvora Európskej únie č. 11/12.

48 DALY, A., FARRAND, B.: Scarlet v SABAM: Evidence of an Emerging Backlash Against Corporate Copyrights Lobbies in Europe? (May 14, 2012).

49 ESSERS, L.: Belgian ISPs sued for providing Internet access without paying copyright levies, PCWorld, 1 May 2013, Dostupné na: http://www.pcworld.com/article/2036961/belgian-isps-sued-for-providing-internet-access-without-paying-copyright-levies.html.

50 Rozhodnutie Európskeho súdu pre ľudské práva z 19 februára 2013. Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden, Appl. nr. 40397/12.

Zakladatelia The Pirate Bay boli stíhaní a v rovnakom konaní žalovaní nahrávacími spoločnosťami a inými držiteľmi autorských práv za porušovanie autorského práva. Súd ich odsúdil za spravovanie stránky, ktorá umožňovala používateľom zdieľať digitálne autorské diela na ročný trest odňatia slobody a náhradu škody vo výške 3,3 milióna eur. Odvolací súd verdikt potvrdil, ale znížil ich trest. Najvyšší súd Švédska ich sťažnosť odmietol. Na Európskom súde pre ľudské práva namietali porušenie práva slobody prejavu,[51] ale súd ich žiadosť odmietol ako neprípustnú. Sudcovia skúmali splnenie podmienok umožňujúcich obmedzenie slobody prejavu, ako sú stanovené v článku 10 ods. 2 Európskeho dohovoru o ľudských právach, a to, či bolo (a) obmedzené ich právo na slobodu prejavu, (b) či obmedzenie bolo predpísané zákonom, (c) či existoval legitímny cieľ obmedzenia, (d) či obmedzenie bolo nevyhnutné v demokratickej spoločnosti.[52]

Je dôležité si uvedomiť, že stránka umožňujúca zdieľanie súborov je podľa súdu chránená slobodou prejavu podľa článku 10 ods. 1 Dohovoru. Súd zdôraznil, že článok 10 *garantuje právo poskytovať informácie a právo verejnosti prijímať ich*. Preto následné odsúdenie administrátorov stránky obmedzilo ich právo slobody prejavu. Nebolo však pochýb, že toto obmedzenie bolo predpísané švédskym autorským a trestným zákonom. Podľa súdu bolo obmedzenie tiež v súlade s cieľom „ochrany práv iných" a „predchádzania zločinnosti" a tiež „nevyhnutné v demokratickej spoločnosti[53]" podľa článku 10 ods. 2.[54] Európsky dohovor nebol porušený, keďže boli splnené podmienky umožňujúce obmedzenie slobody prejavu.

Podľa súdu je pri posudzovaní obmedzenia slobody prejavu potrebné skúmať aj povahu a prísnosť uložených sankcií. V tomto prípade trest odňatia slobody a odškodnenie nemožno považovať za disproporčné. Pred švédskymi súdmi bolo preukázané, že navrhovatelia nevykonali žiadne opatrenia na odstránenie predmetných súborov typu torrent napriek tomu, že o to boli žiadaní.[55]

6. Obmedzenie práva slobody slova blokovaním webových stránok

Popri súkromnej cenzúre ako v prípade Sabam proti Netlog chránia súdy prístup na internet aj pred obmedzeniami zo strany štátu. Reštrikcie práva na slobodu slova na internete majú viacero podôb, a to od technických možností brániacich v prístupe k určitému obsahu ako blokovanie a filtrovanie po nedostatočné garancie práva na súkromie a ochranu osobných údajov, ktoré brzdia šírenie informácií a názorov.[56]

---

51 Podľa článku 10 Európskeho dohovoru o ľudských právach.

52 LAMBERT, J.: Sunk! The Court of Human Rights rejects the Pirate Bay's Complaint. Dostupné na: http://nipclaw.blogspot.co.uk/2013/03/sunk-court-of-human-rights-rejects.html?goback=%2Egna_995887%2Egde_995887_member_222685089.

53 Viac k tejto podmienke pozri rozhodnutie The Observer and The Guardian v. United Kingdom. no. 13585/88.

54 Výkon slobody prejavu môže podliehať takým... obmedzeniam, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti... *na predchádzanie zločinnosti,... ochranu povesti alebo práv iných*...

55 Ak ISP odmietne odstrániť súbory na žiadosť držiteľa autorských práv vstupuje sám do zodpovednostného vzťahu. Viac POLČÁK, R.: *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007.

56 UN Human Rights Council, Report…Ibid. p 9.

V rozhodnutí Ahmet Yıldırım proti Turecku sa Európsky súd pre ľudské práva zastal práva jednotlivca na prístup k internetu ako nástroju na uplatňovanie slobody prejavu.[57] Navrhovateľom bol turecký občan Ahmet Yıldırım, ktorý spravuje svoju webovú stránku umiestnenú na portáli Google Sites. Yıldırım na stránke publikoval vlastné akademické články a jeho názory a komentáre k rôznym témam.[58] Trestný súd v Denizli nariadil blokovanie prístupu k inej stránke, taktiež „hostovanej" v službe Google site, ktorá urážala pamiatku Atatürka, zakladateľa a prvého prezidenta Tureckej republiky, čím stránka porušovala turecké právo. Služba Google Sites ani Yıldırımova osobná webstránka neboli týmto konaním nijak dotknutí. Turecká telekomunikačná autorita spravujúca elektronické dáta, ktorá mala za úlohu zablokovať stránku haniacu Atatürka, požiadala trestný súd o povolenie blokovať celú službu sites.google.com z technických dôvodov. Súd žiadosť povolil. Yıldırım nemal žiadnu možnosť obnoviť prístup k svojej osobnej stránke, namietal preto porušenie článku 10 Európskeho dohovoru, pretože opatrenie v trestnom konaní, ktoré s ním nijak nesúviselo, porušilo jeho právo na slobodu slova.

Európsky súd pre ľudské práva dospel k názoru, že hromadné zablokovanie prístupu k sites.google.com bolo porušením Yıldırımovho práva na slobodu slova z nasledujúcich dôvodov. Sloboda prejavu nie je absolútnym právom.[59] Pripúšťa uloženie obmedzení, ak sú splnené určité podmienky. Obmedzenia slobody prejavu musia byť stanovené zákonom, čo znamená, že musia byť formulované s dostatočnou presnosťou umožňujúcou jednotlivcom regulovať svoje konanie. Obmedzenie slobody slova musí byť ďalej „nevyhnutné v demokratickej spoločnosti."[60] Turecké právo neumožňovalo príslušnému orgánu hromadné blokovanie celej platformy ako Google Sites. Zákon taktiež nedostatočne zabezpečil ochranu pred potenciálnym zneužitím. Ďalej nebolo preukázané, že Google Sites bola upovedomená o tom, že sa na jej serveri nachádza obsah porušujúci zákon, alebo že by odmietla súčinnosť s vykonaním opatrení týkajúcich sa stránky, ktorá bola predmetom trestného konania.[61]

Rozhodnutie Ahmet Yıldırım proti Turecku nám ukazuje, že súdy musia byť opatrené pri určovaní rozsahu blokovania a musí byť zabezpečený súdny prieskum rozhodnutia slúžiaci na ochranu pred zneužitím. Inak môže blokovanie webových stránok porušiť princíp proporcionality práv a podmienky, že obmedzenie práv musí byť „predpísané zákonom."[62]

Záver

Ak hovoríme o práve prístupu na internet, musíme si ujasniť, čo máme na mysli. Rozlíšiť môžeme dve dimenzie: (a) prístup k technickej infraštruktúre nutnej na samotné pripojenie a (b) prístup k digitálnemu obsahu. (a) Ešte stále existujú krajiny s penetráciou[63] internetu menej než 5%. Právom na prístup do informačnej siete sa v tejto súvislosti myslí snaha znížiť „digitálnu priepasť" v geografickom a sociálnom zmysle. K iniciatíve sprístupne-

---

57 Rozhodnutie Európskeho súdu pre ľudské práva Ahmet Yildirim v. Turkey, nr. 3111/10 z 18. decembra 2012.

58 http://www.article19.org/resources.php/resource/3567/en/turkey:-landmark-european-court-decision-finds-blanket-google-ban-was-a-violation-of-freedom-of-expression.

59 Napr. zákaz mučenia.

60 Európsky dohovor o ľudských právach, článok 10 ods. 2.

61 GÜRKAYNAK, G., DURLU, D.: Access Denied. Commercial Dispute Resolution. March - April 2013 Global Legal Group Ltd, London.

62 HUSOVEC, M.: *What's Wrong With UK Website Blocking Injunctions?* Dostupné na http://www.husovec.eu/2013_03_01_archive.html.

63 www.internetworldstats.com.

nia internetu rozvojovým krajinám vyzývajú napr. Miléniové rozvojové ciele OSN.[64] (b) Právo na prístup k digitálnemu obsahu je potrebné chrániť pred obmedzovaním zo strany štátu (blokovanie aktivistov za demokraciu, politických disidentov, občianskych žurnalistov) i pred súkromnou cenzúrou (držiteľov autorských práv). Obmedzenia prístupu k obsahu sa môžu týkať len úzkeho okruhu prípadov: detskej pornografie, neznášanlivých prejavov, podpory a propagácie genocídia, podnecovanie k národnostnej, rasovej a náboženskej nenávisti smerujúce k diskriminácii, nenávisti alebo násiliu.[65] Blokovanie prístupu však musí spĺňať podmienky podľa medzinárodných dohovorov o ľudských právach.

---

[64] Vychádzajú z tzv. Miléniovej deklarácie, ktorá bola podpísaná v septembri roku 2000 na Miléniovom summite. Jej podpis je výsledkom boja proti chudobe a nadväzuje na predchádzajúce rezolúcie a dohody OSN. Cieľ 8F znie: „V spolupráci so súkromným sektorom sprístupniť výhody nových technológií, obzvlášť informačno-komunikačných technológií."

[65] UN Human Rights Council, Report…, Ibid. p 8.

Medzinárodná úprava ochrany osobných údajov na internete a *safe harbors* v medzinárodných vzťahoch

Peter Bobčík

Úvod

Podľa Arthura Millera je súkromie pojem *„vágny a nestály*", pričom Judith Jarvis Thomson dodáva *„najzaujímavejšou vecou na súkromí je to, že nikto nemá príliš presnú predstavu, čo to vlastne je.*"[1] Napriek tomu sú osobné údaje internetových účtov, správy a e-maily nepochybne zložkami, ktoré spoločnosť považuje za súčasť súkromia.

V diskusiách na tému či vládny dohľad nad súkromím jeho občanov a *data mining* predstavuje hrozbu, často odznieva argument, že *„nie je čo skrývať"*, ktorý sa stal postupom času veľmi populárny hlavne v Spojenom kráľovstve, kde vláda inštalovala milióny kamier, cez ktoré úrady vykonávajú sledovanie verejnosti, pričom slogan programu bol *„ak nemáte čo skrývať, nemáte sa čoho báť."*[2] Varianty týchto vyhlásení sa často objavujú na blogoch a internetových fórach, z úst zástancov monitorovania osobných údajov. V nekonečných debatách je úsmevný výrok *„nemám čo skrývať, avšak nemám chuť nič odhaľovať*".

Napriek nechuti občanov zo zberu osobných údajov štátom (alebo rôznymi organizáciami) môžeme konštatovať, že sa transfer osobných informácií stal v určitých prípadoch nevyhnutným pre rozvoj obchodu, prípadne zabezpečenia verejných hodnôt. Cieľom mojej práce je spracovať práve medzinárodnú a vnútroštátnu právnu úpravu k uvedenej problematike, ktorá sa preniesla do ich legislatívy, a uviesť koncepcie ochrany citlivých dát a manipulácie s nimi, s prevažným zameraním na Európsko - Americký vzťah a jeho unikátny prvok tzv. *safe harbors* z pohľadu medzinárodného práva.

1. Ochrana osobných údajov v Európskej únie a tretích strán

Regulácia cezhraničných prenosov dát sa vyvíjala v rôznych krajinách s ohľadom na ich kultúrny základ rôzne. V niektorých regiónoch sa chápe ochrana osobných údajov ako ľudské právo, zatiaľčo iné legislatívy to nemusia rešpektovať[3] – v celom dokumente *APEC Privacy Framework*,[4] ktorej cieľom je spracovať benefity elektronického obchodu (inštitúcia združuje ekonomiky v Ázijsko-Pacifickom regióne) neboli vôbec použité pojmy základné/ľudské právo v kontexte ochrany osobných údajov.

---

1 THOMSON J. J.: The right to Privacy, in Philospophical Dimensions of Privacy: An anthology (Ferdinand David Schoemaned. 1984), [online] Dostupné na: http://books.google.sk/books?id=q_FrmXyl3hUC&pg=PA314&lpg=PA314&dq=Judith+Jarvis+Thomson+The+right+to+Privacy,+in+Philosophical+Dimensions+of+Privacy&source=bl&ots=HYeTYaE8Q6&sig=dgOudCXey8Igm7K4x-jW8_zOwHE&hl=sk&sa=X&ei=mZSCUa2FM-mu4QT3j4DoCg&ved=0CDcQ6AEwAA#v=onepage&q=Judith%20Jarvis%20Thomson%20The%20right%20to%20Privacy%2C%20in%20Philosophical%20Dimensions%20of%20Privacy&f=false.

2 ROSEN J.:The naked Crowd: Reclaiming Security and Freedom in an anxious Age, (2004), ISBN-10: 0375759859.

3 Jedná sa však skôr o faktický stav, keďže vo väčšine štátov nájdeme právo na súkromie zakotvené už v ústavách (resp. prameňoch práva obdobnej právnej sily), pozri GILC (Global Internet Liberty Campaign) Privacy and Human Rights: An International Survey of Privacy Laws and Practice [online] Dostupné na: http://gilc.org/privacy/survey/intro.html.

4 APEC Secretariat: APEC Privacy framerwork [online] Dostupné na: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

Pred koncom deväťdesiatych rokov, existovalo len niekoľko systémov komplexne regulujúcich ochranu osobných údajov, ktoré však mali skôr lokálny charakter[5] postupom času však toto odvetvie začalo naberať medzinárodný rozmer a to z dôvodov exteritoriálneho dosahu, prenosu dát s povahou priemyselného vlastníctva, sankcií, ktoré môžu dosahovať milióny eur a (negatívnej) publicity v prípade odhalenia zneužitie informácií o jednotlivcoch.

1.1. Prístup Európskej únie k ochrane osobných údajov

Niektoré štáty pôvodných Európskych spoločenstiev(napr. Nemecko, Rakúsko)[6] a neskôr krajiny „východného bloku," ktoré pristúpili k Európskej únií sú poznačené ideologickou minulosťou, kde utajené policajné zložky zneužívali osobné informácie občanov, čo sa premietlo do všeobecného odporu obyvateľstva k zákonom zasahujúcim do súkromia a konzervatívnejšiemu prístupu pri prijímaní legislatívy.

Ochranu obyvateľstva pred zneužitím osobných údajov sa kvôli uvedenému cíteniu voličov prejavila vo vlastnej legislatíve Nemecka a Francúzska,[7] ktoré prijali vlastné zákony na ochranu osobných údajov

Snaha o harmonizáciu ochrany osobných údajov v európskych spoločenstvách začala, keď OECD v roku 1980 vyhlásila „Odporúčanie Rady o všeobecných zásadách, ktorými sa riadi ochrana osobných údajov a cezhraničné toky osobných dát,"[8] ktorá však nepriniesla požadovaný výsledok a ochrana osobných údajov sa krajinách európskych spoločenstiev po dlhý čas zásadne líšila.

V roku 1995 vstúpila do platnosti „Smernica na ochranu jednotlivcov pri spracovaní osobných údajov a voľnom pohybe týchto dát",[9] ktorá prikazovala členským štátom, aby do roku 1998 prijali zákon na ochranu dát, ktorý by sa týkal súkromného a verejného sektoru. Smernica sa vzťahuje nielen na elektronické dáta, ale na dáta vo všeobecnosti (menej jasnými príkladmi osobných údajov je aj IP adresa, číslo kreditnej karty, odtlačky prstov),[10]

---

5 DOWLING D. C, Jr.: International Data protection and Privacy Law [online] Dostupné na: http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.

6 Nemecko je z globálneho hľadiska jedným z najprísnejších (ak nie najprísnejším) ochrancom osobných údajov. Prvý zákon týkajúci sa ochrany osobných údajov bol prijatý už v roku 1970 v spolkovej krajine Hessen. V tomto ohľade treba spomenúť, že každá zo spolkových krajín má vlastnú právnu úpravu, ktorá však musí spĺňať podmienky federálnej legislatívy. Komplexná revízia právnej úpravy nastala v roku 2001 pri harmonizácií zákonov so smernicou Komisie o ochrane osobných údajov. PRIVACY INTERNATIONAL: Constitutional Privacy and Data Protection Framework [online] Dostupné na: https://www.privacyinternational.org/reports/germany/i-legal-framework.

7 Začiatky ochrany osobných údajov v širšom zmysle nájdeme vo Francúzsku už v roku 1858. Pozri GILC: Privacy and Human Rights [online] Dostupné na: http://gilc.org/privacy/survey/intro.html.

8 OECD Council, Sept. 23, 1980, [online] Dostupné na: www.giodo.gov.pl/plik/id_p/179/j/en/.

9 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [online] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

10 Digitale Gesellschaft, Germany An introduction to data protection, EDRI papers, issue 06,[online] Dostupné na: http://www.edri.org/files/paper06_datap.pdf.

čo viedlo ku kontrole písaných textov, internetu a aj ústnych rozhovorov[11] (a teda je možné ju aplikovať aj pri kontrole banálnych milostných dopisov). Táto smernica zohráva rozhodujúcu úlohu pri koncipovaní politiky Európskej únie vo vzťahu k ochrane osobných údajov. Smernica vytvorila vlastný zoznam pojmov, ktorý je nevyhnutný pri výklade európskeho konceptu ochrany dát.

Osobnými údajmi sa myslí každá informácia o identifikovanej, alebo identifikovateľnej osobe – teda *„fyzická osoba, ktorá môže byť priamo, alebo nepriamo identifikovaná podľa identifikačného čísla, alebo iných špecifických faktorov vzťahujúcich sa na jeho fyzickú, psycholigickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu".*[12] Zo znenia predpisu je očividné, že plne anonymizovaný zoznam (teda bez uvedenia identifikačného čísla a mena/iných jedinečných údajov) môže obísť smernicu.

– „správca" je každý, kto určuje účely a prostriedky spracovania osobných údajov.

– „spracovávateľ" je každý, kto spracováva osobné údaje

– „treťou stranou" je každý, kto spracováva dáta pod kontrolou správcu, alebo spracovávateľa.

V zmysle takto široko koncipovaných definícií, smernica extenzívne zasahuje do nakladania s osobnými údajmi občanov členskými štátmi s cieľom ochrany ľudských práv a základných slobôd so zameraním na spracovávanie osobných dát. Takáto legislatíva viedla k spoločným pravidlám a zásadám pri uvedených činnostiach, ako sú

1. *„spravodlivosť pri spracovávaní dát;*[13]
2. *Spracovávanie dát sa môže diať iba so špecifickým (a legitímnym) zámerom;*
3. *iba primerané a relevantné dáta sú predmetom zbierania a nesmú presahovať účel zbierania;*
4. *dáta musia byť presné a aktuálne, aby sa predišlo chybám;*
5. *dáta, ktoré sa už ďalej nemajú význam na aký boli zozbierané musia byť zničené;*
6. *správca dát musí zabezpečiť primerané organizačné a technické prostriedky na ochranu osobných údajov*
7. *automatické vyhodnocovanie údajov je zakázané".*

Tieto zásady nemusia byť naplnené kumulatívne. V zmysle legislatívy európskej únie však ani takáto ochrana nie je dostatočná a osobné údaje sa ďalej rozlišujú na *„citlivé informácie*" - teda údaje týkajúce sa *„rasy, alebo etnického pôvody, politických názorov, náboženstva a filozofických názorov, ...zdravia, alebo sexuálneho života*", ktorých spracovávanie je zakázané pokiaľ na to nebol daný výslovný súhlas. Napriek zjavnej tvrdosti týchto noriem si členské štáty európskej únie ponechali právo na kontrolu týchto

---

[11] DOWLING D. C, Jr.: International Data protection and Privacy Law [online] Dostupné na: http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.

[12] 95/46/ECch.I., art2 (a), [online] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[13] Smernica zakazuje zbieranie a spracovávanie osobných údajov, pokiaľ to nie je spravodlivo a zákonným spôsobom. Pozri: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [online] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

údajov v záujme národnej bezpečnosti, vyšetrovania trestnej činnosti, ďalšie výnimky sa vzťahujú na historické, štatistické alebo vedecké informácie."

Spracovávanie dát nesmie podľa legislatívy Európskej únie prebehnúť v tajnosti a subjekty, ktorých sa informácie týkajú majú právo zistiť, aké informácie boli o nich zozbierané a na čo sa použili, keď podľa znenia smernice jednotlivci ktorých dáta sú v procese zbierania musia byť upozornený na túto skutočnosť. Upozornenie pritom musí obsahovať prečo sú informácie získavané, kto ich zbiera a kto k nim má prístup. Spomenutá úprava, jej princípy a zásady sú náčrtom širokého koncipovania ochrany osobných údajov, ktoré poskytuje Európska únia v rámci harmonizácie zákonov jej členských štátov. Niektoré ustanovenia smernice sú aj vzhľadom k historickým tragédiám, ktoré sa v členských štátoch odohrali revolučným prístupom pri ochrane osobných údajov jednotlivcov v rámci únie.

S ohľadom na skutočnosť, že niektoré štáty, právnické osoby by sa mohli rozhodnúť presunúť dáta do iných krajín, aby obišli striktný režim európskeho práva, boli uvedené prísne normy na „vývoz" dát a sú známe prípady, keď interné informácie spoločnosti sídliacej v jednom z členských o jej zamestnancoch, ktoré boli prenesené do centrály v USA museli byť stále pod režimom princípov a zásad smernice.[14] „*Vývoz*" informácií je možný iba do krajín ktoré „*zabezpečia adekvátny stupeň ochrany (osobných údajov)*",[15] pričom výpočet štátov, ktoré disponujú týmto oprávnením je prekvapivo krátky: Švajčiarsko,[16] Argentína, Kanada, Guernsey(správna oblasť), Man (ostrov). Takéto uznanie Komisiou vedie k tomu, že *de facto* neexistuje rozdiel medzi prenosom informácií z Nemecka do Argentíny, ako z Nemecka na Slovensko. Môžeme konštatovať, že „okopírovanie" európskej legislatívy a získanie statusu „tretej krajiny" môže pomôcť obchodu do týchto neeurópskych krajín a stále je pre nich atraktívne. Následný prenos dát z tretích krajín do štátov, ktoré nemajú toto povolenie je ilegálne. Súčasný trend po politických snahách ale smeruje k benevolentnejšiemu výkladu legislatívy v prospech prenosu dát (hlavne do USA).

Právny stav a zjavná nezhoda pri riešení otázok ochrany osobných údajov a ich prenosu do iných štátov veľmi rýchlo priniesla rozpor medzi politikou Európskej únie a USA[17] (ktoré výhody začlenenia na zoznam krajín s adekvátnym stupňom ochrany osobných údajov nepovažovali za dostatočný vzhľadom k požadovanej zmene legislatívy), keďže sa ale jedná o strategických partnerov riešenie sa našlo v podobe tzv. *safe harbors*.

---

[14] DOWLING D. C, Jr.: International Data protection and Privacy Law [online] Dostupné na: http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf.

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 28, [online] Dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[16] Swiss Federal Act on Data Protection (FADP), pre ďalšie pozri. *Safe Harbor Framerwork*, [online] Dostupné na: http://export.gov/safeharbor/swiss/index.asp.

[17] Vyplýva to z benevoletnejšieho prístupu USA k ochrane osobných údajov. Do dnešného dňa USA neprijali právnu úpravu porovnateľnú so spomínanou smernicou EÚ. Ochrana osobných údajov je prijatá skôr na *ad hoc* princípe, napr. *Cable Television Protection and Competition Act* [online] Dostupné na: http://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1439.pdf.

2. *Safe harbors* – ako riešenie problému rozdielnych právnych úprav

Safe harbors sú jedinečný systém prenosu dát z Európskej únie (a členov EHS[18]) do USA, založený na certifikácií subjektov, ktoré sa zaviažu dodržiavať obmedzenia vzťahujúce sa na informácie (akoby sa stále nachádzali v Európskej únií) a následne môžu prenášať dáta z EU do USA (a naspäť).[19] Takéto inštitúcie sú teda chápané, ako štát s adekvátnym stupňom ochrany osobných údajov. Normy ochrany prenášaných údajov subjektov z USA pritom nemusia spĺňať podmienky ochrany podľa smernice EU – stačí, že spĺňajú podmienky dané legislatívou Spojených štátov. Okrem dodržiavania zásad daných smernicou EU a zákonmi USA musí *safe harbor* spĺňať ďalšie zásady:

1. zverejňovať zásady ochrany osobných údajov verejne;
2. prijať jurisdikciu *US Federal Trade Commission* (FTC);
3. upozorniť *US Department of Commerce* o certifikovaní sa.

Safe harbors taktiež musia spĺňať sedem princípov, ktoré sledujú rovnaké ciele, ako smernica EU.

1. **Upovedomenie** – subjekty z EU musia byť upovedemené a informované prečo ich údaje spracováva subjekt z USA a taktiež im musia byť oznámené ich práva obmedziť použitie a prenos ich dát, pričom sa tak musí spraviť presne, jasne a okamžite po požiadaní o predložení osobných údajov;

2. **Výber –** správca *safe harbor* musí dať subjektu európskych dát možnosť výnimky zverejnenia ich osobných údajov tretej strane, ale pre použitie na iné účely než boli údaje zozbierané;

3. **Ďalší prenos –** správca *safe harbor* ktorý chce preniesť osobné údaje tretej strane v USA alebo inde, musí overiť, že tretia strana súhlasila s princípmi *safe harbor*.

4. **Ochrana –** správca *safe harbor* musí zabezpečiť adekvátnu formu ochrany osobných údajov;

5. **Celistvosť dát –** rozsah zozbieraných informácií musí byť ohraničený cieľmi na ktoré sa spoločnosť chce zamerať. Informácie by mali byť presné, úplné a aktuálne;

6. **Prístupnosť –** subjekt európskych dát musí mať možnosť prístupu k svojim osobným údajom uloženým v USA, pričom majú možnosť zmazať, upraviť, zmeniť nepresné informácie. Toto právo môže byť spoplatnené spoločnosťou a obmedzené početnými výnimkami;

7. **Vynútenie –** každý subjekt európskych dát musí mať možnosť dostupných metód na ochranu jeho práv pod *safe harbor*. Toto ustanovenie ukladá spoločnostiam zriadenie mechanizmu na vyriešenie prípadných sporov a náhrady škody poškodených subjektov, podľa minimálnych požiadaviek uvedených v nasledujúcich ustanoveniach predmetnej úpravy.

Prísnosť týchto ustanovení je však len relatívna, ak zistíme, ako jednoduché je získať status *safe harbor* keďže sa jedná o samo-certifikujúcu sa spoločnosť, na ktorej vytvorenie stačí vyplniť jednostranový formulár, ktorý nie je zložitejší od vytvorenia obchodnej spoločnosti v pomeroch Slovenskej republiky. Svoj status si však musí obnoviť *safe harbor* každý rok.

---

18 Island, Lichtenštajnsko a Nórsko.

19 Právnym základom pre tento inšititút je dohoda medzi US Department of Commerce a Komisiou (EÚ) ktorá sa vykladá v zmysle čl. 25 ods 6 smernice 95/46/ spoločne s rozhodnutím komisie z 10/30/2006 [online] Dostupné na: http://export.gov/static/sh_en_DecisionSECGEN-EN_Latest_eg_main_018400.pdf.

Kritika *safe harbors* smeruje hlavne k nepoužiteľnosti vo väčšom merítku než je tranfer dát medzi USA a EÚ, ďalším je kritika *safe harbors* ako neefektívnych v ochraňovaní práv subjektov dát z európskej únie a samo-cetifikujúci sa proces *safe harbors* vzbudzuje od začiatku existencie pochybnosti z Európskej strany čo sa prenieslo aj do správy Komisie v roku 2004[20] kde hlavnými bodmi boli:

– nezverejňovanie zásad ochrany osobných údajov verejne – ktoré efektívne eliminuje snahu súdneho konania, keďže sa nedajú preukázať nekalé obchodné praktiky, pokiaľ nikdy neboli zverejnené;

– nedostatočná vykonateľnosť rozhodnutí FTC.

Skutočným problémom je komplexnosť prenosu dát cez internet, na ktoré neboli ani *safe harbors* postavené (odoslanie osobných údajov e-mailom do viacerých krajín a pod.). Z toho vyplýva, že *safe harbors* nevytvárajú „sekundárnu zodpovednosť" pre poskytovateľov telekomunikačných sietí a pod., keďže týto jednajú iba ako prostredníci a nenesú zodpovednosť.[21]

Napriek týmto nedostatkom sa dá konštatovať, že právny systém Európskej únie je jeden z najkomplexnejších a len výnimočne sa nachádza aj v neeurópskych krajinách.

3. Prehľad úpravy neeurópskych krajín

V nasledujúcej kapitole sa pokúsim stručne opísať právnu úpravu štátov opomenutých svetových regiónov, ktoré sa odlišujú od klasického modelu prezentovaného Madridskou rezolúciou, ktorá je opísaná v závere tejto práce s rovnomenným názvom.

3.1. Čína

Čína má len obmedzenú ochranu pre súkromnú komunikáciu a neautorizovanú manipuláciu osobných údajov o zamestnancoch. Neexistujú právne predpisy porovnateľné s právnou úpravou EÚ a všeobecná ochrana osobných údajov.

Návrh zákona na všeobecnú ochranu dát bol podaný v roku 2005 no do dnešného dňa nebol prijatý.[22] Právna úprava pozná ochranu dát, ktoré sú spojené individuálnymi sektormi (napríklad bankovým a telekomunikáciami. Zmeny v trestnom práve vyžadujú, aby štátne úrady, finančné, zdravotnícke a vzdelávacie inštitúcie zaviedli opatrenia na ochranu osobných údajov, avšak nie je jasné akým spôsobom sa to má odohrať.

Dá sa konštatovať, že nie je presne vymedzený okruh chránených dát a prenos informácií môže byť pod kontrolou z dôvodov národnej bezpečnosti.

3.2. Japonsko

Japonsko má vlastný systém ochrany osobných údajov. Zákon na ochranu osobných údajov vytvoril v Japonsku systém pre správcov dát zo súkromného a verejného sektora. Japonské ministerstvá taktiež vydávajú pokyny (pre telekomunikácie, finančné služby, transport a zdravotníctvo), ktoré síce nemajú silu zákona, avšak sú dodržiavané.

---

[20] Správa komisie na implementáciu rozhodnutia 520/2000/EC, [online] Dostupné na: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf.

[21] US Department of Commerce *U.S.-EU Safe Harbor Framewrok: A Guide to Self-Certification*, [online] Dostupné na: http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

[22] ROSE N.: *Global Data Privacy Directory, str. 107,* [online] Dostupné na: http://www.nortonrose.com/files/global-data-privacy-directory-52687.pdf.

Chránenými údajmi sú v tomto štáte dáta, ktorými sa dá identifikovať žijúcu osobu menom, dátumom narodenia, alebo inou informáciou o jedincovi. Na prenos dát je vo väčšine údajov potrebný súhlas osoby ktorej sa to týka.[23]

3.3. Spojené arabské emiráty

Napriek tomu, že SAE neprijali špecifickú legislatívu na ochranu osobných dát v krajine platí hneď niekoľko zákonov, ktoré môžu ovplyvniť prenos osobných údajov, ba čo viac ekonomické zóny *Dubai International Financial Centre* (DIFC) a *Dubai Healthcare City* (DHCC) majú vlastný právny režim vzťahujúci sa na spoločnosti, ktoré tam vykonávajú činnosti. Všeobecná federálna právna úprava sa vzťahuje na ochranu komunikácií a zákazu spôsobenia škody zverejnením osobných údajov. DIFC sa drží definície dát podľa smernice EÚ, teda chránenými osobnými údajmi sú všetky informácie vzťahujúce sa na osobu. DHCC chráni informácie o pacientovom duševnom, alebo telesnom zdraví v akejkoľvek podobe a taktiež informácie o platbách ak je v rozumnej miere možné predpokladať, že sa takými informáciami dá pacient identifikovať.[24]

4. Budúcnosť ochrany osobných údajov na internete: *Madridská rezolúcia*

Z dôvodov diverzity úrovne ochrany osobných údajov na národnej úrovni a zákonov týkajúcich sa ochrany práva na súkromie vzrástlo medzinárodné volanie po svetovom právnom nástroji na ochranu dát, čo vyústilo do „*Madridskej rezolúcie*" v roku 2009 (ktorej zmluvnými stranami sú garanti z viac ako 50 z štátov, organizovaní Španielskou agentúrou na ochranu osobných údajov), ktorá stanovila návrh zoznamu medzinárodných zásad pre *data protection* a súkromie.[25] Rezolúcia obsahuje ustanovenia týkajúce sa medzinárodných prenosov dát, podľa ktorých sa môžu vykonávať vtedy ak import dát spĺňa úroveň ochrany požadovanú rezolúciou. Dokument ďalej dovoľuje, aby bola ochrana zabezpečená inými prostriedkami, ako napríklad vzájomnými dohodami a zaväzujúcimi obchodnými pravidlami. Rezolúcia umožňuje krajinám povoliť prenosy dát v situáciách (výnimkách) podobných, ako je tomu v smernici EU.[26]

Záver

Oblasť *cyberspace* postavila pred medzinárodné právo nové výzvy spojené s riešením konfliktov legislatív pri otázkach prenosu osobných dát, ohraničenia slobody prejavu, využiteľnosti *soft law*, ako aj práva na sebaobranu štátov pri kyberútokoch. V tejto práci sme sa pokúsili ponúknuť prehľad riešenia prvého problému z pohľadu medzinárodného práva, jeho súčasnej podoby a vôle štátov vyjadrenej Madridskou rezolúciou s cieľom vyššej úrovne ochrany osobných údajov v budúcnosti prevažne podľa vzoru Európskej

---

[23] ROSE N.: *Global Data Privacy Directory, str. 115,* [online] Dostupné na: http://www.nortonrose.com/files/global-data-privacy-directory-52687.pdf.

[24] ROSE N.: *Global Data Privacy Directory, str. 104,* [online] Dostupné na: http://www.nortonrose.com/files/global-data-privacy-directory-52687.pdf.

[25] The Madrid Resolution *International Standards on the Protection of Personal Data and Privacy (2009)*, [online] Dostupné na: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.

[26] Podobne ako smernica aj do textu Madridskej rezolúcie sa presadili ustanovenia o možnosti zmazať už získané informácie na žiadosť oprávnenej osoby, právo prístupu k už zhromaždeným dátam a pod., [online]. Dostupné na: http://www.privacyconference2011.org/htmls/adoptedresolutions/2009_madrid/2009_m2.pdf.

únie. Je nepochybné, že toto rýchlo sa rozvíjajúce odvetvie prinesie nové výzvy, ktoré bude riešiť medzinárodné právo a zdôrazní tak svoju úlohu regulácie medzinárodného spoločenstva.

Svetová konferencia o medzinárodných telekomunikáciách (WCIT 2012) a rozšírenie pôsobnosti medzinárodných telekomunikačných predpisov na oblasť internetu – kto kontroluje internet?

Jozef Bujňák

Úvod

Svetová konferencia o medzinárodných telekomunikáciách 2012 v Dubaji (ďalej len WCIT 2012) vyvolala silný ohlas medzi odbornou, ale aj laickou verejnosťou. Snaha o rozšírenie pôsobnosti predpisov Medzinárodnej telekomunikačnej únie (ďalej len ITU) aj na oblasť internetu, a teda jeho rozsiahlejšiu medzinárodnoprávnu reguláciu spôsobila v mnohých vyspelých krajinách, pochopiteľne, najmä negatívne reakcie. V tejto práci sa nebudem venovať všetkým oblastiam, na ktoré mala WCIT 2012 dopad (a ktoré zahŕňajú široké pole telekomunikačných služieb), ale iba internetu, teda aj jeho právnej regulácii zo strany ITU, ako aj najdôležitejším technikalitám a najnevyhnutnejším ekonomickým aspektom spojeným s touto reguláciou.

1. Medzinárodná telekomunikačná únia – ITU a WCIT 2012

Najprv by som rád stručne priblížil ITU a právny rámec jej fungovania. ITU, čiže International Telecommunication Union je špecializovaná agentúra OSN zameraná na problematiku informačných a komunikačných technológií.[1] Združuje 193 členských štátov; okrem Vatikánu sú všetky ostatné zároveň aj členmi OSN. Na čele ITU stojí Generálny sekretár, volený na obdobie štyroch rokov Konferenciou splnomocnencov; momentálne túto funkciu vykonáva Dr. Hamadoun Touré.[2] Konferencia splnomocnencov (Plenipotentiary Conference) zároveň schvaľuje všetky základné texty ITU.[3]

Základnými textami ITU sú Ústava a Dohovor o ITU, Všeobecné pravidlá konferencií, zhromaždení a schôdzí únie, záväzné Regulácie ITU (ďalej len ITR) a nezáväzné Odporúčania ITU.[4]

ITR sú medzinárodná zmluva a vymedzujú pôsobnosť ITU v oblasti telekomunikácií. Ich cieľom bolo vytvorenie medzinárodnoprávneho rámca, ktorý by umožnil globálny rozvoj telekomunikačných technológií, najmä zlepšil cezhraničnú prepojiteľnosť a interoperabilitu.[5] Tu je potrebné poukázať na fakt, že pred WCIT 2012 boli ITR nezmenené od ich prijatia v roku 1988, čiže v období, kedy bol internet prakticky ešte v plienkach,[6] a teda nielen že sa nevzťahovali na internet, ale ani nemohli predvídať rozvoj v oblasti internetu a telekomunikačných technológií.[7] Z tohto dôvodu bola pociťovaná potreba revízie ITR.

---

1 http://www.itu.int.

2 http://en.wikipedia.org/wiki/International_Telecommunication_Union.

3 http://www.itu.int/plenipotentiary/2010/index.html.

4 http://www.itu.int/net/about/basic-texts/index.aspx.

5 ITU Move to Expand Powers Threatens the Internet: Civil Society Should Have Voice in ITU Internet Debate. Prístupné online na: https://www.cdt.org/files/pdfs/CDT-ITU_WCIT12_background.pdf.

6 Internet Society Background Paper – International Telecommunication Regulations. Prístupné online na: http://www.internetsociety.org/sites/default/files/Internet%20Society%20Background%20Paper-%20International%20Telecommunication%20Regulations(1).pdf.

7 http://www.itu.int/oth/T3F01000001.

Dohľad nad prípravou WCIT 2012 mala ITU Council Working Group (CWG), ktorá už od roku 2011 organizovala sériu prípravných stretnutí, na ktorých si krajiny v jednotlivých regiónoch pripravili spoločné návrhy a stanoviská. Tieto mala CWG spracovať do tzv. Dočasných dokumentov (Temporary Documents, TD). Medzi témy, ktorým sa mala WCIT 2012 venovať, patrili napríklad boj proti spamu, záväzná aplikácia Odporúčaní ITU, kyberbezpečnosť, ochrana osobných dát, modely platieb a úhrad, regulácia nových technológií, distribúcia a alokácia internetových adries.[8]

1.1. Kritika WCIT 2012 najmä zo strany odbornej verejnosti

Záplava kritiky sa týkala nielen jednotlivých koncepcií a navrhovaných zmien ustanovení ITR, ale aj samotnej WCIT 2012. Konferencii ako takej bola vytýkaná najmä netransparentnosť, uzavretosť voči odbornej (a nielen odbornej) komunite,[9] čo sa prejavilo v sťaženej dostupnosti niektorých dokumentov,[10] ako aj nespôsobilosť ITU riešiť problémy spojené s reguláciou internetu – či už kvôli prílišnej vágnosti ustanovení ITR, nepostačujúcich pre komplexné riešenie problémov,[11] alebo pre ťažkopádnosť a pomalosť samotnej ITU – čo je v príkrom kontraste s rýchlym a dynamickým rozvojom internetu.[12] Podľa niektorých odborníkov[13] dokonca ani neexistuje potreba regulácie internetu zo strany ITU, keďže tzv. multistakeholder model - čiže decentralizovaná samoregulácia internetu jednotlivými zainteresovanými stranami (ďalej len stakeholderi), medzi ktoré môžu patriť okrem odborných organizácií a poskytovateľov internetových služieb napríklad aj vlády štátov – dokáže pružnejšie a efektívnejšie reagovať na potreby a situáciu na internete, než väčšinou vágne ustanovenia medzinárodných zmlúv.[14] Napriek tomu, že Generálny tajomník ITU Hamadoun Touré ešte pred samotnou konferenciou vyhlásil, že sa táto konferencia nebude týkať regulácie internetu, nielen že boli na nej predložené návrhy ktoré by rozšírili pôsobnosť ITR na oblasť internetu, resp. sa týkali jeho regulácie, ale boli aj zapracované do finálnej podoby ITR.[15]

---

8 Internet Society Background Paper – International Telecommunication Regulations. Prístupné online na: http://www.internetsociety.org/sites/default/files/Internet%20Society%20Background%20Paper-%20International%20Telecommunication%20Regulations(1).pdf.

9 Napríklad: HAMMOND, B.: Failure to Reach Consensus at WCIT Prompts Calls For Renewed Effort to Support Multistakeholder Approach. In: Telecommunications Reports, 1/2013, s. 1.

10 Významnou bola činnosť internetovej stránky wcitleaks.org.

11 Napríklad: ISOC Opposes WCIT Approach That Would Regulate Networks. In: Telecommunications Reports, 22/2012, s. 5. Nepodarilo sa mi zistiť meno autora tohto článku.

12 STANTON, L., KIRBY, P.: Private Sector Worries About WCIT Internet Proposals. In: Telecommunications Reports, 11/2012, s. 48.

13 Napríklad Terry Kramer, delegát USA na WCIT 2012 a Lawrence E. Strickling z National Telecommunications and Information Administration.

14 ISOC Opposes WCIT Approach That Would Regulate Networks. In: Telecommunications Reports, 22/2012, s. 5.

15 HAMMOND, B.: Failure to Reach Consensus at WCIT Prompts Calls For Renewed Effort to Support Multistakeholder Approach. In: Telecommunications Reports, 1/2013, s. 49 – 51.

2. Najdôležitejšie návrhy týkajúce sa internetu na WCIT 2012

Návrhy na doplnenie ITR mali značne široký záber. Medzi najdôležitejšie patrili rozšírenie pôsobnosti ITR z „recognized operating agencies" na „operating agencies",[16] presun kontroly a dohľadu nad internetom od mimovládnych organizácií (stakeholderov)[17] na ITU, posilnenie pozície ITU pri regulácii poplatkov spojených s internetovými službami a roamingom, zmena Odporúčaní ITU z nezáväzného dokumentu na záväzné zmluvné ustanovenia a návrhy ustanovení ITR, ktoré by upravovali politiku ITU vo vzťahu ku kyberbezpečnosti, kyberzločinu, spamu, súkromným dátam.[18]

2.1. Recognized operating agencies, alebo operating agencies?

Uholným kameňom diskusií týkajúcich sa internetu a WCIT 2012 je rozšírenie pôsobnosti ITR na oblasť internetu. Platné a účinné ITR z roku 1988 sa vzťahujú na „recognized operating agencies" (ROA), čo sú veľké telekomunikačné spoločnosti, štátne alebo súkromné, ktoré existujú prakticky v každej krajine.[19] Komunikácia založená na IP (internet protocol) je podľa platných a účinných ITR mimo ich regulačnej pôsobnosti.[20] Podľa návrhov predložených na WCIT 2012 by sa revidované ITR vzťahovali na „*operating agencies*" – čo by zahŕňalo nielen ROA, ale aj široké spektrum spoločností a služieb momentálne neregulovaných ITR. Proti sa postavili najmä Spojené štáty. Americká Internet Society (ISOC) vo svojom návrhu[21] navrhla obmedziť rozsah pôsobnosti ITR na signatárov zmluvy, a teda zamedziť rozšíreniu pôsobnosti z ROA na operating agencies. Taktiež naliehala, aby Odporúčania ITU naďalej účinkovali na báze dobrovoľnosti a aby problémy spojené najmä s kyberzločinom a spamom zostali mimo dosahu ITU, resp. v pôsobnosti vnútroštátneho práva a stakeholderov. Rovnako bola ISOC proti návrhom, podľa ktorých by sa ITR mali aplikovať napríklad aj na smerovanie dátových tokov a prideľovanie internetových adries. Na druhej strane však ISOC podporila zahrnutie ustanovení týkajúcich sa bezpečnosti telekomunikačných sietí, ako ajkonceptov konkurencie a liberalizácie trhu do revidovaných ITR.[22]

2.2. Návrh ETNO a „*sender pays*" model

Európska asociácia operátorov telekomunikačných sietí (European Telecommunications Network Operators Association, ďalej len ETNO) predložila prostredníctvom členských krajín ITU návrh zmeny článkov 2, 3 a 4 ITR, označovaný ako „návrh ETNO", ktorý by v (deklarovanom) záujme zvýšenia investícií a zlepšenia inovácií v oblasti internetu znamenal zmenu existujúceho IP systému, zavedenie tzv. Quality of Service (QoS) a „*sending party*

---

16 Odborné termíny „*recognized operating agencies*", resp. „*operating agencies*" som sa rozhodol ponechať v anglickom jazyku z dôvodu zachovania lepšej prehľadnosti.

17 Napr. ICANN, viac na http://www.icann.org/.

18 Gross, D. A., Lucarelli, E.: The 2012 World Conference On International Telecommunications: Another Brewing Storm Over Potential UN Regulation Of The Internet. Dostupné online: http://www.whoswholegal.com/news/features/article/29378/the-2012-world-conference-internationaltelecommunications-brewing-storm-potential-un-regulation-internet.

19 V SR sú to napríklad Orange alebo ST. Zoznam ROA je dostupný online na: http://www.itu.int/oth/T0204/en.

20 ITR, Článok 9. Prístupné online na: http://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf.

21 Podanom prostredníctvom delegácie USA.

22 ISOC Opposes WCIT Approach That Would Regulate Networks. In: Telecommunications Reports, 22/2012, s. 5, 6.

network pays" (sender pays) modelu.[23] Teda model, podľa ktorého fungujú telefónne siete, by sa aplikoval na internet - čiže odosielajúca strana by v záujme poskytnutia obsahu používateľom musela za prepojenie operátorovi, pričom najväčší dopad by to malo na cezhraničné dátové toky. To by mohlo znamenať nielen zvýšenie cien poskytovania služieb spojených s internetom, ale aj možnú izoláciu používateľov najmä v rozvojových krajinách od prístupu ku globálnej sieti, nahradenie súčasného, deregulovaného (a funkčného) systému regulovaným, obmedzenie inovácií a tvorby nového obsahu (keďže medzi inovátorom – odosielateľom a používateľom – príjemcom by stál operátor). Takýto model by teda prospel veľkým telekomunikačným operátorom a naopak, poškodil koncových používateľov – a to najmä v krajinách s nedostatočne rozvinutou spoločnosťou, ktoré voľný prístup ku globálnej sieti potrebujú najviac.[24]

2.3. Kyberbezpečnosť a ochrana proti spamu: zálohovanie dát a filtrácia obsahu

Arabská regionálna skupina podala návrh, ktorý by vyžadoval od členských štátov opatrenia vedúce k riešeniu problémov spojených s kyberbezpečnosťou, kyberzločinom, kyberútokmi, spamom (nevyžiadaná elektronická komunikácia) a ochranou osobných údajov. Podobný návrh vzišiel aj od africkej skupiny, volajúc po harmonizácii právnych úprav týchto problémov členskými štátmi. Podľa oboch by mala byť ITU ohniskom medzinárodnej spolupráce v tejto oblasti.

Problémom by v tomto prípade mohla byť statickosť ITR; nedokázali by dostatočne pružne reagovať na vývoj v danej oblasti. Na druhej strane, príliš všeobecne poňaté ustanovenia ITU by otvárali priestor na zneužitie týchto ustanovení niektorými členskými štátmi za účelom medzinárodnoprávneho krytia represívnych opatrení voči používateľom v daných štátoch.[25] Kyberzločinu a kyberútokom sa v tejto práci bližšie venovať nebudem.

Zároveň africká skupina predložila návrh, v ktorom nalieha na členské štáty, aby harmonizovali svoje vnútroštátne právne úpravy zálohovania dát. Problém tu spočíva najmä vo veľkých rozdieloch medzi vnútroštátnymi právnymi úpravami problematiky. Nie je dokonca jasná opodstatnenosť takýchto právnych úprav. Podobne, ako pri kyberbezpečnosti, aj tu vyvstáva otázka, či je ITU schopná regulácie v danej oblasti.[26] Delegácia USA vedená Terrym Kramerom namietala aj zahrnutie ustanovení týkajúcich sa spamu do ITR. Aj spam je totiž forma obsahu; regulácia spamu by potenciálne mohla znamenať aj filtrovanie iných foriem obsahu,[27] a teda možné otvorenie medzinárodnoprávnych dverí cenzúre internetu.

---

23 CWG-WCIT12 Contribution 109. Prístupné online na: http://files.wcitleaks.org/public/ETNO%20C109.pdf.

24 ETNO Proposal Threatens to Impair Access to Open, Global Internet. Prístupné online na: https://www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf.

25 Primárny zdroj je pravdepodobne nedostupný. Security Proposals to the ITU Could Create More Problems, Not Solutions. Prístupné online na: https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf.

26 Security Proposals to the ITU Could Create More Problems, Not Solutions. Prístupné online na: https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf.

27 HAMMOND, B.: Failure to Reach Consensus at WCIT Prompts Calls For Renewed Effort to Support Multistakeholder Approach. In: Telecommunications Reports, 1/2013, s. 50.

3. Výsledky WCIT 2012 – nové ITR

Výsledkom WCIT 2012 bolo uzavretie novej medzinárodnej zmluvy, ktorú podpísalo 89 štátov, zväčša krajín blízkeho východu, afrických krajín, ako aj Rusko a Čína. Zmluvu nepodpísali napríklad USA, Veľká Británia, Kanada, Austrália, ale ani Česká republika a Slovensko.[28] Ide teda o rozkol v medzinárodnoprávnej úprave telekomunikácií, pričom podľa vyjadrenia Európskej komisie tvoria signatári len malý podiel na celkových globálnych dátových tokoch.[29] Nové ITR budú účinné od 1. 1. 2015.

3.1. Zmeny v ustanoveniach ITR

V Preambule ITR pribudla zmienka o ľudských právach; podľa Preambuly majú členské štáty (signatári) aplikovať ustanovenia ITR v súlade s ľudskoprávnou úpravou.[30] Je to odpoveď na diskusie počas WCIT 2012 týkajúce sa internetu a ľudských práv, najmä v súvislosti s cenzúrou.[31] Zároveň Preambula uznáva právo prístupu členských štátov k medzinárodným telekomunikačným službám.[32] Nové ITR sa taktiež nebudú vzťahovať na aspekty telekomunikácií spojené s obsahom[33] a zavádzajú nejasný a nedefinovaný pojem „authorized operating agencies",[34] ukladajú členským štátom záväzok zabezpečiť robustnosť medzinárodných telekomunikačných sietí,[35] a obsahujú aj kontroverzné ustanovenie, podľa ktorého by členské štáty mali podniknúť nevyhnutné opatreniu na zamedzenie spamu;[36] v prípade, že pod „authorized operating agencies" spadajú aj poskytovatelia internetových služieb (čo závisí od spôsobu interpretácie), by toto ustanovenie skutočne mohlo otvoriť ďalšiu cestu k rozsiahlejšiej regulácii obsahu zo strany štátov.[37] WCIT 2012 zároveň prijala aj nezáväznú rezolúciu, ktorá sa priamo týka internetu; v podstate ide o potvrdenie úsilia a zámeru pokračovať v diskusiách o internete na pôde ITU.[38] Táto rezolúcia však nie je súčasťou ITR a je v protiklade s už spomenutými vyjadreniami Generálneho sekretára ITU Hamadouna Tourého.

Záver

Napriek tomu, že v samotných ITR sa termín „internet" nespomína, sa tieto nepochybne týkajú aj internetu. Vyplýva to najmä z ustanovení týkajúcich sa boja proti spamu; keďže diskusie o spame sa viedli v kontexte internetu a problém spamu samotného je najmä problémom internetu. Zároveň tomu nasvedčuje aj „kompromisné" a interpretačne nejasné ustanovenie o „authorized operating agencies", čo podľa môjho názoru môže (a nemusí) zahŕňať aj poskytovateľov pripojenia k internetu. Taktiež vysoko kontroverzné návrhy,

---

28 Zoznam signatárov: http://www.itu.int/osg/wcit-12/highlights/signatories.html.
29 Prístupné online na: http://europa.eu/rapid/press-release_MEMO-12-991_en.htm.
30 Final Acts of WCIT 2012, Preambula.
31 FIDLER, D. P.: Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations. Prístupné online na: http://www.asil.org/insights130207.cfm.
32 Final Acts of WCIT 2012, Preambula.
33 Final Acts of WCIT 2012, Článok 1.1 a).
34 Final Acts of WCIT 2012, Článok 1.1 abis).
35 Final Acts of WCIT 2012, Článok 5A.
36 Final Acts of WCIT 2012, Článok 5B.
37 FIDLER, D. P.: Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations. Prístupné online na: http://www.asil.org/insights130207.cfm.
38 Final Acts of WCIT 2012, Resolution PLEN/3, Dubai 2012.

akým bol napríklad návrh ETNO, neboli prijaté; rovnako je zo zmenených ustanovení badať snahu o kompromis. Či táto snaha bola úspešná, alebo nie, ilustruje fakt, že mnohí najväčší hráči v oblasti internetu na čele s USA odmietli podpísať nové ITR. WCIT 2012 teda nedokázala naplniť očakávania spojené s dosiahnutím konsenzu, naopak, vyústila vo fragmentáciu medzinárodnoprávnej úpravy telekomunikácií (a internetu), čiže v pravý opak toho, čo je účelom medzinárodnoprávnych úprav; to môže do budúcna spôsobiť problémy najmä v ekonomickej oblasti, pričom najviac postihnutí môžu byť práve štáty, ktoré zmluvu podpísali.

Na WCIT 2012 sa vytvorili dva politické bloky, kde na jednej strane stáli zväčša demokratické, vyspelé krajiny; na strane druhej stáli krajiny s autoritárskymi alebo totalitnými režimami, respektíve krajiny známe svojim svojráznym prístupom k vlastným občanom, čím bol definovaný spor o charakter medzinárodnoprávnej regulácie internetu. Tým nechcem, samozrejme, redukovať význam WCIT 2012 iba do politickej roviny – avšak príčina budúcej dvojkoľajnosti medzinárodnoprávnej úpravy telekomunikačných a informačných technológií leží práve v politických sporoch. Kľúčové pozície kontroly internetu (najmä pozícia ICANN-u) teda zatiaľ ostávajú relatívne stabilné a hlas stakeholderov bude mať pri regulácii internetu vo väčšine vyspelých krajín aj naďalej veľkú váhu – avšak WCIT 2012 poukázala na trend zvyšovania miery štátnej kontroly a regulácie internetu vo svete, ako aj na snahu medzinárodnoprávne pokryť takúto kontrolu a reguláciu.

Kyber útoky a medzinárodné právo

Natália Kobulská

Úvod

Súčasný svet je možné označiť za závislý na technológiách a internete. Postupom času sa vytvoril virtuálny svet, na ktorý sa štáty i jednotlivci častokrát spoliehajú. Štáty si postupne začínajú uvedomovať, že čím viac sú odkázané na použitie technológií, tým zraniteľnejšie sa stanú ako možný cieľ nového druhu útokov, ktoré zasahujú práve túto virtuálnu sféru- kyber útokov. V 21. storočí už nie je ťažiskom ozbrojeného konfliktu využitie vojenskej sily štátu, ale objavujú sa nové spôsoby boja i útokov. Medzi ne je možné zaradiť aj kyber útoky. Stále existujúcou, a neustále zväčšujúcou sa hrozbou je terorizmus, ktorého jednu časť tvorí kyberterorizmus. Čo to kyber útok je a dá sa vôbec celá táto oblasť subsumovať pod existujúce inštitúty medzinárodného práva?

1. Pojem kyberútok a vysvetlenie súvisiacich pojmov

Na to, aby bolo možné pri kyber útoku uvažovať o jeho začlenení pod existujúcu medzinárodnoprávnu úpravu, je nutné objasnenie pojmov, aké sa v tejto oblasti vyskytujú, a to najmä kyberpriestorové operácie, kyber útok a počítačovú kriminalita. Prvý menovaný je najširší a zahŕňa v sebe kyber útok aj počítačovú kriminalitu. V súčasnosti neexistuje odvetvie medzinárodného práva (zmluvného či obyčajového), ktoré by obsahovalo pravidlá upravujúce špecifickú oblasť, akou sú kyber útoky, preto je nevyhnutné ho začleniť pod „všeobecné“ normy práva ozbrojených konfliktov. Najširším pojmom, pod ktorý sa dá kyber útok subsumovať, sú kyberpriestorové operácie. Kyberpriestorové operácie sú v literatúre definované ako „použitie kyber prostriedkov, ktorých primárnym cieľom je dosiahnuť ciele v alebo cez kyberpriestor.“[1] Do tejto kategórie patrí aj tzv. information warfare, ktorý sa spomína v kontexte s kyberpriestorovými operáciami ako ozbrojenom konflikte. Počítačová kriminalita je trestná a právom vynútiteľná, pričom používa na dosiahnutie alebo ktorej cieľom je počítač.[2] Ide o konanie jednotlivca (páchateľa), ktoré je postihnuteľné trestným právom konkrétneho štátu. Pojem kyber útok sa v širšom význame používa na prípady kyberpriestorových operácií, ktoré môžu byť považované za ozbrojený konflikt.[3] Keďže legálna definícia tohto pojmu neexistuje, vychádzame z vymedzenia Roscciniho, ktorá je podľa nás najvýstižnejšia. Podľa neho je kyber útok „nepriateľské použitie kybernetickej sily, ktoré môže byť samostatným konaním, prvým úderom ozbrojeného konfliktu, útokom v kontexte už začatého ozbrojeného konfliktu, alebo reakciou na predchádzajúci konvenčný alebo kybernetický útok.“[4] Postupne rozoberieme jednotlivé aspekty tejto definície.

---

1 Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 211.

2 Tamtiež.

3 Tamtiež, s. 212.

4 Roscini, M.: World Wide Warfare- *Jus ad bellum* and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14, 2010, s. 91.

2. Znaky a špecifiká kyber útoku

Kyber útok je špecifické konanie, ktoré má spoločné s „klasickým" útokom minimálne to, že ide o útok, ktorý má svojho pôvodcu a cieľ. Predtým, ako prejdeme k jednotlivým obsahovým aspektom tohto pojmu, je potrebné poukázať na niektoré špecifiká, ktoré ho oddeľujú od klasického vnímania útoku, čím ho stavajú do osobitného postavenia, ku ktorému je nutné prispôsobovať kvalitatívne inak:

- *priestor, v akom sa odohráva:* nejde o priestor štátu vymedzeného územím, ale o kyberpriestor,
- *irelevancia územia:* pri kyber útoku sa pôvodca neviaže na územie, ale na cieľ, preto je nepodstatné, ako sú vymedzené štátne hranice (útok môže prejsť naraz desiatky hraníc za niekoľko sekúnd), pevnina alebo more (ak je cieľové zariadenie umiestnené na mori, vo vzdušnom priestore, na obežnej dráhe),
- *cieľ útoku:* nemusí ísť o územie štátu, budovy, jednotlivcov, ale o počítače, ich systémy, technológie, software,
- *útočník:* veľký okruh potenciálnych subjektov, môže ísť o štát alebo teroristov (to je spoločná črta s klasickým útokom), ale môže ísť o jednotlivca, napr. pri hackerskom útoku, skupinu ľudí, organizáciu či neznámy zdroj kvôli anonymite internetu a jeho používateľov,
- *časové hľadisko:* keďže vzdialenosť nehrá rolu, útok môže byť začatý aj dokonaný v priebehu niekoľkých sekúnd, a to aj súčasne na rôznych kontinentoch, práve jeho rýchly začiatok spôsobuje takmer nulovú predvídateľnosť zo strany napadnutého štátu, prípadne môže byť otázny aj jeho začiatok či čas dokonania,
- *prostriedky:* je možný ich rýchly vývoj a zmena, s postupom vedy a techniky sa vytvára čoraz viac možností jej využitia i na tento účel, tiež ľahká dostupnosť a finančná nenáročnosť,[5] keď na niektoré druhy kyber útoku stačí počítač, čo je v súčasnosti ľahko dostupné médium pre jednotlivca.

Keďže neexistuje osobitná skupina noriem zaoberajúca sa kyber útokmi, je nutné ich subsumovať pod platné pravidlá práva ozbrojených konfliktov, hoci nie sú výslovne spomenuté nielen v Charte OSN, ale ani v Ženevskom či Haagskom dohovore. Pomôckou je výklad MSD v prípade Legálnosti použitia jadrových zbraní, kde Súd vyložil články Charty OSN v tom zmysle, že „neodkazujú na špecifické zbrane...aplikujú sa na akékoľvek použitie sily bez ohľadu na použité zbrane."[6] Vzhľadom na to, že kyber útoky sú novou formou použitia sily, ktorú v čase schvaľovania Charty OSN nebolo možné predvídať, je cez extenzívny výklad jej ustanovení možné kyber útoky pod ustanovenia Charty zahrnúť aj za pomoci výkladu MSD a považovať prostriedky útoku za zbrane. Tým sa však problém úplne nevyriešil, a to z viacerých dôvodov.

---

5 Ľahkú dostupnosť a finančnú nenáročnosť spomenul Roscini, odk. 4.

6 *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 I C J 22, par. 39: „These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter."

V prvom rade nie je možné považovať akúkoľvek ofenzívnu operáciu v kyberpriestore za útok (môže ísť napr. o počítačovú kriminalitu),[7] pretože sa jedná o špecifický typ konania, v ktorom sa nemusí vyskytovať ani násilie, prípadne nemusí byť namierené voči ľuďom alebo nespôsobuje škodu.[8] Po druhé, je zložité identifikovať pôvodcu útoku, čiže pričítateľnosť konania útočníkovi alebo štátu (pozri nižšie). Na určenie, či sa jedná o kyber útok, a nielen o kyber priestorovú operáciu, je možné použiť viacero metód. Handlerová predstavuje 3 podstatné kritériá, ktoré musia byť splnené, a to:

1. výber cieľa,
2. dopad útoku a
3. načasovanie.

1. Cieľom je podstatná infraštruktúra, teda sektory, ktoré najviac ovplyvnia dopad útoku, alebo tiež podstatné zložky národnej sily, napr. diplomatické, vojenské, ekonomické alebo informačné, ale väčší dôraz sa kladie na infraštruktúru, bez ohľadu na jej prepojenie so štátom.
2. Ide o kritérium rozsahu útoku a efektu, ktorý vyvolal. Pri tomto kritériu sa opiera o výklad MSD v prípade Nicaragua, keď pri výklade pojmu ozbrojený útok Súd použil práve rozsah a účinok. Tu sa nevyžadujú priame kinetické účinky, stačí účinok v užšom zmysle, teda narušenie alebo znemožnenie komunikácie, alebo v širšom zmysle ako znemožnenie koordinácie, ako je panika a zmätok.
3. Pri tomto kritériu treba rozlišovať, či ide o kyber útok, ktorý doprevádza iný útok alebo je samostatným útokom. V prvom prípade musí ísť o blízkosť ku kinetickým účinkom, ktoré majú nastať. Musia sa udiať v časovej súvislosti s ďalším útokom, ktorý doprevádza.[9] O kinetický účinok útoku ide vtedy, ak vyvolá fyzickú ujmu alebo zničenie. Zo spojenia týchto kritérií vyplýva, že niektoré z nekinetických kyberpriestorových operácií, ktoré spôsobujú kinetické účinky, môžu byť zahrnuté pod pojem útok.[10]

3. Špecifické aspekty

3.1. Pričítateľnosť konania

Dôležitou otázkou je pričítateľnosť konania štátu, ktorá zakladá medzinárodne protiprávne konanie štátu podľa Návrhu článkov Komisie pre medzinárodné právo.[11] Pri kyber útokoch je to však zriedkakedy priamo štát, ktorý útočí. Okruh subjektov je veľmi široký, môže ísť o neštátnych aktérov, teroristické skupiny, jednotlivcov, a pod. Vývoj techniky ešte nedospel do štádia, kedy by vedel presne určiť pôvodcu dostatočne presne a zároveň včas na to, aby mohol proti nemu efektívne zasiahnuť, keďže subjektom môže byť v najširšom zmysle slova každý používateľ počítačov. Vynára sa nevyhnutnosť vyvodenia zodpovednosti štátu za konanie. Niekedy však je možné útočníka identifikovať, podľa Rosciniho ide o prípad, ak predchádzajúci/nasledujúci/súčasne prebiehajúci konvenčný útok odhalí

---

7 Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 220.

8 Tamtiež.

9 Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 226-232.

10 Podrobnejšie v: Tamtiež, s. 236.

11 Návrhy článkov o zodpovednosti štátov za medzinárodne protiprávne konanie Komisie pre medzinárodné právo, Príloha rezolúcie Valného zhromaždenia OSN A/RES/56/83.

autora kyber útoku. Ak je vyriešený pôvodca, je nastolená otázka pričítateľnosti jeho konania štátu.[12] Na zúženie zodpovednosti štátu slúži test Medzinárodného súdneho dvora v prípade Nicaragua (tzv. Nicaragua test), kde sa Súd vyjadril, že štát musí vykonávať „test efektívnej operatívnej kontroly", ktorá vyjadruje mieru zodpovednosti štátu, ktorý by konal akoby cez štátne orgány.[13] Súd v danom rozsudku konštatoval, že „účasť Spojených štátov, hoci prevažujúca alebo rozhodujúca, na financovaní, organizovaní, školení, dodávaní a vybavení *contras*, výberom ich vojenských alebo polovojenských cieľov, a plánovanie celej akcie, je nedostatočné samo o sebe ... na pričítanie konania *contras* Spojeným štátom".[14] Tento test sa uplatní v prípade, ak je útočníkom človek alebo organizácia, pričom nemôže ísť o prípad štátneho orgánu, ktorého konanie je priamo pričítateľné štátu bez nutnosti vykonania testu.

V prípade, že ide o útok pochádzajúci z počítača, ktorý sa nachádza na území určitého štátu bez jeho účasti, nejde o konanie, ktoré by bolo štátu pričítateľné, avšak štát má povinnosť urobiť primerané a nevyhnutné opatrenia na zabránenie alebo zastavenie útoku. Porušenie tejto povinnosti však nezakladá jeho zodpovednosť za kyber útok, ale za porušenie povinnosti „vedome nedovoliť využiť svoje územie na protiprávne konanie voči iným štátom".[15]

4. Samostatné konanie/súčasť iného konania

Kyber útok nemusí vystupovať ako samostatné konanie, ale aj ako súčasť vojenského ťaženia štátu, ktoré dopĺňa. Môže byť vykonaný súčasne s ním alebo v blízkej dobe. Hoci sám o sebe by možno nepredstavoval hrozbu, v spojení s vojenským ťažením je spôsobilý zvýšiť jeho negatívny dopad alebo inak dopomôcť k jeho úspešnému uskutočneniu, čím predstavuje veľké nebezpečenstvo pre napadnutý štát. Príkladom z praxe je útok Izraela na jadrové zariadenia v Sýrii z roku 2007.[16] Podľa Handlerovej je nutné rozlíšiť aj režim, podľa ktorého sa kyber útok bude posudzovať, teda či pôjde o trestné konanie alebo o konanie vojenské. Toto je nevyhnutné posudzovať najmä z dôvodu odpovede napadnutého štátu, teda aby štát konal tak, aby neporušil normy medzinárodného práva (napr. odpoveďou na trestné konanie nemôže byť vojenský zásah).[17]

5. Pojem ozbrojený útok

Je nespochybniteľné, že kyber útok je útokom podľa medzinárodného práva. Časť právnej teórie sa venuje problému, či je kyber útok možné zahrnúť pod pojem „ozbrojený útok", ktorý je spomenutý v Charte OSN, ale doteraz nie je presne nedefinovaný. Proti jeho zahrnutiu pod ozbrojený útok stojí argument, že nevyvoláva priamo kinetické účinky, resp. nespôsobuje fyzickú škodu. Navyše tu chýba prvok „ozbrojenia", keďže ide o špecifický druh konania, čo však nevylučuje, že je spôsobilý spôsobiť rovnaké následky ako „klasický" ozbrojený útok. Nie je možné poprieť ani fakt, že kyber útok spôsobuje nekinetické účinky,

---

12 Porov. Roscini, odk. 4.

13 Military and Paramilitary Activities In and Against Nicaragua, ICJ Reports, In: Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 214 a 232.

14 Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, bod 115.

15 Prípad Corfu Channel, ICJ Reports 1949, bod 4 a nasl. In: Roscini, odk. 4.

16 Viac o konkrétnych prípadoch použitia kyber útokov v časti 6.

17 Podrobnejšie v: Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 216.

môže, a často sa tak deje, umožniť účinné spôsobenie kinetických účinkov, preto by to podľa Handlerovej[18] nemalo brániť zahrnutiu kyber útoku pod širší pojem ozbrojeného útoku, s ktorým sa stotožňujeme. Podľa Schmitta stojí kyber útok niekde medzi ozbrojenou silou a ekonomickým donútením (economic coertion).[19] Niektorí autori sa pridržiavajú zdržanlivejšieho postoja, napr. Greenwood uviedol, že ak je kyber útok považovaný za ozbrojený útok, je nutné byť zvlášť opatrný, pretože napadnutý štát má právo odpovedať vojenskou akciou. Zároveň však nevylúčil, že pri účinkoch obdobných tým, ktoré by mohol vyvolať ozbrojený útok, je akceptovateľný pohľad na kyber útok ako na ozbrojený útok.[20] Z toho vyplýva, že Greenwood zaradenie kyber útoku pod pojem ozbrojený útok neposudzuje jeho povahu alebo náležitosti, ale účinky, aké vyvoláva a prirovnáva ich k účinkom ozbrojeného útoku. Kritérium účinku, hoci s inými závermi prezentoval Mačák, keď tvrdil, že nie je dôležitá povaha útoku, ak má deštruktívny účinok, tak z pohľadu medzinárodného práva nie je podstatné, či ide o ozbrojený klasický útok alebo kyber útok, pričom zdôrazňuje extenzívny výklad pojmu ozbrojeného útoku a použitia sily.[21] Určujúcim kritériom je teda jeho účinok, keďže spôsob a metódy sú pri kyber útoku netradičné, a často ich ani nie je možné predpokladať, pretože môžu mať akúkoľvek formu. Ak by sme zobrali do úvahy doslovný výklad, „ozbrojený" znamená byť vybavený zbraňou a to, či ide o zbraň v prípade kyber útokov, z rozsudku MSD vo veci Legálnosť použitia jadrových zbraní vyplýva, že áno (pozri vyššie).[22] Je dôvodné považovať kyber útok, ktorého účinkom je zničenie majetku alebo smrť ľudí, za použitie ozbrojenej sily.

6. Agresia

Pri vyjasnení vzťahu pojmov ozbrojený útok a kyber útok je nutné venovať pozornosť aj pojmu agresia. Na rozdiel od ozbrojeného útoku agresia definovaná je, a to v rezolúcii Valného zhromaždenia ako „použitie ozbrojenej sily štátom proti zvrchovanosti, územnej celistvosti alebo politickej nezávislosti iného štátu alebo akýmkoľvek iným spôsobom nezlučiteľným s Chartou OSN."[23] Problém môže spôsobiť prítomnosť spojenia „použitie ozbrojenej sily štátom". Musí ísť o konanie štátu alebo o konanie štátu pričítateľné. Tiež musí byť použitá ozbrojená sila, teda nie každý kyber útok bude definíciu spĺňať, ale len ten, ktorý využil ozbrojenú silu. Vzhľadom na skutočnosť, že v súčasnosti sú súčasťou armád štátov kybernetické jednotky, zaraďujú sa medzi ozbrojené zložky štátu a ich konanie bude môcť byť vyhlásené za agresiu po splnení ďalších podmienok.[24]

---

18 Podrobnejšie v: Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 225.

19 Schmitt, M. N.: Computer Network Attack and the Use of Force in International Law: Thoughts on a normatic framework, The Columbia Journal of Transnational Law, Volume 37, 1999, s. 885-937.

20 Porov. Greenwood, Ch.: Self-defence, In: The Max Planck Encyclopedia of Public Inernational Law, Volume IX, Oxford University Press 2012, s. 106-107.

21 Podrobnejšie v: Mačák, K.: Kyberagresia: Pília USA a Izrael konár, na ktorom sedíme všetci? http://jinepravo.blogspot.sk/2012/06/kyberagresia-pilia-usa-izrael-konar-na.html (navštívené dňa 14.4.2013).

22 Podrobnejšie v: Roscini, M.: World Wide Warfare - *Jus ad bellum* and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14, 2010, s. 106.

23 Rezolúcia Valného zhromaždenia OSN A/RES/3314 (XXIX) Definícia agresie. Slovenský preklad in: Klučka, J.: Medzinárodné právo verejné, Iura edition, Bratislava 2008.

24 Porov. Papanastasiou, A.: Application of International Law in Cyber Warfare Operations, dostupné na: http://ssrn.com/abstract=1673785.

7. Kyber útok v kontexte použitia sily

V medzinárodnom práve platí zákaz použitia sily zakotvený v Charte OSN, ktorý zakazuje riešenie konfliktu ozbrojenou silou, pričom v prípade útoku je možné brániť sa vo forme sebaobrany, ktorá je jediným prostriedkom obrany, ale iba ako výnimka zo zákazu použitia sily, a to len v prípade, keď je štát napadnutý. V súčasnom medzinárodnom práve je však stále problematický výklad pojmu ozbrojený útok (pozri vyššie). O to ťažšie je zaradiť špecifickú oblasť kyber útokov nielen pod tento pojem, ale aj pod širší pojem použitie sily, a to najmä z hľadiska výkladu a praktických dôsledkov.

Článok 2 odsek 4 Charty OSN zakazuje hrozbu silou alebo použitie sily voči územnej celistvosti alebo politickej nezávislosti každého štátu, ale aj každý iný spôsob nezlučiteľný s cieľmi OSN. Jedným z cieľov OSN je aj udržanie medzinárodného mieru a bezpečnosti, čo podľa nášho názoru pokrýva kyber útok, ktorý nebýva namierený voči prvým dvom hodnotám. Je však kyberútok použitím sily alebo hrozba silou? Pri hrozbe silou je to jednoznačnejšie, pretože práve kyberpriestor je ideálnym nástrojom na vyhrážanie sa silou, kyber útok by tak mohol predstavovať len „varovanie", že bude nasledovať klasický ozbrojený útok, resp. ďalší, tentoraz závažnejší kyber útok. Pri použití sily to je zložitejšie, pretože kyber útok môže mať rôznu formu, cieľ a dôsledky, preto nie je možné zahrnúť každý kyber útok pod pojem použitie sily. Zákaz použitia sily je kogentná norma, preto je dôležité, aby, ak bol kyber útok klasifikovaný ako použitie sily, prichádza do úvahy zvažovanie, či sa nejedná o výnimku zo zákazu použitia sily. Výnimkami sú právo na sebaobranu, ktoré je zakotvené v článku 51 Charty OSN, a kolektívne sankcie Bezpečnostnej rady OSN podľa kapitoly VII Charty OSN.[25]

Právo na sebaobranu je vyjadrené priamo v článku 51 Charty OSN: „Ak dôjde k ozbrojenému útoku proti členovi Organizácie Spojených národov, nijaké ustanovenie tejto Charty neprekáža prirodzenému právu na individuálnu alebo kolektívnu sebaobranu, kým Bezpečnostná rada neurobí potrebné opatrenia na zachovanie medzinárodného mieru a bezpečnosti."[26] Na to, aby kyber útok mal atribúty na odpoveď výkonom práva na sebaobranu, musí podľa Grosswalda spĺňať kritériá povahy útoku, motívu a miesta vzniku, ktoré ďalej konkretizuje.[27] Iba kyber útok, ktorý sa dá považovať za ozbrojený útok, môže oprávňovať napadnutý štát na výkon práva na sebaobranu.

8. Konkrétne prípady kyber útoku

Estónsko 2007

Kyber útok na Estónsko bol reakciou na odstránenie ruského vojnového pamätníka z Talinnu, ktorý trval tri týždne. Počas nich najprv znefunkčnil vládne webstránky, neskôr sa rozšíril na noviny, televízne stanice, banky a iné ciele. Nepodarilo sa však dokázať participáciu Ruska na tomto útoku.

Izrael/Sýria 2007

Útok na sýrske jadrové zariadenia v roku 2007 dokumentuje, ako sa s pomocou kyber útoku, ktorý iba dopĺňal bombardovanie, dosiahol zničujúcejší efekt. Izraelské letectvo úspeš-

---

25 Porov. Klučka, J.: Medzinárodné právo verejné, Iura edition, Bratislava 2008, str. 207.

26 Článok 51 Charty OSN:: OSN, Charter of the United Nations, 24 October 1945, 1 UNTS XVI, dostupná na: http://www.unhcr.org/refworld/docid/3ae6b3930.html [stránka navštívená v apríli 2013], Slovenský preklad Charty OSN v: Klučka, J.: Medzinárodné právo verejné, Iura edition, Bratislava, 2008, str. 538.

27 Grosswald, L.: Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, Brooklyn, Journal of International Law; 2011, Vol. 36 Issue 3, p1151-1181.

ne zbombardovalo cieľ potom, ako sa dostalo do sýrskeho vzdušného priestoru bez povšimnutia, keďže bol hackerským útokom nabúraný sýrsky bezpečnostný systém, ktorý lietadlá nezachytil, pretože bol vyradený z prevádzky.[28] Na tomto príklade je preukázateľná nebezpečnosť kyber útokov a ich možných následkov.

Rusko/Gruzínsko 2008

Rusko namiesto použitia „klasických" zbraní na zničenie komunikačných sietí použilo kyber operácie s nekinetickými účinkami, ktoré spôsobili narušenie a zabránenie prístupu k podstatným komunikačným sieťam, správam a vládnym stránkam, čo spôsobilo zmätok a stratu komunikácie, čím uľahčilo vojenské získanie územia a vyvolanie fyzickej ujmy.

9. Spôsoby riešenia a aktuálne otázky

Zložitou otázkou je aj reakcia na kyber útok. Keďže ide o netypický druh konania, aj obrana voči nemu je problematická, a to hlavne pre jeho špecifickosť (neviaže sa na územie, ale na kyberpriestor, rýchlosť začatia, malá predvídateľnosť, neznámy útočník, atď.). Prvým medzinárodnoprávnym riešením je obrátiť sa na porušiteľa, pričom napadnutý štát ho môže žiadať o odstránenie protiprávneho stavu, čo sa však v praxi môže ťažko uskutočniť, a to najmä pre vyššie spomenuté ťažkosti s identifikáciou útočníka. Ďalším riešením je obrátiť sa na súd. To úvahy prichádza Medzinárodný súdny dvor, ktorý však nemá povinnú jurisdikciu a nevzťahuje sa na prípady sporov, kde nie sú stranami štáty. Problémom môže byť aj založenie jeho právomoci. Je však možné požiadať ho o stanovisko.

Druhým spôsobom je oznámenie útoku Bezpečnostnej rade OSN. Bezpečnostná rada následne rozhodne, či ide o porušenie mieru alebo nie. Ak áno, príjme potrebné opatrenia. S obrátením sa na Bezpečnostnú radu súvisí aj výkon práva na sebaobranu, ktorý musí spĺňať kritériá nevyhnutnosti a proporcionality. Je možné ako sebaobranu voči kyber útoku použiť „klasický" spôsob, teda ozbrojenú silu? Domnievame sa, že áno, aj keď nie bezpodmienečne. Cieľom sebaobrany je zabrániť ďalšiemu pokračovaniu útoku, a ak je to možné a efektívne dosiahnuť použitím klasického útoku, medzinárodné právo by tomu nemalo brániť. Právo na sebaobranu prináleží len voči istej množine kyber útokov, ktorá spadá pod článok 51 Charty, teda nedá sa aplikovať všeobecne. Odpoveďou na kyber útok nemôže byť vždy použitie sily, ale iba v medziach podmienok uvedených vyššie. Ďalším spôsobom môžu byť prostriedky bez použitia sily, a to retorzie a protiopatrenia. Dôležitým prvkom na riešenie legálnej odpovede na kyber útok je spolupráca štátov, vytvorenie špecializovaných orgánov a jednotiek, ktoré sa zameriavajú na kyber útoky, šírenie informácií a prevenciu takéhoto druhu útokov.[29]

10. Záver

Hoci medzinárodnoprávna úprava často zaostáva voči skutočnému stavu, ak sa objaví nová oblasť, dosiaľ medzinárodnými normami neregulovaná, je nutné na expanziu kyber útokov reagovať. Ako jedným z možných riešení sa javí pripodobnenie kyber útoku ku klasickému ozbrojenému útoku, čím by sa tento nový druh konfliktu dal začleniť pod právo ozbrojených konfliktov, s čím súvisí jeho charakteristika ako agresie, ozbrojeného útoku

---

[28] Pozri bližšie v: Handler, S. G.: The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, Winter 2012, Vol. 48 Issue 1, s. 223.

[29] Podrobnejšie o možných riešeniach pozri Roscini, M.: World Wide Warfare - *Jus ad bellum* and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, Volume 14, 2010.

a samozrejme ich legálnych reakcií, ako je napr. sebaobrana. Charta OSN, kde je právo na sebaobranu zakotvené už viac ako 60 rokov, sa dokázala „prispôsobiť" zmenám bez zmeny jej textu, je však otázne, či sa tak môže udiať aj pri kyber útokoch, ktoré majú svoje odlišnosti a špecifiká, kvôli ktorým je nutné k nim pristupovať kvalitatívne inak. Najzákladnejším rozdielom je priestor, v ktorom sa odohrávajú, teda kyberpriestor, to znamená, že nejde o štátne hranice, územie štátov, sťažuje predvídateľnosť, identifikáciu útočníka, možnú odpoveď na kyberútok i pričítateľnosť konania. Je na praxi štátov, aby reagovaním na konkrétne kyber útoky vytvorili najprv obyčajové pravidlá, ktoré by neskôr mohli byť kodifikované.

Dohovor Rady Európy o počítačovej kriminalite
Oliver Buhala

1. Počítačová kriminalita

Informatizácia spoločnosti okrem množstva nesporných výhod súčasne prináša aj riziko zneužitia telekomunikačných a informačných technológií pre rôzne nelegálne účely. Neustále sa tiež rozširuje miera, frekvencia a paleta spôsobov akými k ich zneužívaniu dochádza. V 21. storočí tak spoločnosť čelí novému druhu kriminality – počítačovej kriminalite.

Prvý zaznamenaný prípad kybernetickej kriminality sa však datuje až do roku 1820, kedy francúzsky továrnik Joseph Maria Jacquard zostrojil prvý programovateľný, autonómne riadený tkáčsky stroj (možno hovoriť o počiatkoch softvéru). Jacquardovi zamestnanci, ktorí v obavách o svoje zamestnanie páchali sabotáže aby Jacquarda odradili od používania zariadenia, sa tak dopúšťali zrejme prvej „počítačovej" kriminality vôbec. Podoby počítačovej kriminality sú dnes neporovnateľne rozvinutejšie a sofistikovanejšie. Vznik internetu v 60-tych rokoch a začiatok masívneho využívania výpočtovej techniky verejnosťou v 90-tych rokoch so sebou priniesli aj vzostup rôznych foriem kybernetickej trestnej činnosti a tým aj potrebu právnej regulácie. Existuje niekoľko dôvodov, prečo podobné aktivity zaznamenávajú rapídny rozmach – cenová dostupnosť technológií, pocit anonymity, technologická nenáročnosť alebo rýchlosť vykonania operácie[1] sú len niektoré z nich.

Na označenie opísaného fenoménu sa používa niekoľko pojmov. Popri počítačovej kriminalite sa synonymicky narába s pojmami *IT kriminalita* alebo *kybernetická kriminalita*, v anglickej literatúre zase s výrazmi *cybercrime, computer crime, high-tech crime* a pod. Pokiaľ ide o definíciu pojmu zrejme najjednoduchšou je tá, ktorá vymedzuje počítačovú kriminalitu ako protiprávne konanie, pri ktorom počítač je nástrojom, cieľom alebo oboma. Od toho sa odvíja aj rozlišovanie dvoch základných skupín IT kriminality:

priama - protiprávne konania smerujúce k počítaču a

nepriama - protiprávne konania s využitím počítača.[2]

Pretože nie je geograficky obmedzené ani viazané štátnymi hranicami, môžu byť následky takéhoto konania o to ďalekosiahlejšie. Európske krajiny považujú túto formu trestnej činnosti za jednu z globálnych hrozieb a jedným z nástrojov na jej potieranie je Dohovor o počítačovej kriminalite z 23. novembra 2001.[3]

2. Dohovor Rady Európy o počítačovej kriminalite

2.1. História vzniku a signatári

Dohovor Rady Európy o počítačovej kriminalite, známy tiež ako Budapeštiansky dohovor o počítačovej kriminalite alebo jednoducho Budapeštiansky dohovor je dokument predstavujúci jediný mnohostranný zmluvný nástroj, ktorý obsahuje úpravu znakov skutkových podstát trestných činov v oblasti počítačovej kriminality, ako aj účinnej a rýchlej medziná-

---

1 OSTER, J.: Kriminalita v informačných technológiách. Dostupné na: http://zodpovedne.sk/kapitola4.php?cl=kriminalita_it.

2 ZÁHORA J.: Počítačová kriminalita v európskom kontexte. In: Justičná revue, 2/2005, s. 207.

3 Oficiálna webová stránka Ministerstva vnútra SR. Dostupné na: http://www.minv.sk/?pocitacedusevne.

rodnej spolupráce.[4] Výbor ministrov Rady Európy ho prijal na svojom 109. zasadnutí 8. novembra 2001. Následne bol dohovor otvorený na podpis v Budapešti 23. novembra 2001 a do platnosti vstúpil o necelé tri roky, 1. júla 2004.[5]

História dohovoru však siaha až do roku 1996 kedy sa Európsky výbor pre problémy kriminality (CDPC)[6] rozhodol zriadiť osobitný výbor expertov na počítačovú kriminalitu.[7] Uvedomujúc si, že cezhraničný charakter počítačových trestných činov je v rozpore s územnou pôsobnosťou vnútroštátnych orgánov vynucovania práva, sa CDPC vyjadril, že na jednanie s takýmto konaním je potrebné koordinované úsilie na medzinárodnej úrovni a aby bol tento boj účinný, je možné dosiahnuť iba záväzným medzinárodným nástrojom.

Na odporúčanie CDPC vo februári 1997 Výbor ministrov Rady Európy zriadil[8] Výbor expertov pre kriminalitu v kyberpriestore (PC-CY).[9] Výbor sa ujal rokovaní za účelom vypracovania Dohovoru o počítačovej kriminalite. Okrem členských štátov sa na rokovaniach zúčastnili aj štyri nečlenské štáty – Japonsko, Južná Afrika, Kanada a USA ako pozorovatelia. Dohovor bol vypracovaný v Štrasburgu a v súčasnosti má 51 zmluvných strán,[10] z toho 39 štátov ho aj ratifikovalo a 12 podpisov zatiaľ ostáva bez ratifikácie.[11] Slovenská republika k Dohovoru o počítačovej kriminalite pristúpila 23. novembra 2001, ratifikačná listina bola uložená u Generálneho tajomníka Rady Európy 8. januára 2008 a platnosť pre SR nadobudol dohovor 1. mája 2008.[12] Oznámenie Ministerstva zahraničných vecí Slovenskej republiky o podpísaní Dohovoru o počítačovej kriminalite bolo publikované pod číslom 137/2008 Z.z.

7. novembra 2002 prijal Výbor ministrov rady Európy Dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov. Na podpis bol otvorený 28. januára 2003 v Štrasburgu. K súčasnosti k nemu pristúpilo 36 štátov, z toho 20 protokol aj ratifikovalo. Slovenská republika k signatárom dodatkového protokolu nepatrí. Je vhodné povedať, že ratifikácia samotného Dohovoru o počítačovej kriminalite nezaväzuje ratifikujúci štát prijať akékoľvek opatrenia vo vzťahu k dodatkovému protokolu.[13]

---

4 Slovensko ratifikuje Dohovor o počítačovej kriminalite. Dostupné na: http://www.sme.sk/c/3420242/slovensko-ratifikuje-dohovor-o-pocitacovej-kriminalite.html.

5 Aby vstúpil do platnosti bola potrebná ratifikácia dohovoru aspoň 5 štátmi, z ktorých aspoň 3 sú členmi Rady Európy v súlade s čl. 36, ods. 3 Dohovoru o počítačovej kriminalite.

6 European Committee on Crime Problems.

7 Rozhodnutie č. CDPC/103/211196.

8 Rozhodnutie č. CM/Del/Dec(97)583.

9 Committee of Experts on Crime in Cyber-space.

10 Zmluvné štáty zároveň členmi Komisie Dohovoru o počítačovej kriminalite - Cybercrime Convention Committee (T-CY).

11 44 zo 47 členských štátov Rady Európy: Albánsko, *Andorra*, Arménsko, Azerbajdžan, Belgicko, Bosna a Hercegovina, Bulharsko, Chorvátsko, Cyprus, *Česká republika*, Čierna Hora, Dánsko, Estónsko, Fínsko, Francúzsko, *Grécko*, Gruzínsko, Holandsko, Island, *Írsko*, *Lichtenštajnsko*, Litva, Lotyšsko, *Luxembursko*, Macedónsko, Maďarsko, Malta, Moldavsko, *Monako*, Nemecko, Nórsko, *Poľsko*, Portugalsko, Rakúsko, Rumunsko, Slovensko, Slovinsko, Srbsko, Španielsko, Švajčiarsko, *Švédsko*, Taliansko, *Turecko*, Ukrajina, Veľká Británia + 6 nečlenských štátov: Austrália, Dominikánska republika, *Kanada*, Japonsko, *Južná Afrika*, USA. Kurzívou sú vyznačené bez ratifikácie. (Údaj ku dňu 5.5.2013).

12 V zmysle čl. 36, ods. 4 Dohovoru o počítačovej kriminalite.

13 National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press, 2010.

2.2. Koncepcia a východiskové ciele

Samotný Dohovor o počítačovej kriminalite tvorí Preambula a 4 kapitoly, obsahujúce celkovo 48 článkov. Koncepcia dohovoru je nasledovná:

Preambula

Kapitola I – Použitie pojmov (čl. 1)

Kapitola II – Opatrenia, ktoré je potrebné prijať na vnútroštátnej úrovni

Oddiel 1 – Trestné právo hmotné (5 hláv: čl. 2 – 13)

Oddiel 2 – Procesné právo (5 hláv: čl. 14 – 21)

Oddiel 3 – Právomoc (čl. 22)

Kapitola III – Medzinárodná spolupráca

Oddiel 1 – Všeobecné zásady (4 hlavy: čl. 23 – 28)

Oddiel 2 – Osobitné ustanovenia (3 Hlavy: čl. 29 – 35)

Kapitola IV – Záverečné ustanovenia (čl. 36 – 48)

Problémy, ktoré dohovor upravuje, je možné rozdeliť do akýchsi troch základných okruhov:

- počítačové trestné činy,
- vyšetrovacie postupy,
- medzinárodná spolupráca.[14]

2.2.1 Počítačové trestné činy

Jednou z úloh, ktoré dohovor plní je harmonizácia vnútroštátnych trestnoprávnych úprav skutkových podstát a súvisiacich ustanovení v oblasti počítačovej kriminality.[15] Úprava sa týka 9 trestných činov rozdelených do 4 kategórií a nachádza sa v článkoch 2 až 11.

Kategóriu ***trestných činov proti dôvernosti, hodnovernosti a dostupnosti počítačových systémov*** tvorí:

Nezákonný prístup - neoprávnený prístup do počítačového systému ako celku alebo do jeho časti.

Nezákonné zachytenie údajov - neoprávnené zachytávanie neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v rámci tohto systému vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje také počítačové údaje vykonané technickými prostriedkami.

Zasahovanie do údajov - neoprávnené poškodenie, vymazanie, zhoršenie kvality, pozmenenie počítačových údajov alebo zamedzenie prístupu k nim.

Zasahovanie do systému - neoprávnené závažné marenie funkčnosti počítačového systému vkladaním, prenášaním, poškodením, vymazaním, zhoršením, pozmenením počítačových údajov alebo zamedzenie prístupu k nim.

Zneužitie zariadení - výroba, predaj, obstarávanie na účely použitia, dovoz, distribúcia alebo iné sprístupnenie prípadne držba zariadenia vrátane počítačového programu vytvo-

---

[14] National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press, 2010.

[15] Dôvodová správa k Dohovoru o počítačovej kriminalite, bod 16. Dostupné na: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

reného alebo upraveného predovšetkým s cieľom spáchať niektorý z vyššie uvedených z trestných činov. A výroba, predaj, obstarávanie na účely použitia, dovoz, distribúcia alebo iné sprístupnenie prípadne držba počítačového hesla, prístupového kódu alebo podobných údajov, ktorých pomocou je možný prístup do počítačového systému ako celku alebo niektorej jeho časti, s úmyslom ich použiť na spáchanie niektorého z trestných činov uvedených vyššie.

Druhou je skupina tzv. ***počítačových trestných činov***. Patrí tu:

Falšovanie počítačových údajov- vloženie, pozmenenie, vymazanie počítačových údajov alebo zamedzenie prístupu k nim, v ktorých dôsledku stratia údaje autentickosť, s úmyslom považovať ich za autentické alebo aby sa na základe nich ako autentických údajov konalo, na právne účely, bez ohľadu na to, či tieto údaje sú alebo nie sú priamo čitateľné alebo zrozumiteľné

Počítačový podvod- spôsobenie majetkovej ujmy inému vložením, pozmenením, vymazaním počítačových údajov alebo zamedzením prístupu k nim, zásahom do fungovania počítačového systému s podvodným alebo nečestným úmyslom neoprávnene získať pre seba alebo pre iného majetkový prospech

Tretia je skupina ***trestných činov týkajúcich sa obsahu***:

Trestné činy týkajúce sa detskej pornografie- výroba za účelom distribúcie, ponuka alebo sprístupnenie, distribúcia alebo prenos, zaobstarávanie detskej pornografie počítačovým systémom pre seba alebo pre iného, držba detskej pornografie v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov

Osobitnú, štvrtú kategóriu tvoria ***trestné činy týkajúce sa porušenia autorských práv a príbuzných práv***:

Porušenie autorského práva alebo príbuzného práva vymedzeného právnym poriadkom zmluvnej strany

Štát zmluvnej strany je rovnako povinný kriminalizovať pokus, napomáhanie a navádzanie na ktorýkoľvek z vyššie uvedených trestných činov. Dohovorom sa takisto zaviedla zodpovednosť právnických osôb[16] za ním vymedzený trestný čin, ak ho spáchala fyzická osoba samostatne alebo ako súčasť orgánu právnickej osoby a ktorá má v nej vedúce postavenie. Zodpovednosť právnickej osoby sa zakladá aj v prípade, ak nedostatočný dohľad alebo kontrola vyššie spomenutej fyzickej osoby umožnili spáchanie trestného činu podľa dohovoru. Ratifikujúci štát pritom môže určiť, či zodpovednosť takto vzniknutá bude trestnoprávna, občianskoprávna alebo administratívnoprávna. Cieľom dohovoru je, aby jednotlivé zmluvné strany ustanovili, aby tieto trestné činy boli trestnými činmi aj podľa ich vnútroštátneho práva. Úprava dohovorom nevylučuje prípadné rozšírenie zoznamu trestných činov v oblasti IT kriminality domovským právom štátov. Strana má takisto určitý priestor na podmienenie trestnosti konania uvedeného v dohovore – napr. strana si môže vyhradiť právo vyžadovať, aby následkom konania bola značná škoda a pod.

Trestnosť všetkých z uvedených činov dohovor podmieňuje prvkom úmyselného zavinenia, a teda nepozná trestné činy spáchané z nedbanlivosti. Vymedzenie úmyslu (čo to úmysel je) je ponechané interpretácii jednotlivých zmluvných strán. Okrem toho, vo vzťahu k jednotlivým skupinám trestných činov dohovor pripája aj iné podmienky trestnosti. Čo sa týka sankcií a opatrení,[17] aj tu vznikajú štátom isté povinnosti. Zmluvná strana je preto zaviazaná prijať potrebné legislatívne a iné opatrenia aby spomenuté trestné činy boli

---

16 Pozri čl. 12 Dohovoru o počítačovej kriminalite.

17 Pozri čl. 13 Dohovoru o počítačovej kriminalite.

trestané účinnými, primeranými a odrádzajúcimi sankciami vrátane odňatia slobody. Vo vzťahu k zodpovednosti právnických osôb je nutné, aby tieto (ak ich zodpovednosť vznikla) podliehali účinným, primeraným a odrádzajúcim trestnoprávnym, občianskoprávnym alebo správnym sankciám alebo opatreniam vrátane peňažných sankcií. Takéto zosúladenie trestnoprávnej úpravy, má význam na úrovni národnej aj medzinárodnej. Pokiaľ na úrovni jednotlivých štátov sa má zamedziť tomu, aby bolo zneužívanie počítačových systémov presmerované do štátov s nižším štandardom úpravy, na medzinárodnej úrovni ide o uľahčenie v oblasti vzájomnej právnej pomoci alebo extradície v súvislosti s požiadavkami obojstrannej trestnosti.

2.2.2. Vyšetrovacie postupy

Druhým významným aspektom, na ktorý sa dohovor zameriava je zakotvenie procesných mechanizmov a postupov za účelom uľahčenia vyšetrovania a trestného stíhania počítačových trestných činov, ako aj ďalších trestných činov spáchaných prostredníctvom počítača alebo činov, ktorých dôkazy je možné získať v elektronickej forme. Tu si treba uvedomiť, že mnoho z procesných ustanovení dohovoru nie je obmedzených na kybernetické trestné činy, ale týkajú sa akéhokoľvek trestného činu, pre ktorý je možné získavanie dôkazov v elektronickej forme. V tomto duchu je samotný názov „Dohovor o počítačovej kriminalite“ do istej miery zavádzajúci. V súlade s s článkami 14 až 21 sú ratifikujúce štáty povinné vybaviť svoje príslušné orgány hneď niekoľkými právomocami:

- nariadiť urýchlené uchovanie určených počítačových údajov, vrátane prevádzkových údajov, pri existencii rizika ich straty alebo pozmenenia,
- uložiť povinnosť osobe uchovať a udržať určené dáta (na čas najviac 90 dní),
- zabezpečiť urýchlený prístup k prevádzkovým údajom v dostatočnom množstve umožňujúcom im identifikovať prevádzkovateľa služieb a trasu prenosu komunikácie,
- nariadiť osobe v ich územnej pôsobnosti predloženie určených počítačových údajov,
- nariadiť poskytovateľovi služieb v ich územnej pôsobnosti predloženie informácií o odberateľovi jeho služieb,
- vykonať prehliadku a zaistenie počítačového systému, pamäťového nosiča a údajov v nich obsiahnutých,
- zhromažďovať alebo zaznamenávať prevádzkové údaje v reálnom čase prenášané v rámci určenej komunikácie na svojom území alebo k tomu prinútiť poskytovateľa služieb, prípadne ho donútiť k spolupráci a pomoci príslušným orgánom v tejto veci.

Vo vzťahu ku skupine závažných trestných činov[18] zhromažďovať alebo zaznamenávať obsahové údaje v reálnom čase prenášané v rámci určenej komunikácie na svojom území alebo k tomu prinútiť poskytovateľa služieb, prípadne ho donútiť k spolupráci a pomoci príslušným orgánom v tejto veci. K problematike právomoci[19] dohovor zaväzuje strany prijať legislatívne alebo iné opatrenia, aby mala právomoc konať o trestných činoch,[20] ktoré boli spáchané:

- na jej území,
- na palube lode plávajúcej pod vlajkou tejto strany,
- na palube lietadla registrovaného podľa právneho poriadku tejto strany,
- jej občanom, ak je tento čin trestný podľa právneho poriadku miesta, kde bol spáchaný alebo ak miesto spáchania trestného činu nie je územím žiadneho štátu.

---

18 Tieto zmluvná strana vymedzí vo svojom vnútroštátnom poriadku.
19 Pozri čl. 22 Dohovoru o počítačovej kriminalite.
20 Pozri časť 2.2.1.

Vo vzťahu k bodom b., c. a d. si môže strana určiť výnimky pri uplatňovaní pôsobnosti, nemôže to však urobiť vo vzťahu k písmenu a. Ak sa páchateľ nachádza na jej území a zároveň ho z dôvodu štátneho občianstva nevydala druhej strane, musí mať právomoc v danej veci konať. Kľúčovým je tu princíp *aut dedere aut judicare* - vydať alebo stíhať. Problém v súvislosti s vyšetrovaním a stíhaním počítačovej kriminality vzniká na dvoch úrovniach. Tou prvou je štrukturálna úroveň, vyjadrená konfliktom globálneho charakteru internetu na jednej a štátnymi hranicami obmedzenej pôsobnosti štátov na druhej strane. Druhou je technická úroveň, charakterizovaná nestálou povahou počítačových údajov, ktoré je možné zmeniť, doplniť alebo presunúť v priebehu niekoľkých sekúnd. V dôsledku toho existuje značné riziko straty dôkazového materiálu.

Dohovorom bolo potrebné tieto problémy prekonať. Nakoľko zásada právneho konzervativizmu medzi štátmi neumožnila vytvorenie medzinárodnej kyberpolície, prípadne zverenie univerzálnej jurisdikcie národným súdom, dohovorom zavedené reguláty v oblasti procesného práva sú iba na vnútroštátnej úrovni. Pri zavádzaní procesných ustanovení, musí každý zmluvný štát zabezpečiť, aby podliehali zárukám jeho vnútroštátneho poriadku a teda primeranej ochrane základných ľudských práv a slobôd a neodporovali zásade proporcionality. Aj tieto ustanovenia predstavujú minimálnu úpravu a nevylučujú rozšírenie spektra procedurálnych opatrení jednotlivými zmluvnými stranami.

2.2.3. Medzinárodná spolupráca

Tretia oblasť Dohovoru o počítačovej kriminalite je určená na vytvorenie podmienok priaznivých pre vzájomnú asistenciu zmluvných strán pri vyšetrovaní počítačových trestných činov, resp. trestných činov zahŕňajúcich dôkazový materiál v elektronickej forme. Takáto spolupráca sa má uskutočňovať prostredníctvom príslušných medzinárodných nástrojov na medzinárodnú spoluprácu v trestných veciach, dojednaní prijatých na základe vzorového zákona alebo vzájomnosti a vnútroštátnych zákonov, a to v čo najväčšom rozsahu.[21] Prierez úpravy obsiahnutej v článkoch 24 až 35 vyzerá asi takto:

Extradícia. Ide o významný inštitút, na základe ktorého sa trestné činy upravené v dohovore stávajú extradičnými činmi. Vydanie medzi stranami je možné, ak za trestný čin vymedzený v dohovore právne poriadky oboch dotknutých strán umožňujú uložiť trest odňatia slobody alebo ochranné opatrenie s hornou hranicou najmenej jeden rok alebo prísnejší trest. Samotná extradícia však podlieha podmienkam stanoveným predpismi dožiadanej strany alebo príslušnými zmluvami o vydávaní, vrátane dôvodov, kedy možno vydanie odmietnuť. Ak strana odmietne vydanie osoby z dôvodu štátnej príslušnosti alebo z dôvodu domnienky, že má nad prípadom právomoc, je povinná na žiadosť dožadujúcej sa strany predložiť prípad svojim orgánom na účely trestného stíhania a o výsledku podá dožadujúcej sa strane správu (*aut dedere aut judicare*). Ak medzi stranami neexistuje extradičná zmluva, je možné považovať za právny základ vydania samotný dohovor. Strany musia pri vyšetrovaní počítačových trestných činov, resp. trestných činov zahŕňajúcich dôkazový materiál v elektronickej forme poskytnúť pomoc v čo najširšom meradle. To znamená, že musia prijať a reagovať na žiadosti o právnu pomoc a s tým súvisiacu korešpondenciu. Štáty však môžu odmietnuť spoluprácu na základe akéhokoľvek dôvodu vyplývajúceho z jej vnútroštátneho práva alebo zmlúv o právnej pomoci. Pomoc nie je možné odmietnuť ak sa žiadosť týka fiškálneho trestného činu. Strana môže bez predchádzajúcej žiadosti, kedykoľvek zaslať inej strane informácie získané počas vyšetrovania ak sa domnieva, že by to druhej strane mohlo pomôcť pri vyšetrovaní kybernetickej kriminality.

---

21 Pozri čl. 23 Dohovoru o počítačovej kriminalite.

Ak strany medzi sebou nemajú existujúcu zmluvu o vzájomnej právnej pomoci alebo iné dojednanie, je potrebné aby každá strana vytvorila ústredný orgán, ktorý zodpovedá za zasielanie, odpovedanie a vybavovanie žiadostí o právnu pomoc alebo ich predkladá orgánom príslušným na ich vybavenie.[22] Zoznam týchto ústredných orgánov vedie Generálny tajomník Rady Európy. Vybavovanie žiadostí prebieha v súlade s postupmi určenými dožadujúcou stranou (ak nie sú nezlučiteľné s právnym poriadkom dožiadanej strany). Za pozornosť stojí, že dohovor dáva strane možnosť odmietnuť pomoc nielen z dôvodu vyplývajúceho z jej vnútroštátneho práva alebo zmlúv o právnej pomoci, ale tiež ak považuje trestný čin, o ktorý sa jedná, za politický trestný čin, prípadne čin s politickým trestným činom súvisiaci a ak má za to, že vybavením žiadosti by došlo k narušeniu jej suverenity, bezpečnosti, verejného poriadku alebo iných zásadných záujmov. Toto ustanovenie umožňuje značne široký výklad a teda vytvára rozsiahly priestor pre potenciálne odmietnutie právnej pomoci.

Strana môže požiadať inú stranu aby zabezpečila urýchlené uchovanie dát uložených prostredníctvom počítačového systému na jej území, vo vzťahu ku ktorým má záujem žiadať o prehliadku, zaistenie alebo sprístupnenie. Následné uchovanie dát trvá po dobu min. 60 dní. Aj v tomto prípade má strana možnosť odmietnuť takúto žiadosť ak sa domnieva, že ide o politický trestný čin alebo by došlo k narušeniu jej suverenity, bezpečnosti, verejného poriadku alebo iných zásadných záujmov. Strana má povinnosť vybaviť žiadosť na vykonanie prehliadky, zaistenia alebo sprístupnenia takto uchovaných údajov. Strana môže pristupovať k verejne dostupným zdrojom dát a prijímať dáta uložené na území inej strany, ak má súhlas osoby, ktorá je oprávnená ich sprístupniť. Strany si poskytnú vzájomnú pomoc pri zhromažďovaní prevádzkových údajov v reálnom čase. Táto pomoc sa riadi predpismi vnútroštátneho práva, avšak strany sú povinné ju poskytnúť aspoň vtedy, ak by bolo zhromažďovanie prevádzkových údajov v reálnom čase možné v podobnom vnútroštátnom prípade. Zmyslom tohto ustanovenia je umožniť vystopovať zdroj útoku počas trvania prenosu. Strany si poskytnú pomoc aj pri zhromažďovaní obsahových údajov určených komunikácii v reálnom čase.

Sieť 24/7. Strana je povinná zriadiť kontaktné miesto dostupné 24 hodín denne, 7 dní v týždni určené na poskytovanie okamžitej pomoci pre účely vyšetrovania alebo konania v prípade trestných činov súvisiacich s počítačovými systémami alebo údajmi alebo na účel zhromažďovania dôkazov o trestnom čine v elektronickej forme.[23] Obsahom tejto pomoci je uľahčenie, resp. priame vykonanie (ak je to umožnené vnútroštátnym právnym poriadkom) technického poradenstva, uchovávania údajov, zhromažďovania dôkazov, poskytovania právnych informácií alebo lokalizovania podozrivých osôb. Strana taktiež zaistí vyškolený personál a potrebné vybavenie.

3. Dodatkový protokol k Dohovoru o počítačovej kriminalite

Pri zostavovaní Dohovoru bola diskutovaná možnosť obsiahnuť do neho v rámci trestných činov týkajúcich sa obsahu aj šírenie rasistickej propagandy prostredníctvom počítačového systému. Pretože v otázke kriminalizácie konania tohto charakteru nebola dosiahnutá zhoda, stala sa obsahom Dodatkového protokolu k Dohovoru o počítačovej kriminalite týkajúceho sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostred-

---

22 V prípade SR tieto úlohy plní Ministerstvo spravodlivosti a Generálna prokuratúra.

23 V prípade SR túto úlohu plní Prezídium policajného zboru, Úrad medzinárodnej policajnej spolupráce a Národná ústredňa Interpol Bratislava.

níctvom počítačových systémov. Vypracovaný bol Výborom expertov na kriminalizáciu aktov rasistickej a xenofóbnej povahy (PC- RX).[24]

Protokol rozširuje zoznam činov v oblasti počítačovej kriminality o:

- šírenie rasistických a xenofóbnych materiálov prostredníctvom počítačových systémov,
- rasisticky a xenofóbne motivované vyhrážanie,
- rasisticky a xenofóbne motivované urážanie,
- popieranie, hrubé zľahčovanie, schvaľovanie alebo ospravedlňovanie zločinov proti ľudskosti.

Trestným činom v zmysle Protokolu je aj napomáhanie a navádzanie na spáchanie niektorého z týchto trestných činov. Aj pri týchto činoch je podmienkou trestnosti úmyselné spáchanie. Prijatím protokolu sa rozširujú procesné ustanovenia a ustanovenia týkajúce sa medzinárodnej spolupráce stanovené dohovorom na činy, ktorých výpočet priniesol dodatkový protokol. Niektoré články dohovoru sú platné mutatis mutandis pre protokol.[25]

4. Riešenie sporov

Dohovor nezavádza žiadny mechanizmus per se na zabezpečenie plnenia záväzkov, ktoré stranám z dohovoru vznikajú.[26] Štáty preto priebežne poskytujú informácie o výklade a uplatňovaní dohovoru Európskemu výboru pre problémy kriminality (CDPC). V prípade sporu pri vykladaní alebo uplatňovaní strany pristúpia k rokovaniam alebo iným zmierlivým prostriedkom urovnania, vrátane predloženia sporu CDPC, rozhodcovskému súdu alebo Medzinárodnému súdnemu dvoru.[27]

Záver

Samotná povaha počítačovej kriminality z nej robí problém predurčený na reguláciu medzinárodným právom, z čoho plynie potreba prijímať zodpovedajúce právne nástroje na medzinárodnej úrovni. Napriek tomu, že dohovor vznikol na pôde Rady Európy ako regionálnej medzivládnej organizácie, nemá striktne regionálnu povahu. Práve naopak, aby bolo skutočne naplnené jeho poslanie je nevyhnutné, aby k dohovoru pristúpilo čo najviac štátov medzinárodného spoločenstva. Možno konštatovať, že štáty zúčastnené na rokovaniach nepredstavujú naozaj problémové krajiny. Páchatelia často smerujú svoje útoky cez portály v krajinách, ktoré nie sú zmluvnými stranami dohovoru (napr. KĽDR alebo Jemen).

Masívna kritika sa na dohovor zniesla zo strany rôznych občianskych skupín, ktoré sa domnievajú, že kontrolné právomoci zachádzajú priďaleko čo spôsobuje znepokojenie pokiaľ ide o právo na súkromie. V Európe sa objavili obavy z migrácie osobných údajov do mimoeurópskych krajín, ktoré však boli zo strany predstaviteľov Rady Európy odmietnuté, pričom argumentovali, že dohovor poskytuje dostatočné záruky ochrany občianskych práv a limitácie pokiaľ ide o prenos informácií. Niektorí sa nazdávajú, že dohovor prináša prílišné zvýšenie nákladov pre poskytovateľov služieb, bráni rozvoju bezpečnostných technológií a podobne.

---

24 Committee of Experts on the Criminalization of Acts of a Racist and xenophobic Nature committed through Computer Systems.

25 Články: 1, 12, 13, 22, 41, 44, 45 a 46.

26 National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press, 2010.

27 Pozri čl. 45 Dohovoru o počítačovej kriminalite.

Výsledkom *Octopus Conference*[28] v roku 2011 bola celková zhoda, že napriek kritike dohovor poskytuje jediný efektívny a praktický nástroj na boj s globálnou on- line kriminalitou.[29] Faktom ostáva, že reprezentuje významný počin v boji s počítačovou kriminalitou. Je to jediná existujúca multilaterálna zmluva konkrétne riešiaca počítačovú kriminalitu a zhromažďovanie elektronických dôkazov.[30] Predstavitelia Rady Európy tvrdia, že sankcie a status počítačových trestných činov ako činov extradičných, zníži počet krajín, v ktorých sa páchatelia môžu vyhnúť trestnému stíhaniu. Existujú aj názory, že procesné ustanovenia týkajúce sa zabezpečovania dôkazov môžu napomôcť v boji s terorizmom. Tak či onak, Dohovor o počítačovej kriminalite predstavuje istý paradox kedy Rada Európy, ako organizácia zameraná predovšetkým na ochranu ľudských práv vypracovala zmluvu, ktorej procesné mechanizmy umožňujú štátnej moci nemalé zásahy do súkromia občanov.

---

28 Ide o konferenciu organizovanú Radou Európy zameranú na kooperáciu v boji proti počítačovej kriminalite.

29 Ten Years On: The Budapest Convention – A Common Force Against Cybercrime. Dostupné na: http://news.hostexploit.com/cyber-security-news/5023-ten-years-on-the-budapest-convention-a-common-force-against-cybercrime.html.

30 Henrik Spang-Hanssen, The Future of International Law: CyberCrime (2008). Dostupné na: http://ssrn.com/abstract=1090876.

Návrhy na vytvorenie medzinárodného súdneho orgánu pre počítačovú kriminalitu
Simona Masicová

Úvod

Jednou z najväčších globálnych hrozieb v súčasnosti je spoločenský fenomén nazývaný počítačová kriminalita, obsahom ktorej sú kyberútoky zamerané proti kritickým informáciám infraštruktúry. Zjednodušene povedané sa jedná o trestné činy zamerané proti počítačom alebo páchané pomocou počítača, čo v konkrétnejšej koncepcii môže predstavovať napríklad napadnutie systému a neoprávnené získanie a zneužitie údajov a utajovaných informácií, počítačové podvody, krádež počítača, programu, komunikačného zariadenia, šírenie poplašných správ a ďalšie. Pre niektoré druhy kyberkriminality sa v medzinárodnom spoločenstve ustálili známe pojmy, ako napríklad:

Hacking[1] - prenikanie do cudzích počítačov a počítačových systémov inou než štandardnou cestou,

Warez (počítačové pirátstvo) - časť skupiny odstraňuje resp. blokuje ochranné prvky diel chránených autorským právom, zatiaľ čo druhá časť skupiny pomocou často vlastných serverov a webstránok šíri tieto diela zbavené ochrany za účelom zisku,

Cracking - neoprávnený zásah alebo úprava softvéru za účelom odstránenia alebo zablokovania jeho určitých funkcií, ktoré sú páchateľom považované za nežiaduce, nakoľko ich účelom je často ochrana pred neoprávneným šírením softvéru,

Sniffing - neoprávnené odpočúvanie, resp. zachytávanie komunikácie na sieti, ktorého účelom je monitoring diania na sieti, zachytávanie hesiel, čítanie cudzích emailov, správ a pod.

Počítačová kriminalita predstavuje veľkú hrozbu pre organizácie, krajiny samotné a v konečnom dôsledku medzinárodné nebezpečenstvo ako také. Jej rapídny rozmach, priamo úmerný informatizácii spoločnosti, je primárne výsledkom skutočnosti, že tento druh kriminality predstavuje veľmi jednoduchý a pohodlný spôsob realizácie zločincov ako kauzálny dôsledok jeho statusu veľmi ťažko riešiteľného druhu kriminality. Totiž pri kyberútokoch je skutočne problematické získať potrebné stopy a následne vypátrať zločincov. Pretože sa tu nejedná o klasické stopy, ako pri iných zločinoch, ale o tzv. digitálne stopy,[2] ktoré páchateľovi podstatne zjednodušujú zahladenie zmien spôsobených spáchaním činu. Okrem toho tu ide o to, že zločinec nepotrebuje zbrane ani žiadne násilie k vykonaniu činu, nemusí byť ani prítomný na danom mieste v danej krajine, z pohodlia utajeného miesta často krát behom niekoľkých sekúnd uskutoční kyberútok. Aj takýto deficit fyzickej prítomnosti na mieste činu spôsobuje výrazne sťaženie vyšetrovania, následnú absenciu sankcionovateľnosti (kyberútoky sa často krát označujú za zločiny, ktoré ostávajú nepotrestané) a ak sa k tomu pridá pohodlnosť a jednoduchosť uskutočnenia zločinu, je rozmach kyberkriminality zjavný. Preto vznikajú iniciatívy na riešenie tohto problému, príkladom čoho je vytvorenie návrhu na zavedenie medzinárodného súdneho orgánu pre počítačovú kriminalitu, na ktorý je táto práca zameraná.

---

1 LUKIČ, L.: Základne formy pocitacovej kriminality, najpravo.sk, 21. 10. 2012, dostupné online: http://www.najpravo.sk/clanky/zakladne-formy-pocitacovej-kriminality.html.

2 HUDEC, L..: Riesenie pocitacovych bezpecnostnych incidentov.

1. Prípady kyberkriminality

Útok na Estónsko:

Veľmi známym je útok Ruska na estónske servery a ich komunikačnú sieť, čomu predchádzalo odstránenie komunistických pamätníkov z Tallinu, ktoré pobúrilo tisíce Rusov žijúcich v Estónsku, no aj Rusov mimo neho. Reakciou na to bol masívny kyberútok, ktorému sa nevyhli banky, estónske média ani veľké spoločnosti. Cieľom bolo predovšetkým znefunkčniť internetové stránky, čo sa podarilo napr. v prípade ministerstva zahraničia a ministerstva spravodlivosti, televíznych staníc a estónskych organizácií. Útok spôsobil natoľko závažné škody, že sa tým zaoberala aj estónska vláda, a preto bolo viacero severov dočasne odrezaných od sveta.[3]

Útok Sýrskych hackerov:

Jedným z posledných a najnovších príkladov je nový prípad z roku 2013, kedy Sýrsky hackeri zaútočili na mediálne organizácie v západných krajinách, ako BBC, France 24 TV a National Public Radio v Spojených štátoch, britské noviny The Guardian, či jednotlivé Twitter účty ako aj útok na vládu Kataru. Predpokladá sa, že cieľom je demonštrácia podpory úradujúceho sýrskeho prezidenta Bašára Asada.[4]

Ich zatiaľ posledným útokom bolo napadnutie Twitter konta tlačovej agentúry Associated Press (AP), kde zverejnili, že prezident Obama bol zranený bombovým útokom v bielom dome. Správa sa rozšírila veľmi rýchlo a vyvolala veľký rozruch na burze, spôsobila pokles akciových trhov o 1%.

Iné:

V roku 2004 skupina hackerov v Rumunsku získala prístup k počítačom, ktoré riadia systémy na ochranu života vo výskumnej stanici v Antarktíde. Vinníci síce boli zastavení ešte predtým, ako k uskutočneniu došlo, no ak by ich misia bola úspešná, boli by ohrozené životy 58 ľudí.[5] Škodlivé následky kyberútokov demonštruje aj prípad Austrálčana, ktorý sa nabúral do systému odpadového hospodárstva v Queenslande iba preto, lebo mu zamietli žiadosť do agentúry. Jeho činnosť viedla k úniku miliónov odpadovej vody do rieky, miestnych parkov a do okolia hotelu Hyatt Regency. Podobných príkladov je veľmi veľa, spôsobujú závažné problémy a výrazne komplikujú fungovanie medzinárodného spoločenstva.

2. Dôvody legitímnosti vytvorenia návrhov a zavedenia tribunálu

S rastúcou kvantitou kyberútokov úmerne k tomu eskaluje aj potreba ich riešenia a vyporiadavania sa so zločincami. Je nesporné a spoločnosťou vysoko podporované a žiadané, aby sa vzhľadom na nebezpečný charakter a status mimoriadnej hrozby, počítačová kriminalita eliminovala a odstránila sa nepríjemná skutočnosť v podobe nepotrestaných kyber zločinov, ktoré predstavujú tak nebezpečný spoločenský fenomén. Avšak súčasným stavom sa to nedocieli, ten je neúčinný v boji s počítačovou kriminalitou, a preto je potrebné zaviesť nový systém na riešenie spomínanej problematiky. Schojberg na to reaguje plánom tribunálu, ktorý by mal nedostatky odstrániť.

Teda prvým dôvodom jeho potreby a zároveň dôvodom potreby inovácie v riešení problému je spomínaná skutočnosť, že **status QUO je neefektívny a nedostatočný**. To je zaprí-

---

3 Kybernetický útok Ruska na Estonsko, Zvědavěc, 22. 5. 2007, dostupný online: http://www.zvedavec.org/pohledy/2007/05/2066-kyberneticky-utok-ruska-na-estonsko.htm.

4 Stačil jeden falošný tweet a Wall Street padol, SME, 24. 4. 2013, dostupné online: http://www.sme.sk/c/6779402/stacil-jeden-falosny-tweet-a-wall-street-padol.html.

5 www.intellectualtakeout.org, Cyber attack frequently asked questions.

činené tým, že kyberútoky často krát riešia dotknuté štáty samotné, pričom participácia predstavuje vydávanie páchateľov a vzájomnú právnu pomoc. Avšak v mnohých prípadoch to predstavuje ťažko dosiahnuteľné prostriedky z toho titulu, že štáty majú mnoho krát problém so získavaním dôkazov, dostatočne relevantných a so samotným odhalením páchateľov. Ide o to, že v oblasti počítačovej kriminality je omnoho ťažšie vypátrať zločinca, nakoľko sa nejedná o bežné stopy ako pri klasických trestných činoch, ale v tomto prípade ide o tzv. digitálne stopy, ktoré sú náročnejšie na vypátranie a získanie. Oblasť počítačovej kriminality je nebezpečná, okrem iného, aj z dôvodu miesta pobytu páchateľa v čase vykonania činu. Nachádza sa často krát v inej krajine, ako v tej, v ktorej ku následkom konania dôjde, a teda je skutočne problematické vypátrať takéhoto zločinca, ktorý sa fyzicky nenachádza v okolí miesta činu. Preto štáty takmer vo všetkých prípadoch zlyhávajú vo vyriešení útokov a v ich efektívnom odstraňovaní.

Okrem toho je problematické, že štáty riešia situáciu prostredníctvom vlastnej legislatívy, čo môže vyvolať nedostatok vôle stíhať vlastných občanov, určitým spôsobom dehonestovať seba ako štát. Tvrdí to aj sudca Stein Schojberg, že by s týmto štáty mohli mať problém, a ak skutočne takáto hrozba existuje, tak je legitímne povedať, že súčasný stav môže byť neúčinný a kontraproduktívny a že by bolo omnoho prospešnejšie zaviesť nezávislý, objektívny súdny orgán. V súvislosti s vlastnou legislatívou je potrebné spomenúť aj to, že počas existencie štátu môžu nastať rôzne situácie ako napríklad zrútenie súdneho systému danej krajiny a podobne. V takejto situácii by bolo skutočne problematické efektívne vyriešiť útok v oblasti kyberpriestoru.

Ďalším determinantom predpokladu na začiatku spomínaného je fakt, že *Convention on Cybercrime*, teda istý dohovor o počítačovej kriminalite, nerieši situáciu dostatočne. Pokrýva totiž iba niektoré druhy počítačovej kriminality a okrem toho je založený na terminológii z roku 1990, ktorá nezodpovedá súčasnosti v plnom rozsahu.

Tieto spomínané skutočnosti spôsobujú ďalší dôvod potreby vytvorenia súdneho orgánu, a to fakt, že v súčasnom modeli mnohé kyberútoky ostávajú nepotrestané. Explicitne to opisuje aj sudca Stein Schojberg, že bez existencie medzinárodného orgánu ostanú kyberútoky nepotrestané, čo je obrovský problém, ktorý iba prehlbuje silu a rozmach počítačovej kriminality. Totiž ak to ostáva v rovine nepotrestania, tak tým pádom je tu značný deficit, ba dokonca úplná absencia nejakej hrozby, prekážky pre eventuálneho páchateľa. Skutočne ho nič neodradí, keď vie, že súčasný systém je tak neefektívny, že za svoje zločiny nebude trestaný, čo mu vytvára voľnú cestu k realizácii trestných činov. Akonáhle chýba hrozba následnej sankcie, je celá záležitosť ťažko riešiteľná a jej zlepšenie, respektíve eliminácia takmer nemožná, veľmi nízko pravdepodobná. No nielen praktický dôsledok je problémový v rámci statusu nepotrestania v konečnom dôsledku, ide aj o odkaz, ktorý sa týmto dáva spoločnosti. Voči potenciálnym páchateľom týmto signalizujeme, že nemienime robiť nič viac, že nemienime voči tomu radikálne a efektívne zakročiť, napriek tomu, že jasne vidíme, ako je súčasný stav neúčinný. No napriek tomu nemienime zakročiť radikálnejšie a týmto postojom akoby sme dávali najavo akceptáciu počítačovej kriminality, akoby stále mala miesto v tejto spoločnosti. No realita je úplne opačná a odkaz sa má diametrálne líšiť od terajšieho postoja. Nie je predsa správne, aby mali páchatelia pocit, že je spoločnosť natoľko slabá, že s tým nedokáže nič urobiť, nijak docieliť spravodlivosť v podobe vypátrania a potrestania, pretože to im iba dodáva silu, odvahu a marí akúkoľvek snahu o zavedenie hrozby.[6]

---

[6] SCHJOLBERG, S.: An international criminal tribunal for cyberspace (ICTC) – Proposals for new legal mechanism on combatting cybercrime and global cyberattacks, A paper for EastWest tu-

V tomto možno vidieť výhodu medzinárodného orgánu, ktorý svojím systémom dokáže efektívne vypátrať a vyriešiť problém, čím dokáže zabezpečiť chýbajúci inštitút trestania, a teda vytvára priestor pre elimináciu počítačovej kriminality, čím sa stáva najvhodnejším a najpotrebnejším nástrojom na riešenie tejto problematiky. Práve táto skutočnosť, že mnohé kyberútoky v konečnom dôsledku ostávajú nepotrestané, bez zásahu súdneho orgánu, je kľúčovým a jedným z dôvodov urgentnej potreby zavedenia a vytvorenia tohto chýbajúceho článku v medzinárodnom právnom systéme.

S cieľom riešenia medzinárodných zločinov boli vytvorené orgány ako napríklad International Court of Justice alebo International Criminal Court a ďalšie. Spoločnosť sa zhoduje na tom, že je iracionálne, ak pri takýchto zločinoch možno detekovať prítomnosť spravodlivosti v podobe rozhodnutia súdneho orgánu a potrestania zločincov, no v prípade počítačovej kriminality, ktorá zo svojej podstaty predstavuje často krát väčšiu hrozbu, to ostáva nepotrestané.

3. Návrhy medzinárodného súdneho orgánu (ICTC)

Na odporúčanie Nórskeho sudcu Steina Schojberga bol vytvorený z dielne pracovnej skupiny EastWest Institute významný návrh medzinárodného tribunálu pre počítačovú kriminalitu, ktorý v zásade obsahuje dve alternatívy, pričom druhá je koncipovaná v zmysle ďalších dvoch podalternatív. Táto kapitola bude zameraná na druhú alternatívu návrhu, nakoľko tejto sa venovali pri vypracovávaní plánu obšírnejšie a predstavuje pravdepodobnejšiu podobu finálneho tribunálu.

Prvou možnosťou by bola situácia, kedy by stíhanie počítačovej kriminality mal na starosti Medzinárodný trestný súd- International Criminal Court (ICC). Tento tribunál stíha jednotlivcov za činy ako genocída, zločiny proti ľudskosti či vojnové zločiny. Nový plán by teda spočíval v rozšírení zoznamu zločinov, ktorých stíhanie má na starosti ICC, čo by v konečnom dôsledku znamenalo aj nevyhnutnú zmenu Rímskeho štatútu, ako zakladajúceho dokumentu ICC.

Druhá možnosť spočíva vo vytvorení nového orgánu ICTC, teda inštitucionalizácia, čo by bolo možné dosiahnuť dvomi spôsobmi:

1. Vytvoril by sa tribunál ako oddelenie na ICC, teda by bol jeho súčasťou a jeho právnym základom by bol Roma Statue- Rímsky Štatút.
2. Tribunál by vznikol ako samostatný súdny orgán, bez statusu pododdelenia ICC. Jeho právnym základom by bola rezolúcia Bezpečnostnej rady OSN, podobne ako pri ICTY a ICTR.

1. Ak by sa tribunál skonštruoval podľa prvého návrhu, nie je isté, že by rovnako ako ICC sídlil v Haagu. No je to jedna z možností, totiž *prvá varianta* spočíva vo vytvorení tribunálu, ktorého sídlom sa stane Haag, a teda nastane vytvorenie komplexu ICC a ICTC, zatiaľ čo *druhá časť návrhu* uprednostňuje vytvorenie sídla pre ICTC v Singapure. To bude mať za následok koncepciu súdneho orgánu ako samostatného tribunálu, no stále sa bude riadiť jurisdikciou ICC, nakoľko takisto bude predstavovať jej pododdelenie. Špecifikum druhého návrhu spočíva aj v tom, že súdny orgán bude založený prostredníctvom INTERPOLU, čo je od roku 1980 vedúca inštitúcia obsahujúca znalosti vo vyšetrovaní medzinárodných kyberútokov. Zameriava sa na rozvoj inovatívnych nástrojov na

---

te (EWI) Cybercrime Working Group, May 2011 dostupné na: http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf.

účinný boj proti počítačovej kriminalite. Interpol pracuje na vytvorení Interpol global comlpex - IGC, ktorého vznik je naplánovaný na rok 2014 situovaný v Singapure, čo dotvára determináciu rozhodnutia uvažovať aj o Singapure ako eventuálnom sídle tribunálu pre počítačovú kriminalitu. Pretože by to otváralo možnosť vzájomnej kooperácie s vynikajúcimi vyšetrovacími inštitúciami. Tribunály by sa *riadili jurisdikciou ICC*, nakoľko z toho následne vyplýva ďalšia významná a veľmi dôležitá skutočnosť, a síce, že by súdny orgán bol „pokrytý" a zastrešený Rímskym Štatútom. *Roma Statue* predstavuje dokument, na základe ktorého bol založený International Criminal Court a ktorý bol ratifikovaný 111 štátmi a vstúpil do platnosti 1. Júla 2002. Štatút je považovaný za mimoriadne signifikantný pre súdny orgán počítačovej kriminality, čo dokazuje aj vykreslenie jeho úloh po zavedení tohto orgánu. Jedná sa o vytvorenie právneho rámca na zabezpečenie proti imunite zo sankcií z týchto činov. Štatút obsahuje články, ktoré pojednávajú o vyšetrovaní a stíhaní.

2. Situovanie tribunálu buď do Haagu alebo do Singapuru je situácia aj v prípade vytvorenia samostatného súdneho orgánu. Avšak tam už by bol právny základ iný.[7]

3.1. Spoločné znaky návrhov

Návrhy sa síce rozchádzajú v niektorých veciach, no v zásade obsahujú spoločné charakteristiky a vyznačujú sa viacerými rovnakými atribútmi:

Ako už vyplýva z uvádzaných dôvodov na zavedenie tribunálu, *cieľom* (a to bez ohľadu na to, ktoré sídlo sa v konečnom dôsledku zvolí) je signalizovať spoločnosti, že kyberútoky nie sú viac tolerované, že tu pre nie je viac miesto. A teda opačný signál, aký je vysielaný v súčasnosti. Tribunál by taktiež vznikol za účelom predchádzania páchaniu trestných činov prostredníctvom jasných varovaní, a zároveň za účelom následného vyšetrovania, trestania a sankcionovania. No generickou sumarizáciou dospievame k tomu, že primárne pôjde o *eliminovanie kyberútokov* prostredníctvom odstránenia skutočnosti, že mnohé činy teraz ostávajú nepotrestané.

Čo sa týka systému, ktorý bude fungovať v rámci tribunálu, efektívne pátranie, vyšetrovanie a trestné stíhanie bude zabezpečené prostredníctvom *úradu Prokurátora*. Mal by to byť nezávislý orgán, ktorý by vyhodnotil informácie a následne by začal s vyšetrovaním. Zároveň by sa však mohol obrátiť na orgán Pre-trial Chamber, ktorý by vykonával nevyhnutné vyšetrovacie úkony, v dôsledku čoho by takýto systém mohol výrazne pomôcť pri riešení útokov proti informačnej infraštruktúre v kyberpriestore.

Úrad Prokurátora by mal byť skutočne nezávislý a neprijímať inštrukcie od žiadnej vlády ani žiadneho zdroja, vďaka čomu nehrozí riziko zaujatosti a neobjektívnosti, ako v prípade štátov v súčasnom systéme. Avšak, úradu môže radiť poradná komisia zložená z 5 členov volených stálymi členmi bezpečnostnej rady OSN.

Prokurátor by bol volený na obdobie 4 rokov s možnosťou opakovaného zvolenia. Súčasťou úradu by boli tiež pracovníci, ktorý by zastávali svoju funkciu minimálne na dva roky, taktiež s možnosťou opakovaného zvolenia, pričom volení by boli generálnym tajomníkom OSN na odporúčanie Prokurátora.

Spomínaný „chamber" alebo inak sudcovská komora by mala pozostávať zo 16 stálych sudcov volených Valným zhromaždením OSN, ktorí by boli rozdelení do 3 skúšobných

---

7 An International Criminal Tribunal for Cyberspace – Judge Stein Schjolberg´s Recommendation. November 11, 2012, dostupné na: http://theitcountreyjustice.wordpress.com/2012/11/11/an-international-criminal-tribunal-for-cyberspace-judge-stein-schjolbergs-recommendation/.

komôr a jednej odvolacej komory, za predpokladu, že odvolacia komora by pozostávala zo 7 sudcov. Volení by boli na obdobie 4 rokov.[8]

Z navrhovaného vyplýva, že orgánmi tribunálu by boli úrad prokurátora a súdna komora.

Jednou z najdôležitejších je otázka *kompetencie* tribunálu. Súdny orgán bude stíhať osoby zodpovedné za trestné činy v rámci počítačovej kriminality. Základným kameňom odstrašovania v kyberpriestore by teda bola skutočnosť, že každý jednotlivec by mohol byt stíhaný za ktorýkoľvek druh kyberútokov, ktorých skutková podstata bude obsiahnutá v zozname stíhateľných podstát.

Vyšetrovanie a trestanie bude vo všeobecnosti zamerané na masívne a koordinované kybernetické útoky proti kritickým informáciám infraštruktúry a na porušovanie globálnej zmluvy alebo súboru zmlúv o počítačovej kriminalite. V konkrétnom ponímaní sa bude jednať o skutkové podstaty ako neoprávnený prístup, protiprávne sledovanie, zasahovanie do dát, počítačové podvody, trestné činy týkajúce sa detskej pornografie a ostatné podstaty, ktoré napĺňajú definíciu neoprávnených a škodlivých útokov na rozsiahle infraštruktúry.

Úloha sudcov by v rámci docielenia ochrany medzinárodného práva a ľudských práv v kyberpriestore nemala byť odlišná od role zastávanej sudcami v ostatných trestných činoch. Jurisdikcia navrhovaných tribunálov by pôsobila súbežne vo vzťahu ku vnútroštátnym súdom, no súd pre počítačovú kriminalitu musí mať prednosť a musí mať možnosť prevziať vyšetrovanie a konanie v ktorejkoľvek fáze.

Schojberg navrhuje systém úzkej spolupráce Prokurátora s Interpolom z dôvodu pravdepodobnosti, že Úrad Prokurátora nebude mať dostatočnú schopnosť sám efektívne viesť vyšetrovanie, napriek tomu, že bude disponovať rozsiahlymi právomocami a zodpovedajúcou kvalifikáciou. A teda v záujme dosiahnutia čo najkvalitnejšieho konania sa spolupráca javí ako vysoko prospešná. No okrem tejto je navrhovaná aj kooperácia s Virtuálnou globálnou pracovnou skupinou, ktorá bude pozostávať z odborníkov napr. z Google, Apple, Youtube, Microsoft, facebook a iné. Očakáva sa, že takáto spolupráca rapídne zvýši schopnosť odhaľovania páchateľov a získavania dôkazov.[9]

No veľmi dôležité je zároveň to, že spôsob realizácie činnosti tribunálu bude spočívať aj v jeho kooperácii spolu so štátmi, ktoré by mali súhlasiť so všetkými žiadosťami o pomoc a s požiadavkami súdnej komory, a to bez zbytočného odkladu. Jednalo by sa napríklad o identifikáciu osôb, ich zatknutie a pozbavenie slobody a ich odovzdanie, výsluch a zhromažďovanie dôkazov. Sankcia uložená súdnym senátom má podobu odňatia slobody. Tento trest by bol podávaný v štáte určenom Medzinárodným trestným tribunálom zo zoznamu štátov, ktoré uviedli ochotu prijať odsúdených.

Tu však vidieť jeden z problémov, ktorý vedie ku skepse ohľadne efektívnosti budúceho tribunálu a jeho schopnosti skutočne dosiahnuť eliminácíu kyberútokov. Ide o spomínanú spoluprácu so štátmi, ktorá je nevyhnutná na to, aby stíhanie prebiehalo relatívne bez problémov. Avšak plán nerieši explicitne, ako sa zabezpečí, že štáty skutočne budú ochotné poskytnúť pomoc, stíhať a vydávať svojich občanov či poskytovať iné služby. Návrhom nie je ošetrená vymáhateľnosť, čo je jedna z kľúčových vecí. Totiž ak dôvodom zlyhávania súčasného stavu je aj to, že štáty riešia situáciu prostredníctvom vlastnej legislatívy, čo vyvoláva riziko deficitu vôle stíhať svojich občanov, očakáva sa, že nový tribunál bude

---

8 www.cybercrimelaw.net, An international criminal tribunal for cyberspace (ICTC).

9 WAKEFIELD, M: International Criminal Tribunal for Cybercrime and Human Rights, The Human Rights Brief, December 10, 2012, dostupné na: http://hrbrief.org/2012/12/international-criminal-tribunal-for-cybercrime-and-human-rights/.

nastavený tak, aby k tomuto nedochádzalo a aby s týmto problém nebol. No nanešťastie, ako možno vidieť, plán neposkytuje záruky, že štáty budú ochotné, zatiaľ nemá prostriedky na to, ako docieliť spoluprácu štátu, v prípade, že skutočne odmietne súhlasiť so žiadosťami o pomoc. Pretože možno je tu nastavená situácia tak, že samotné odhaľovanie stôp a zločincov bude efektívnejšie ako v súčasnosti, nebude to stačiť v prípade, že sa štát rozhodne byť pasívny a nebudú existovať účinné metódy vymáhania. V globále nemožno tvrdiť, že je tu stopercentná istota alebo minimálne vysoká pravdepodobnosť dosiahnutia želaného cieľa. Áno, nový tribunál isté aspekty problémovej situácie síce rieši, no tie podstatné ostávajú otvorené, čo spôsobuje neistotu ohľadom účinnosti tribunálu a celkovo jeho zavedenia v konečnom dôsledku.

Záver

Je zjavná urgentnosť potreby regulácie a koordinácie oblasti počítačovej kriminality vzhľadom na jej status mimoriadnej hrozby pre spoločnosť, pre fungovanie štátov a pre celú medzinárodnú oblasť v konečnom dôsledku. No ako možno vidieť, status QUO je kontraproduktívny a značne neefektívny v boji s kyberútokmi. Chýba tu úspešnosť vypátrania páchateľov a vyriešenia problému v konečnom dôsledku, čo následne spôsobuje nemožnosť a deficit sankcionovateľnosti, ktorá je tak potrebná, lebo bez jej existencie v zásade neexistuje entita na dosiahnutie eliminácie kyberútokov a dosiahnutia vytýčeného cieľa. Preto sudca Schojberg navrhuje a odporúča plán zavedenia medzinárodného trestného tribunálu pre oblasť počítačovej kriminality. Ten sa javí ako prospešný a účinný v mnohých bodoch, no bohužiaľ plán nie je vypracovaný do takej miery, aby bolo možné legitímne vyhlásiť, že ním dosiahneme zníženie počtu kyberútokov. Riziká, ktoré hrozia v súčasnosti pri štátoch a ďalšie nedostatky s tým súvisiace, tie plán nemá ošetrené dostatočne, a preto je tu vysoká miera pravdepodobnosti, že aj zavedenie tribunálu bude zlyhávať v kľúčových veciach a problémy neodstráni. Teda záverom možno povedať, že je skutočne otázne, do akej miery by bol takto nastavený tribunál efektívny, pretože napriek tomu, že sa zdá, že by situácie riešil účinnejšie, kľúčové problémy ošetrené nie sú. Každopádne však faktom ostáva, že mohutný rozmach v oblasti počítačovej kriminality si vyžaduje nutnú koordináciu! A vytvorenie návrhu môže byť prínosom v istých ohľadoch.

Charakteristika Obchodnej dohody proti falšovaniu (ACTA) z pohľadu medzinárodného práva

Ján Dulovič

Obchodná dohodaproti falšovaniu (ACTA) je zameraná na účinnejšie presadzovanie práv duševného vlastníctva na medzinárodnej úrovni. Ekonomiky jednotlivých štátov práve vďaka falšovaniu výrobkov a pirátstvu pociťujú značné škody. V štúdii OECD z roku 2009 o celosvetovom rozmere falšovania a pirátstva sa odhaduje, že medzinárodný obchod s falšovaným tovarom vzrástol z objemu iba mierne presahujúceho 100 miliárd USD v roku 2000 na 250 miliárd USD v roku 2007 a to bez zarátania digitálnych produktov na internete a podomácky vyrobených kópií.[1] Táto suma je väčšia než HDP asi 150 krajín. Tento jav má negatívny dopad na obchod a konkurencieschopnosť nielen samotných štátov ale aj samotnej EÚ a tým aj na hospodársky rast a pracovné miesta v EÚ. Reakciou na túto skutočnosť mala byť práve dohoda ACTA (*Anti-Counterfeiting Trade Agreement* - Obchodná dohoda proti falšovaniu). Cieľom uvádzaným v dôvodovej správe dohody ACTA teda bolo vytvorenie právneho rámca na spoluprácu členských krajín EÚ a niektorých tretích krajín v boji proti šíreniu falšovaného tovaru a služieb v cezhraničnom kontexte, a to prostriedkami občianskeho, správneho a trestného práva. ACTA nevytvára nové práva duševného vlastníctva, ale ide o dohodu v oblasti presadzovania práv, ktorej cieľom je účinne bojovať proti porušovaniu týchto práv. V práve duševného vlastníctva je viac ako v akomkoľvek inom právnom odvetví a priori daný nepomer medzi právami, ktoré sú právnym poriadkom garantované, a reálnou možnosťou vymožiteľnosti právnych nárokov vyplývajúcich z porušenia týchto výhradných práv. Z hľadiska efektívnej ochrany duševného vlastníctva nie je kľúčovým problémom hľadanie medzinárodného konsenzu o tom, či má autorskoprávna ochrana trvať 50 rokov alebo 70 rokov, ale o tom, ako v praxi vymôcť nároky nositeľov duševného vlastníctva, v prípade, ak bol porušené. Kľúčovým má byť obchodný rozsah porušenia. Súčasný digitálny svet internetu existujúci problém vymožiteľnosti práv duševného vlastníctva ešte výrazne prehĺbil. Došlo k vytvoreniu asymetrií v tom, ako ľahko je možné porušovať práva duševného vlastníctva, a ako ťažko je zabezpečiť ich efektívnu vymožiteľnosť. Táto asymetria súčasne priniesla, že aj vo vyspelom svete nezanedbateľná časť obyvateľstva pravidelne porušuje autorské práva tretích osôb, ale najmä to, že vznikla ekonomicky silná vrstva „podnikateľov", ktorí takéto porušenia umožňujú na masovej úrovni a prináša im to zisk. Adresátom preto nie sú bežní spotrebitelia, ale hlavne veľkí porušovatelia motivovaní komerčne. Práva duševného vlastníctva, ktoré sú predmetom ochrany tejto dohody, tvoria súčasť majetkových práv a právo na majetok je jedným zo základných ľudských práv.

1. Rokovania

Dohadovanie zmluvy ACTA neprebiehalo na pôde žiadnej z medzinárodných inštitúcii. Podľa Úradu pre obchodné zastúpenie Spojených štátov (Office of the United States Trade Representative, USTR) začali predbežné rozhovory o ACTA medzi USA, Kanadou, Európskou komisiou, Švajčiarskom a Japonskom už v rokoch 2006 a 2007. 23. októbra 2007 vydali Spojené štáty, Európske spoločenstvo, Švajčiarsko a Japonsko spoločné vyhlásenie o

---

1 http://www.europarl.europa.eu/news/sk/headlines/content/20120220FCS38611/9/html/%C4%8Co-by-ste-mali-vedie%C5%A5-o-ACTA.

tom, že začali rokovať o ACTA. Do rokovaní sa následne zapojili ďalšie štáty: Austrália, Kórejská republika, Nový Zéland, Mexiko, Jordánsko, Maroko, Singapur a Spojené arabské emiráty. Rokovania o zmluve ACTA boli do 22. mája 2008 vedené v utajení. Hoci rokovania prebiehali v utajení, rad korporácií mal zastúpenie v poradných výboroch USTR a mal prístup k utajovaným dokumentom. V septembri 2009 sa zistilo, že USTR dal text pracovného návrhu ACTA k dispozícii vybraným subjektom mimo formálnych poradných orgánov prostredníctvom dohôd zakazujúcich zverejnenie.[2] Začiatkom roka 2010 sa však na internet dostala časť tejto dovtedy utajovanej dohody z ktorej vyplývalo, ktoré štáty žiadali, resp. súhlasili s jednotlivými požiadavkami a ustanoveniami dohody. Z tejto zverejnenej časti teda bolo ľahko dedukovateľné, aké ciele sledovali jednotlivé štáty touto Dohodou. Napriek tomu, že väčšina rokovaní bola uskutočňovaná tajne, 21. apríli 2010 pod značným tlakom verejnosti Kancelária prezidenta Baracka Obamu zverejnila predbežné znenie dohody. V tomto znení však už boli odkazy na jednotlivé štáty opomenuté. Ešte v júli 2010 však bol návrh v Európskej únii utajovaný v režime „Vyhradené" a nebol žiadateľom podľa zákona o slobodnom prístupe k informáciám poskytnutý. Konečný text bol zverejnený 15. novembra 2010, v ktorom taktiež odkazy na jednotlivé štáty boli opomenuté.[3] V júni 2010 označili India a Čína, ktoré sa na rokovaniach nezúčastnili, opatrenie ACTA ako „TRIPS-plus", pretože navrhovaná zmluva podľa nich ďaleko prekračovala rozsah Dohody o obchodných aspektoch práv k duševnému vlastníctvu (TRIPS), ktorá bola prijatá na pôde Svetovej obchodnej organizácia (WTO).

2. Schvaľovanie

Zmluvu ACTA podpísalo dňa 1. októbra 2011 v Tokiu 8 štátov (USA, Austrália, Kanada, Japonsko, Maroko, Singapur, Kórejská republika). Tri subjekty, ktoré sa zúčastnili na rokovaniach (Európska únia, Švajčiarsko, Mexiko) vtedy ešte dohodu nepodpísali, ale vydali spoločné vyhlásenie, podľa ktorého ju podpíšu, len čo to bude možné. 26. januára 2012 zmluvu ACTA pri ceremónii pre EÚ na ministerstve zahraničia v Japonsku podpísali zástupcovia EÚ a celkovo 22 štátov (Rakúsko, Belgicko, Bulharsko, Česko, Dánsko, Fínsko, Francúzsko, Grécko, Maďarsko, Írsko, Taliansko, Litva, Lotyšsko, Luxembursko, Malta, Poľsko, Portugalsko, Rumunsko, Slovinsko, Španielsko, Švédsko a Spojené kráľovstvo). Z členských krajín EÚ ju nepodpísali Nemecko, Slovensko, Cyprus a Estónsko s dôvodom, že čakajú na dokončenie príslušných vnútroštátnych procedúr. V reakcii na podpis zmluvy ACTA Európskou komisiou rezignoval na svoju funkciu jej hlavný spravodajca v Európskom parlamente Kader Arif. Svojou rezignáciou chcel upozorniť na to, že ACTA bola od začiatku prerokúvaná bez zapojenia občianskej spoločnosti, a že snahou Európskej komisie bolo dohodu schváliť v zrýchlenom procese. Kader sa vyjadril, že táto zmluva môže mať významné dopady na životy občanov a napriek tomu Európsky parlament o svojom konaní nepovedal takmer ani slovo.

3. Európska únia

22. februára 2012 Európska komisia požiadala Európsky súdny dvor o vyjadrenie či je táto dohoda v súlade alebo rozpore so základnými právami a slobodami Európskej únie. V európskom parlamente bola dohoda primárne priradená na preskúmanie stálemu Výboru pre medzinárodný obchod, pred ním sa však najprv poradne k dohode vyjadrili 4 ďalšie

---

2 http://www.keionline.org/blogs/2009/03/13/who-are-cleared-advisors.

3 *Joint statement on the Anti-Counterfeiting Trade Agreement (ACTA) from all the negotiating partners of the agreement.* Evropská komise, tisková zpráva ze dne 15. listopadu 2010.

stále výbory parlamentu (výbor pre rozvoj, výbor pre občianske slobody, spravodlivosť a vnútorné záležitosti, výbor pre priemysel, výskum a energetiku a výbor pre právne záležitosti), z ktorých všetky zmluvu zamietli. Výbor pre medzinárodný obchod sa na základe stanoviska ostatných výborov a svojho vlastného stanoviska rozhodol, že ratifikáciu dohody v takomto znení tiež neodporúča prijať. Vo výbore pre medzinárodný obchod hlasovali 19 proti, 12 za a nikto sa nezdržal. Následne 4. júla o dohode hlasoval európsky parlament v pléne. Proti ratifikácii hlasovalo 478 poslancov, za bolo 39 poslancov a hlasovania sa zdržalo 165 poslancov. Európsky parlament teda dohodu jednoznačne neratifikoval. 20. decembra 2012 Európska komisia nakoniec stiahla návrh na Európsky súdny dvor ohľadom preskúmania dohody ACTA.[4]

4. Stanoviská výborov EÚ

Výbor pre občianske slobody, spravodlivosť a vnútorné veci (LIBE) v stanovisku uznáva dôležitosť ochrany práv duševného vlastníctva a upozorňuje na skutočnosť, že ACTA nevytvára nové práva duševného vlastníctva, ale že ide iba o dohodu v oblasti presadzovania práv, ktorej cieľom je účinne bojovať proti porušovaniu týchto práv. Toto vo svojom stanovisku potvrdil aj Výbor pre právne veci (JURI), ktorý uviedol, že Dohodou ACTA sa nevytvárajú nové práva duševného vlastníctva pre zmluvné strany – dohodou ACTA sa zavádzajú všeobecné povinnosti pre primerané vykonávanie rozličných opatrení. Inými slovami, čo v súčasnosti chránia európske právne predpisy, zostáva chránené, čo nechránia, zostáva nechránené. Tým tiež pripomína, že Európa potrebuje medzinárodnú dohodu v záujme posilnenia boja proti falšovaným výrobkom, pretože takéto výrobky spôsobujú európskym firmám každoročne významné škody, čo môže mať negatívny dopad aj na samotnú zamestnanosť nielen v EÚ, ale aj celom svete. V súvislosti s tým sa objavil hneď prvý problém dohody ACTA, pretože práve krajiny, v ktorých dochádza k najväčšiemu porušovaniu práv duševného vlastníctva, ako sú Čína, Pakistan, Rusko a Brazília, neboli prizvané k podpisu dohody ACTA a je nepravdepodobné, že ju tieto štáty v blízkej budúcnosti podpíšu. To vyvolalo ďalšie dôležité otázky o efektívnosti opatrení navrhnutých v dohode ACTA.

V stanovisku však výbor pre občianske slobody, spravodlivosť a vnútorné veci (LIBE) ďalej uvádza, že úroveň transparentnosti rokovaní, ako aj mnohé ustanovenia samotnej dohody ACTA boli predmetom sporov, ktorými sa Európsky Parlament opakovane zaoberal počas všetkých etáp rokovania. Zdôraznil, že v súlade s článkom 218 ods. 10 Zmluvy o fungovaní Európskej únie (ZFEÚ) musí byť Parlament ihneď a v plnom rozsahu informovaný vo všetkých etapách konania, a preto sa domnieva, že počas rokovaní o dohode ACTA sa nezabezpečila primeraná úroveň transparentnosti. Komisia síce vyvinula úsilie na to, aby informovala Parlament, avšak požiadavky na transparentnosť sa interpretovali veľmi úzko a iba v dôsledku tlaku Parlamentu a občianskej spoločnosti.[5] Podľa Viedenského dohovoru o zmluvnom práve z roku 1969 (článok 32): *„Doplnkové prostriedky výkladu, včítane prípravných materiálov na zmluve a okolností, za ktorých sa zmluva uzavrela, možno použiť buď pre potvrdenie významu, ktorý vyplýva z použitia článku 31, alebo pre určenie významu, keď výklad urobený podľa článku 31 a) buď ponecháva význam nejednoznačným alebo nejasným;*

---

4 WHITTAKER, Z.: ACTA dealt major blow as Europe rejects the controversial treaty, CNet, 4 July 2012, dostupné online: http://news.cnet.com/8301-13578_3-57466330-38/last-rites-for-acta-europe-rejects-antipiracy-treaty/.

5 Pozri napríklad uznesenie Európskeho parlamentu z 10. marca 2010 o transparentnosti a stave rokovaní o ACTA (Ú. v. EÚ C 349E, 22.12.2010, s. 46) a vyhlásenie Európskeho parlamentu z 9. septembra 2010 o nedostatočnej transparentnosti procesu a potenciálne spornom obsahu obchodnej dohody o boji proti falšovaniu (ACTA) (Ú. v. EÚ C 308E, 20.10.2011, s. 88).

alebo b) vedie k výsledku, ktorý je zrejme protizmyselný alebo nerozumný." Je teda možné pri výklade zmluvy využiť dodatočné prostriedky výkladu, a to vrátane činností na príprave zmluvy a okolností jej uzavretia. Výbor (LIBE) poukázal na to, že nie všetky činnosti na príprave zmluvy ACTA boli verejne dostupné a teda pred začatím rokovaní o dohode ACTA sa nerozvinulo dodatočné a rozhodné úsilie o ďalšie konzultácie so všetkými zainteresovanými stranami ani o zapracovanie ich názorov do rokovaní. V súvislosti s dohodou ACTA sa teda nenaplnili prísne normy transparentnosti a dobrej správy, o ktoré sa Únia usiluje. Výbor (LIBE) uviedol, že dohoda ACTA prichádza veľmi predčasne, najmä v súvislosti s oblasťami, kde Únia ešte nemala príležitosť na zorganizovanie rozsiahlej verejnej diskusie. Akoby to nestačilo, dohoda si v článku 36 vytvára vlastný systém prijímania zmien, na ktorý už nebude mať priamo vplyv národný parlament. Robí tak prostredníctvom tzv. *výboru ACTA*, ktorá môže ako jediná navrhovať zmeny k medzinárodnej dohode a má konečné slovo o výklade jej ustanovení (čl. 34). Štáty tak reálne strácajú suverenitu v pomerne citlivých otázkach. Nehovoriac o tom, že demokratický deficit pri prijímaní tejto dohody sa zrejme prenesie aj do prijímania rozhodnutí *výboru ACTA*. Je dôvodné predpokladať, že sa v budúcnosti všetky nejasné ustanovenia ešte väčšmi sprísnia výkladom *Výboru*. Zmenu výkladu by bolo možné samozrejme dosiahnuť zmenou dohovoru samotného. Akýkoľvek návrh zmeny dohovoru však musí odsúhlasiť opäť ten istý Výbor (čl. 42 ods. 1).[6]

V 10. bode stanoviska Výbor odkázal na stanoviská Európskeho parlamentu, ktoré vyjadril vo svojom odporúčaní Rade z 26. marca 2009 o posilňovaní bezpečnosti a základných slobôd na internete,[7] ktoré boli relevantné pre vtedy prebiehajúce diskusie, vrátane otázky sústavnej starostlivosti venovanej absolútnej ochrane a zvýšenej podpore základných slobôd na internete. V súvislosti s tým však konštatoval, že k dohode ACTA nebolo vykonané žiadne špecifické vyhodnotenie vplyvu na základné práva a nebolo uznané presvedčenie, že „*neexistuje dôvod vykonať vyhodnotenie vplyvu dohody ACTA, pretože táto dohoda nejde nad rámec acquis [Únie] a nie je potrebné prijímať žiadne vykonávacie opatrenia*", a to najmä so zreteľom na stanovisko Komisie obsiahnuté v oznámení z roku 2010 s názvom Stratégia účinného uplatňovania Charty základných práv Európskou úniou.[8]

Podľa výboru (LIBE) opatrenia umožňujúce identifikáciu majiteľa internetového pripojenia, ktorého účet mal byť zneužitý na porušenie práv, by predpokladali zavedenie rôznych spôsobov sledovania toho, ako jednotlivci využívajú internet. Súdny dvor Európskej únie však jednoznačne uviedol, že sledovanie všetkých elektronických správ, ktoré je časovo neobmedzené a nemá presne stanovený rozsah (napríklad systém filtrovania uplatňovaný poskytovateľmi služieb internetu alebo zber údajov vykonávaný majiteľmi autorských práv) nezabezpečuje primeranú rovnováhu medzi právami duševného vlastníctva a inými základnými právami a slobodami. Predovšetkým ide o práva na ochranu osobných údajov, práva na získavanie a rozširovanie informácii a slobodou podnikania (články 8, 11 a 16 Charty).[9] V dohode ACTA nebola jasne stanovená úloha poskytovateľov služieb internetu, čo by mohlo viesť k neoprávneným zásahom a porušeniam práv osôb, ale aj štátov. Poskytovatelia služieb internetu by nemali pôsobiť ako internetová polícia, a preto bola Európska Komisia a členské štáty vyzvané, aby zabezpečili právnu jasnosť, pokiaľ ide o úlohu

---

6 HUSOVEC, M.: Právna analýza vybraných ustanovení ACTA, dostupné online: http://www.eisionline.org/index.php/10-projekty/novinky-z-aktivit/23-acta-pravna-analyza.

7 Ú. v. EÚ C 117E, 6.5.2010, s. 206.

8 Vec C-540/03 Parlament proti Rade (bod 105), vec C-402/05 P a vec C-415/05 P Kadi a Al Barakaat International Foundation proti Rade a Komisii (bod 285).

9 Vec C-70/10, Scarlet Extended SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), body 47 – 49.

poskytovateľov služieb internetu. Výbor pre právne veci (JURI),ktorý je zodpovedný za otázky týkajúce sa výkladu a uplatňovania práva Únie, súladu aktov Únie s primárnym právom, ako aj výkladu a uplatňovania medzinárodného práva, však vo svojom návrhu stanoviska uviedol, že pokiaľ ide o informácie, ktoré musí poskytnúť na základe rozhodnutia oprávneného vnútroštátneho orgánu[10] poskytovateľ internetového pripojenia (Internet service provider, ISP), výslovne sa uvádza, že táto možnosť poskytnutá zmluvným stranám sa musí uskutočniť *v súlade* so zákonmi a právnymi predpismi každej strany. Právo Únie je v tomto smere jasné. V článku 15 smernice 2000/31/ES[11] sa zabraňuje členským štátom možnosť uložiť všeobecnú povinnosť monitorovať sprostredkovateľom poskytovateľov služieb, ako sú napríklad ISP. Tento bod nedávno potvrdil aj Súdny dvor EÚ.[12] V dôsledku toho právo Únie zakazuje všeobecné monitorovanie internetu. V práve Europskej Únie[13] sa ustanovuje, že v súvislosti s jasne vymedzeným sporom týkajúcim sa porušenia práv duševného vlastníctva môžu príslušné súdne orgány nariadiť poskytnutie niektorých informácií. Tento bod takisto potvrdil Súdny dvor EÚ, ktorý spresnil, že sa nevylučuje možnosť, aby *„členské štáty stanovili na základe článku 8 ods. 1 smernice 2004/48 pre poskytovateľa prístupu na internet informačnú povinnosť.“*[14]

Výbor (LIBE) mal za to, že dohoda ACTA sa zameriavala len na rozsiahle porušovanie práv duševného vlastníctva, pričom zmluvným stranám umožňovala vyňať nekomerčné využívanie z ich ustanovení o postupoch trestnoprávneho presadzovania. Teda ďalším z vágnych ustanovení dohody bolo nejasné vytýčenie línie medzi komerčným a nekomerčným využívaním napriek tomu, že je nesmierne dôležité rozlišovať medzi nekomerčným sťahovaním malého rozsahu a porušovaním práv duševného vlastníctva. Podľa výboru (JURI)sa však trestnoprávne presadzovanie vzťahuje len na skutky vykonávané na obchodnej úrovni, ku ktorým patria prinajmenej tie, ktoré sú vykonávané ako komerčné aktivity za priamu alebo nepriamu hospodársku alebo obchodnú výhodu.[15] Keďže sa zameriava výlučne na obchodnú úroveň, trestná sankcia sa nemôže vzťahovať na mladého človeka, ktorý nelegálne preberá dáta. Takéto sankcie by boli okrem iného v rozpore so zásadou proporcionality uvedenou v čl. 6 ods. 3 dohody ACTA *„Pri vykonávaní ustanovení tejto kapitoly každá zmluvná strana zohľadní potrebu proporcionality medzi závažnosťou porušenia, záujmami tretích strán a uplatniteľnými opatreniami, opravnými prostriedkami a sankciami.*“ Výbor (JURI) tiež v návrhu stanoviska uvádza, že vymedzenie termínu „obchodná úroveň“ nie je širšie ako jeho vymedzenie v práve Únie. V odôvodnení smernice 2004/48/ES[16] sa vymedzuje konanie na obchodnej úrovni ako konanie *„s cieľom priameho alebo nepriameho ekonomického prospechu; to spravidla nezahŕňa dobromyseľné konanie konečných spotrebiteľov.“*

Úmyselné falšovanie a porušovanie práv duševného vlastníctva v komerčnom rozsahu je v informačnej spoločnosti závažným javom a preto je potrebné vypracovať komplexnú stratégiu Únie na jeho riešenie. Podľa výboru (LIBE) by sa takáto stratégia nemala zameriavať iba na potláčanie alebo vplyv falšovania a porušovania práv duševného vlastníctva, ale aj na ich príčiny, mala by plne rešpektovať základné práva v Únii a mala by byť pre spoločnosť ako celok účinná, prijateľná a zároveň zrozumiteľná. Na základe žiadosti Eu-

---

10 Článok 27 ods. 4 dohody ACTA.

11 Smernica 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).

12 Vec C-360/10, Sabam Netlog zo 16. februára 2012.

13 Článok 8 ods. 1 smernice 2004/48/ES.

14 Vec LSG Téléz, C-557/07, z 19. februára 2009, bod 41.

15 Článok 23 ods. 1 dohody ACTA.

16 Smernica 2004/48/ES z 29. apríla 2004 o vymožiteľnosti práv duševného vlastníctva.

rópskeho Parlamentu[17] sa Komisia vo svojej stratégii *Digitálna agenda pre Európu* zaviazala prijať v roku 2012 kódex práv EÚ v online prostredí. Komisia má zabezpečiť, že kódex práv EÚ v online prostredí bude jednoznačne vymedzovať používateľské práva občanov Únie a stanovovať, čo môžu alebo nemôžu robiť v digitálnom prostredí, vrátane prípadov, keď používajú obsah chránený právami duševného vlastníctva.

Vzhľadom na všetky uvedené skutočnosti a bez toho, aby bolo dotknuté hodnotenie Súdneho dvora Európskej únie v tejto veci, ale berúc do úvahy úlohu Parlamentu pri ochrane a podpore základných práv, Výbor pre občianske slobody, spravodlivosť a vnútorné veci vyvodil záver, že navrhovaná dohoda ACTA, v súvislosti s ktorou bol Parlament požiadaný o vyjadrenie súhlasu, nie je v súlade s právami zakotvenými v charte, a vyzval Výbor pre medzinárodný obchod, aby ako gestorský výbor odporučil Parlamentu neudeliť súhlas s uzavretím dohody ACTA.

5. Dohoda ACTA a jej dopad na základné ľudské práva EÚ

Ostrej kritike však boli podrobené aj iné ustanovenia dohody ACTA. Verejnosť, ale aj samotný odborníci sa častokrát vyjadrovali k nejasnému či vágnemu textu dohody, k širokej možnosti vykladania daných pojmov a právnej neistote, ktorá z nej vyplývala. Napríklad ustanovenia článku 4 *Ochrana súkromia a zverejňovanie informácií*, [18] článku 6 *Všeobecné povinnosti v súvislosti s presadzovaním, konkrétne primeraná ochrana práv všetkých účastníkov a požiadavka proporcionality,* [19] alebo článku 27 odsek 3 *„Každá zmluvná strana usiluje o podporovanie spolupráce v rámci podnikateľských kruhov, aby účinne riešila porušovanie ochranných známok a autorských práv alebo súvisiacich práv pri zachovaní zákonnej hospodárskej súťaže a v súlade s právnymi predpismi zmluvnej strany a pri zachovávaní základných zásad, ako sú sloboda prejavu, spravodlivý proces a súkromie.“* treba považovať za ustanovenia všeobecnej (článok 4 a článok 6) a špecifickej (článok 27 odsek 3) povahy, ktoré vymedzujú len štandardnú a minimálnu ochrannú klauzulu. Ochrana súkromia a sloboda prejavu však nie sú iba jednoduchými zásadami, ako uvádza dohoda ACTA. Právo na ochranu súkromia, slobody prejavu a iné, boli uznané ako základné práva, okrej iného aj v Medzinárodnom pakte o občianskych a politických právach, EDĽP, charte a Všeobecnej deklarácii ľudských práv.[20] Na druhej strane však Výbor (JURI) uviedol, že článok 6 ustanovením, ktoré sa pri vykonávaní všetkých opatrení uvedených v dohode uplatňuje horizontálnym spôsobom. V tomto článku sa zavádza zásada proporcionality. Konkrétne tým, že každá zmluvná strana zohľadňuje potrebu *„proporcionality medzi závažnosťou porušenia, záujmami tretích strán a uplatniteľnými opatreniami, opravnými prostriedkami a postihmi“*.[21] V dôsledku toho sa nemôže podľa tohto ustanovenia v rámci právomoci Európskej únie presadzovať prehnaná náhrada škody, lebo sa musí zhodnotiť závažnosť vplyvu a musia sa zohľadniť záujmy tretích strán. V tomto horizontálnom ustanovení sa takisto uvádza, že tieto opatrenia sa uplatňujú takým spôsobom, ktorým sa vylúči *„vytváranie prekážok zákonnému obchodu a poskytne sa ochrana pred ich zneužitím*.“[22]

---

17 Uznesenie Európskeho parlamentu z 21. júna 2007 o dôvere spotrebiteľov v digitálnom prostredí (Ú. v. EÚ C 146E, 12.6.2008, s. 370), body 25 – 28.

18 Ochrana súkromia a zverejňovanie informácií. Dohoda ACTA.

19 Všeobecné povinnosti v súvislosti s presadzovaním, konkrétne primeraná ochrana práv všetkých účastníkov a požiadavka proporcionality. Dohoda ACTA.

20 Odsek 64 stanoviska Európskeho dozorného úradníka pre ochranu údajov uvedeného vyššie.

21 Článok 6 ods. 3 dohody ACTA.

22 Článok 6 ods. 1 dohody ACTA.

Otázku vyvolali aj ďalšie pojmy zakotvené v dohode ACTA, ako sú hlavné zásady či pojem „spravodlivý proces". Riešila sa zlučiteľnosť s pojmami zakotvenými v charte, ako sú základné práva či právo na spravodlivý súdny proces podľa článku 47. Hoci je pochopiteľné, že medzinárodná dohoda prerokovaná medzi stranami s rozdielnymi právnymi tradíciami bude koncipovaná všeobecnejšie než právne predpisy Únie,[23] pretože zohľadňuje rozdielne spôsoby, ktorými jednotlivé strany dosahujú primeranú rovnováhu medzi právami a záujmami, a umožňuje určitú pružnosť, je tiež dôležité, aby dohoda ACTA viedla k právnej istote a obsahovala vyhranené a presne vymedzené ochranné prvky. Obavy z ustanovení, ktoré ponechávajú pružnosť pri ich uplatňovaní bol vyslovený najmä pod hrozbou uplatňovania týchto ustanovení v Únii spôsobom, ktorý by mohol byť nezákonný alebo dokonca v rozpore so základnými právami. Značná právna neistota spôsobená znením niektorých kľúčových ustanovení dohody ACTA (napr. článok 11 *informácie súvisiace s porušovaním*, článok 23 *trestné činy*, článok 27 *uplatňovanie v digitálnom prostredí*, a najmä článok 27 ods. 4 spôsobuje vznik možnosti, že táto dohoda povedie k fragmentácii prístupov v rámci Únie, čo by mohlo ohroziť dodržiavanie základných práv, predovšetkým práva na ochranu osobných údajov, práva na riadny proces a slobody podnikania. Tieto riziká sú relevantné najmä v súvislosti s článkom 27 ods. 3 a 4 z dôvodu nepresnosti týchto textov, ale aj vzhľadom na praktiky, ktoré sa v súčasnosti využívajú v niektorých členských štátoch (napr. rozsiahle monitorovanie internetu súkromnými subjektmi) a ktorých zlučiteľnosť s chartou je otázna. Výbor (LIBE) zdôraznil, že Oddiel 5 *Presadzovanie práv duševného vlastníctva v digitálnom prostredí* osobitne potrebuje väčšiu jasnosť a koherenciu, pretože nepresnosti a neúplnosti môžu vyústiť do odlišných vnútroštátnych predpisov, a takýto fragmentovaný systém by pôsobil ako prekážka pre vnútorný trh, ktorý by v internetovom prostredí bránil rozsiahlejšiemu cezhraničnému využívaniu predmetov chránených právami duševného vlastníctva.

Ak ide o základné práva, nejednoznačnosť nie je na mieste. Dohoda ACTA sa takejto nejednoznačnosti nevyhla, ba naopak, obsahuje ďalšie rozličné aspekty nejednoznačnosti. Judikatúra Európskeho súdu pre ľudské práva potvrdzuje, že účinky každého obmedzenia základných práv a slobôd predpokladaného právom musia byť predvídateľné a takéto obmedzenie musí byť jednoznačné, presné a dostupné, ako aj nevyhnutné v demokratickej spoločnosti a primerané sledovaným cieľom.

Často pretriasaným(najmä verejnosťou) bolo opatrenie, ktoré údajne malo slúžiť k osobným a batožinovým prehliadkam na hraniciach, ba dokonca ku kontrole softvéru na notebookoch. Samotná dohoda ACTA v článku 14 *Malé zásielky a osobná batožina* síce umožňuje vylúčenie malých množstiev tovaru nekomerčnej povahy v osobnej batožine cestujúcich, avšak to ani zďaleka neznamená kontrolu v rozsahu aká bola médiami a verejnosťou uvedená. Okrem toho sa táto časť nevzťahuje na patenty a na ochranu nezverejnených údajov, aby sa nepoškodil zákonný obchod s generickými liekmi.[24] Jedna z často uvádzaných obáv, ktorá bola sčasti oprávnená podľa spravodajkyne výboru (JURI) požiadaného o stanovisko, je založená na skutočnosti, že ak by aj dohoda bola v súlade s právom Únie, jej transpozícia EÚ môže ovplyvniť základné práva. Spravodajkyňa výboru (JURI) požiadaného o stanovisko pripomenula, že povinnosti, ktoré nastoľuje medzinárodná dohoda, by nemali poškodzovať ústavné zásady EÚ, medzi ktorými figuruje aj zásada, podľa ktorej musia všetky akty Spoločenstva dodržiavať základné práva.[25] V dôsledku toho

---

[23] Pracovný dokument útvarov Komisie z 27. apríla 2011 s názvom „Poznámky európskych akademických pracovníkov k dohode ACTA."

[24] Poznámka pod čiarou č. 6 dohody ACTA.

[25] Spojené veci Kadi a i., C-402/05 P a C-415/05 P, bod 285.

Súdny dvor EÚ okamžite sankcionuje akýkoľvek akt transpozície, ktorý by bol v rozpore so základnými právami. Európsku komisia bola v súvislosti s týmto problémov požiadaná, aby vypracovala správu o presadzovaní transpozície dohody ACTA Európskou úniou a členskými štátmi. Táto správa sa mala každoročne predkladať Európskemu parlamentu, aby Ten k nej mohol vydať svoje odporúčania.

6. Nesúlad dohody ACTA s medzinárodným právom

Existujú 3 základné inštitúty, ktoré zastrešujú autorské práva: *Bernský dohovor o ochrane literárnych a umeleckých diel* (zaviedol postihovanie autorských práv štátmi, bez ohľadu na to, kde bola práca publikovaná), *Dohody o obchodných aspektoch práv k duševnému vlastníctvu TRIPS* (medzinárodná dohoda o duševnom vlastníctve) a *Zmluva Svetovej organizácie duševného vlastníctva o autorskom práve WCT* (vylepšila úroveň ochrany poskytovanej Bernským dohovorom). Práve na tieto dohovory a zmluvy reagovala skupina akademikov z EÚ, ktorý spísali svoj názor na dohodu ACTA a na jej nesúlad s týmito dohodami. Najväčší problém dohody ACTA videli v tom, že dohoda zachádza vo svojich ustanoveniach ďalej do práv ľudí, ako už prijaté dohody, resp. zmluvy. V článku 47 dohody TRIPS sa pri práve na informácie uvádza *„Členovia môžu stanoviť, že súdne orgány budú mať právomoc nariadiť porušiteľovi, aby oznámil nositeľovi práv totožnosť tretích osôb zúčastnených na výrobe alebo na distribúcii porušujúceho tovaru alebo služieb, ako aj informácie o ich distribučnej sieti, ak by to nebolo v nepomere k závažnosti porušenia..“* Dohoda ACTA však posilňuje právomoci súdov, pretože podľa článku 11 dohody *Informácie týkajúce sa porušenia* už zmluvné strany majú povinnosť ustanoviť, že v občianskoprávnom konaní budú súdy oprávnené žiadať tieto informácie, hoci v spomínanom článku 47 dohody TRIPS majú zmluvné strany len možnosť tohto ustanovenia. Druhým závažným rozšírením v tomto článku je, že na rozdiel od dohody TRIPS, kde sa informácie týkajúce sa porušenia vzťahovali len na porušovateľov, pri dohode ACTA sa vzťahujú už aj na údajných porušovateľov. Porušená je taktiež proporcionalita uvedená v článku 47 dohody TRIPS (posledná veta), ktorá je v článku 11 dohody ACTA úplne vypustená. Dohoda ACTA taktiež neobsahuje žiadne ustanovenie, ktoré by zabraňovalo a chránilo zneužívanie získaných informácii.

Rozpor medzi dohodou TRIPS a ACTA nastáva aj v ustanoveniach týkajúcich sa ochranných opatrení. Článok 56 dohody TRIPS hovorí, že *„Príslušné orgány sú oprávnené nariadiť žiadateľovi, aby zaplatil dovozcovi, príjemcovi a majiteľovi tovaru primeranú náhradu za každú škodu, ktorú im spôsobil neoprávneným zadržaním tovaru alebo zadržaním tovaru prepusteného podľa článku 55.“* avšak ACTA neobsahuje žiadne ekvivalentné ustanovenie, ktoré by riešilo otázku kompenzácie pri neoprávnenom zadržaní tovaru. Čl. 55 dohody TRIPS obsahuje presne stanovenú lehotu trvania počiatočného zadržania tovaru podozrivého z falšovania na základe ktorého musí byť postavený a začatý prípad alebo bude tovar prepustený. ACTA opäť neobsahuje žiadne tomu ekvivalentné pravidlo. Čl. 19 dohody ACTA totiž neurčuje žiadnu presne stanovenú lehotu, používa iba slovné spojenie „v primeranej lehote“ po začatí konania.

7. Nesúlad dohody ACTA s právom EÚ

7.1. Problém dočasných opatrení

Čl. 12 dohody ACTA neobsahuje žiadny špecifický odkaz na procedurálne záruky pre odporcu položené v Smernici EÚ 2004/48 čl. 9 ods.4 *„Členské štáty zabezpečia, aby predbežné opatrenia uvedené v odsekoch 1 a 2 mohli byť vo vhodných prípadoch prijaté beztoho, aby bol odporca vypočutý, najmä ak by akékoľvek omeškanie spôsobilo vlastníkovi práv nenapraviteľnú ujmu. V takom prípade o tom budú účastníci bezodkladne informovaní, a to najneskôr*

po vykonaní opatrení" a čl. 9 ods. 5 *„Členské štáty zabezpečia, aby predbežné opatrenia uvedené v odsekoch 1 a 2 na návrh odporcu boli zrušené alebo inak prestali byť účinné, ak navrhovateľ nepodá v primeranej lehote na príslušný súdny orgán návrh na začatie konania vedúceho k rozhodnutiu vo veci samej, pričom lehotu stanoví súdny orgán nariaďujúcim opatrenia, ak to právne predpisy členského štátu umožňujú alebo, ak také stanovenie chýba, v lehote nepresahujúcej 20 pracovných dní alebo 31 kalendárnych dní, podľa toho, ktorá je dlhšia.*" Takýto je stav je rozporuplný, keďže Európsky súdny dvor zdôraznil dôležitosť týchto opatrení „na zabezpečenie zachovania rovnováhy medzi konkurenčnými právami a záväzkami držiteľa práva a právami odporcu".[26] Oba, Luxemburský aj Štrasburský súd opakovane uznali, že právo byť vypočutý zastáva významnú pozíciu v organizácii a vykonávaní spravodlivého súdneho procesu.[27] Zatiaľ čo špecifické pravidlá zaoberajúce sa právom byť vypočutý sa môžu líšiť podľa naliehavosti prípadu (teda umožňuje adaptáciu dočasných opatrení „*inaudita altera parte*" tak ako sú uvedené v čl. 12 ods. 2 dohody ACTA), každé obmedzenie využitia tohto práva musí byť náležite odôvodnené a pokryté procesnými zárukami zabezpečujúcimi, že osoba dotknutá takýmto postupom skutočne bude mať možnosť namietať ustanovenie prijaté v naliehavosti."[28] Je preto len ťažko pochopiteľné a vágne, že dohoda ACTA na jednej strane prijíma dočasné opatrenia „inaudita altera parte", no zároveň na druhej strane nepreberá procesné záruky stanovené v smernici 2004/48, ktoré sú nevyhnutné na zabezpečenie, že osoba zasiahnutá týmito opatreniami bude mať neskoršiu možnosť namietať tieto opatrenia.

7.2. Problém opatrení na hraniciach.

Ustanovenie dohody ACTA v oblasti opatrení na hraniciach obsahuje nejednoznačnosť a otvára priestor na prípadne zneužitie. Zatiaľ čo čl.2 ods.1 nariadenia Rady (ES) č. 1383/2003 o prijatí opatrení colnými orgánmi pri tovare, pri ktorom je podozrenie z porušovania niektorých práv duševného vlastníctva a opatrení, ktoré sa majú prijať pri tovare, pri ktorom sa zistilo, že sa práva duševného vlastníctva porušili špecificky zužuje sféru aplikácie hraničných opatrení porušenia ochranných známok iba na „*falzifikovaný tovar*", čl. 13 dohody ACTA povoľuje hraničné opatrenia v prípade „práv duševného vlastníctva" vo všeobecnosti a tak povoľuje ich aplikáciu aj na každý druh porušenia ochranných známok, ale aj na dizajny či úžitkové vzory. Práva duševného vlastníctva sú definované v čl.5 ods. h) dohody ACTA ako všetky kategórie duševného vlastníctva pokryté dohodou TRIPS. Tu je teda prípustná interpretácia čl.13 dohody ACTA, ktorá zahŕňa nielen prípady falšovania, ale tiež všetky formy porušenia ochranných známok založených čisto na podobnosti znakov. Nejde tu teda len o jasnú extenziu *acqius* EÚ, ale vynára sa partikulárny problém v medzinárodnom obchode s tzv. generickými liekmi, ktoré by mohli byť zadržané na základe porušovania „bežnej" ochrannej známky. Čl.13 by preto potreboval buď jasnejšiu definíciu, doplnenie a zmenu textu alebo aspoň reštriktívny výklad a implementáciu. V protiklade k tomu však tiež treba uviesť, že celá kapitola 3 dohody ACTA (opatrenia na hraniciach) by sa na štáty EÚ ani vôbec nevzťahovala (keďže európsky priestor je colnou úniou). V tomto kontexte je potrebné vnímať aj skutočnosť, že ACTA nebola vyjednávaná verejne, nakoľko v konečnom dôsledku iba v medzinárodnom kontexte potvrdzuje a presadzuje štandardy opatrení už zavedené v EÚ.

---

26 ECJ Case C-89/99, [2001] ECR I-5851 para. 38 seq. – Schieving-Nijstad.
27 ECHR App.-No. 17056/06 para. 78 seq. – Micallef v. Malta.
28 ECJ Case C-341/04, [2006] ECR I-3813 para. 66 – Eurofood.

7.3. Problém kriminálneho vynútenia

V súčasnosti v rámci štruktúry práva EÚ neexistujú opatrenia na kriminálne vynútenie si práv duševného vlastníctva. Preto ACTA prirodzene ide za hranice práva EÚ a vyžadovala by si tak dodatočné legislatívne procesy na úrovni EÚ. Čl. 23 ods.1 dohody ACTA poskytuje širokú definíciu „komerčného rozsahu": *„Každá zmluvná strana ustanoví trestnoprávne postupy a sankcie minimálne v prípadoch úmyselného falšovania ochranných známok alebo porušenia autorského práva a súvisiaceho pirátstva práv v komerčnom rozsahu. Na účely tohto oddielu medzi skutky vykonávané na obchodnej úrovni patria prinajmenej tie, ktoré sú vykonávané ako komerčné aktivity za priamu alebo nepriamu hospodársku alebo obchodnú výhodu.*" Kontrastne na to vo svojom stanovisku Európsky parlament zo dňa 25.Apríla 2007 z tohto rozsahu výslovne vylučuje skutky „vykonané súkromnými používateľmi a na neziskové účely".[29] Európsky parlament tiež prehlásil, že „čestné použitie chránenej práce, zahŕňajúc použitie reprodukcií a kópií alebo v inom spôsobe na účely ako kritika, komentár, novinárske reportáže, výučba(zahŕňajúc viacero používaných kópii v triede), bádanie a prieskum, nenapĺňajú skutkovú podstatu trestného činu." ACTA však opätovne nepotvrdzuje tieto garancie pre súkromných používateľov a pre stanovené výnimky. Európsky akademici v súvislosti s týmto uvádzajú problém, ktorý vzniká pri kinematografických dielach. Zatiaľ čo z čl. 23 ods. 3 dohody ACTA *„Zmluvná strana môže v primeraných prípadoch ustanoviť trestnoprávne postupy a sankcie za neoprávnené kopírovanie kinematografických diel z predstavenia v zariadeniach na premietanie filmov určené širokej verejnosti."* vyplýva, že trestné opatrenia pre neautorizované kopírovanie kinematografických diel sú čisto fakultatívne, ACTA vyzýva Podpisujúce strany aby takéto činy kvalifikovali ako trestné činy aj mimo komerčnej škály. Toto ustanovenie opäť neprihliada na výnimku, ktorú vo svojom stanovisku Európsky parlament zo dňa 25. apríla 2007 z tohto rozsahu výslovne vylučuje ako skutky "vykonané súkromnými používateľmi a na neziskové účely."[30]

Podľa vyjadrenia európskych akademikov na dohodu ACTA nesúladným s právom EÚ je aj článok 23 odsek 2 dohody ACTA *„Každá zmluvná strana ustanoví trestnoprávne postupy a sankcie pre prípady úmyselného dovozu a vnútroštátneho použitia etikiet alebo obalov v obchodnom styku a v komerčnom rozsahu"* Podľa akademikov jazyk použitý v tomto článku je vágny a dá sa z neho vyvodiť, že pokrýva aj dovoz a domáce používanie produktov, ktoré aj keď boli zákonne predané v krajine exportu, neboli autorizované v krajine importu. Takáto interpretácia by bránila tzv.parallel import v EÚ. Európsky parlament v čl. 1 svojho vyjadrenia navrhol, aby tento tzv. parallel import bol špeciálne vyňatý z rozsahu trestných činov. Táto výnimka však v dohode ACTA nie je premietnutá.[31]

Záver

Európska Komisia aj Európsky parlament uznávajú a vítajú fakt, že ACTA predstavuje vynútenie vyšších štandardov ochrany, ako tie ktoré sú momentálne upravené medzinárodným právom. Napriek tomu však niektoré ustanovenia Dohody ACTA nezabezpečujú

---

[29] Position of the European Parliament adopted at first reading on 25 April 2007 with a view to the adoption of Directive 2007/.../EC of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (EP-PE_TC1-COD(2005)0127).

[30] Position of the European Parliament adopted at first reading on 25 April 2007 with a view to the adoption of Directive 2007/.../EC of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (EP-PE_TC1-COD(2005)0127).

[31] Opinion of European Academics on Anti-Counterfeiting Trade Agreement.

a nevyvažujú dostatočne záujmy rôznych strán, keďže buď eliminujú záruky existujúce v súčasnom medzinárodnom práve alebo po posilnení donucovacích opatrení zlyhávajú v predložení adekvátnych ochranných opatrení.

Spoločnosti však hrozí predovšetkým nebezpečný precedens. Prijatie právneho aktu, ktorý bol úmyselne skrývaný pred verejnosťou, a ktorého celý obsah nebol tak dlho známy, je výrazným signálom „lobingu" veľkých firiem práve v tomto odvetví priemyslu. Popri WIPO a WTO tak ACTA plánuje vytvoriť nový systém. Systém, ktorý dokáže flexibilnejšie prijímať zmeny, pričom zásady jeho fungovania zatiaľ nie sú stanovené (čl. 36 ods. 5). Prijatie ACTA nespôsobí len posun k prísnejšej právnej ochrane, ale ACTA aj napriek snahe Európskeho parlamentu by mohla zmraziť akúkoľvek podstatnú reformu autorského práva či iných práv duševného vlastníctva do budúcna. Multilaterálna dohoda, ktorej zmluvnou stranou je EÚ sama, by sa tak mohla stať aktom konzervovania mnohých zastaralých ustanovení vo vymáhaní práv duševného vlastníctva. Duševné vlastníctvo je potrebné chrániť. Ochrana základného práva vlastniť majetok, ktorého súčasťou sú práva duševného vlastníctva, musí byť však vyvážená s ochranou ďalších základných práv (Scarlet Extended C-70/10). ACTA poriadne záruky vyváženosti nedáva, naopak, skôr ich berie.[32]

[32] HUSOVEC, M.: Právna analýza vybraných ustanovení ACTA, dostupné online: http://www.eisionline.org/index.php/10-projekty/novinky-z-aktivit/23-acta-pravna-analyza.

ACTA a jej dopad na základne práva a slobody

Martin Blaha

Úvod

Obchodná dohoda o boji proti falšovaniu (The Anti-Counterfeiting Trade Agreement; ďalej len "ACTA")[1] je medzinárodná zmluva, ktorej vytvorenie bolo motivované reálnym alebo len subjektívne vnímaným nedostatkom progresu vo vynucovaní práv duševného vlastníctva (ďalej len "PDV") v medzinárodnom prostredí.[2] Oficiálne rokovania o zmluve začali v októbri 2007 a boli ukončené po 11 kolách rokovaní v Októbri 2010 v Tokiu, Japonsko. Stranami rokovaní a neskôr signatármi boli Austrália, Kanada, Kórejská republika, Maroko, Nový Zéland, Singapur, Švajčiarsko, Mexiko, Spojené Štáty Americké a Európska Únia, pričom hlavné rozvojové štáty a najväčší porušovatelia práv duševného vlastníctva ako Čína, Brazília a India neboli formálne prizvané k participácii.[3] Signatári podpísali zmluvu v dvoch kolách,[4] z členských krajín Európskej Únie ju podpísalo celkovo 22 štátov, neboli medzi nimi Nemecko, Holandsko, Estónsko, Cyprus a Slovenská republika.[5]

Obsahovo ACTA pokrýva falšovanie tovarov s ochrannou známkou a porušovanie autorských práv vytváraním pirátskych kópií tovarov, aj tých distribuovaných online, a požaduje trestné sankcie za také úmyselné porušenie práva za účelom zisku na komerčnej úrovni.[6] Po úvodných ustanoveniach a všeobecnom vymedzení pojmov v Kapitole I, v Kapitole II je upravený právny rámec na presadzovanie PDV, v Kapitole III samotné postupy presadzovania a vynucovania. Kapitola IV upravuje medzinárodnú spoluprácu a nakoniec, Kapitola V navrhuje vytvorenie novej medzinárodnej inštitúcie, Výboru ACTA, ktorý má mať v kompetencii dozor nad riadnym dodržiavaním dohody.

ACTA napriek svojmu názvu nie je klasická medzinárodná obchodná dohoda, je to najmä medzinárodná zmluva proti falšovaniu a je prvá svojho druhu,[7] no na základe odporúčania

---

1 Oficiálny text ACTA [online]. [cit. 2013-03-24]. Dostupné na internete: http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf.

2 OECD, *Executive summary of The Economic Impact of Counterfeiting and Piracy* [online]. str. 1. 2008 [cit. 2013 03-24]. Dostupné na internete: http://www.oecd.org/sti/ind/40896133.pdfana: <http://www.oecd-ilibrary.org/trade/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en>; OECD analýza odhaduje straty v medzinárodnom obchode v dôsledku falšovania a pirátstvu na 200 miliárd amerických dolárov v roku 2005, pričom nezahŕňa domáce produkty a produkty distribuované online.

3 Európsky parlament, DG for External Policies of Union. *The Anti-Counterfeiting Agreement (ACTA): An Assessment* [online]. str. 6. 2011. [cit. 2013-03-24]. Dostupné na internete: http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=4373.

4 Viď oznámenie Ministerstva zahraničných vecí Japonska [online]. [cit. 2013-03-24]. Dostupné na internete: http://www.mofa.go.jp/policy/economy/i_property/acta1201.html.

5 Viď grafiku Európskeho parlamentu [online]. [cit. 2013-03-24]. Dostupné na internete: http://www.europarl.europa.eu/pdf/acta_vote/Acta_vote_en.pdf.

6 Korff, D., Brown, I. *Opinion on the compatibility of the Anti-Counterfeiting Trade Agreement (ACTA) with the European Convention on Human Rights & the EU Charter of Fundamental Rights* [online]. bod 1.1, str. 5. [cit. 2013-03-24]. Dostupné na internete: http://rfc.act-on-acta.eu/fundamental-rights.

7 *2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement* [online]. str. 2. 2011. [cit. 2013-03-24]. Dostupné na internete: http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf.

Európskej komisie sa v rámci legislatívneho postupu podľa práva EU ACTA považovala za tzv. „zmiešanú dohodu"[8] v súlade s Článkom 218(6)(a)(v) ZFEU (Zmluva o fungovaní Európskej Únie).[9] Jej oficiálnym cieľom je vytvorenie *„komplexnej, prvej, medzinárodnej štruktúry, ktorá bude zmluvným stranám asistovať v ich snahách efektívne bojovať proti porušovaniu práv duševného vlastníctva, najmä proti šíreniu falšovania a pirátstva, ktoré oslabujú legitímny obchod a udržateľný rozvoj svetovej ekonomiky."*[10] Pre rokovania o tejto dohode nebola zvolená často využívaná inštitucionálna podpora WIPO (World Intellectual Property Organization) alebo štruktúra v rámci WTO (World Trade Organization), ale dohoda vznikla nezávisle od týchto inštitúcií. Aj v náväznosti na to boli rokovania o ACTA pod veľkou kritikou vzhľadom na ich tajný priebeh.[11] Vnímanie ACTA verejnosťou je do veľkej miery ovplyvnené médiami, ktoré túto dohodu charakterizovali rôzne, pozitívne aj negatívne. No odozva bola nakoniec podozrievavá a negatívna, najmä pre už spomenuté neverejné rokovania a ich absurdné odôvodnenie ochranou národnej bezpečnosti, či kvôli uniknutým verziám ACTA postupne uverejňovaným od roku 2008 na známej webovej stránke WikiLeaks, čo len dopĺňalo pocit konšpirácie.[12]

V Európskej Únii existuje kritika dohody ACTA z dôvodu názorov a obáv, že nebude v súlade s právom EU, ktoré bude treba následne meniť a je v rozpore so základnými právami zakotvenými najmä v Charte základných práv Európskej Únie (ďalej len „Charta")[13] a Dohovore o ochrane ľudských práv a základných slobôd (ďalej len „Dohovor").[14] V tejto práci bude analyzovaný súlad ACTA s právom Európskej Únie, najmä s jednotlivými základnými právami a slobodami, a budú konfrontované odlišné názory akademikov a inštitúcií Európskej Únie na predmetné potencionálne konflikty týchto noriem. Rozobrané budú najmä *právo vlastniť majetok*, *právo na slobodu prejavu a prístup k informáciám*, *právo na súkromie a ochranu osobných údajov* a *právo na spravodlivý súdny proces*, ktorými sa zaoberali Douwe Korff[15] a Ian Brown[16] vo svojej analýze kompatibility dohody ACTA s Chartou základných práv Európskej Únie a Dohovorom o ochrane ľudských práv a základných slobôd pre Európsky parlament, kde konštatujú, že: *„nekompatibilita dohody ACTA s Dohovorom o ochrane ľudských práv a základných slobôd a Chartou základných práv Európskej Únie by podľa práva EU spôsobila nelegálnosť prijatia a implementácie tejto Dohody"*.[17] Ďalšími dôležitými dokumentmi, s ktorými bude táto práca narábať sú: štúdia dohody ACTA na žiadosť Európskeho parlamentu, ktorá konštatuje, že: *„...ustanovenia ACTA sú vo väčšine prípadov v súlade s EU acquis communautaire. Napriek tomu, v niektorých*

---

8 Matthews, D. *The Rise and Fall of The Anti-Counterfeiting Trade Agreement (ACTA): Lessons for the European Union* [online]. str. 5. Legal studies Research Paper No. 127/2012. Queen Mary University of London, School of Law [cit. 2013-03-24]. Dostupné na internete: http://ssrn.com/abstract=2161764.

9 Konsolidované znenie zmluvy o fungovaní Európskej Únie, Článok 218.

10 Viď spoločné vyhlásenie všetkých strán rokovaní k ACTA [online]. 2010. [cit. 2013-03-24]. Dostupné na internete: http://trade.ec.europa.eu/doclib/press/index.cfm?id=623.

11 Myška, M. *ACTA: Evil Inside?* [online]. str. 3. [cit. 2013-03-24]. Dostupné na internete: http://www.law.mmu.ac.uk/wp-content/uploads/2011/04/ACTA-EVIL-INSIDE.pdf.

12 Viď analýzu EU parlamentu vyššie, pozn. p. č. 3, str. 14.

13 Charta základných práv Európskej Únie [online]. [cit. 2013-03-24]. Dostupné na internete: http://eur-lex.europa.eu/sk/treaties/dat/32007X1214/htm/C2007303SK.01000101.htm.

14 Dohovor o ochrane ľudských práv a základných slobôd [online]. [cit. 2013-03-24]. Dostupné na internete: http://www.echr.coe.int/NR/rdonlyres/5989ED6B-D455-48DE-A143-4F7491582C98/0/Convention_SLK.pdf.

15 Profesor medzinárodného práva na London Metropolitan University, London (UK).

16 Senior Research Fellow na Oxford Internet Institute, University of Oxford (UK).

17 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6.

prípadoch, ACTA je ambicióznejšia ako právo EU, poskytujúc mieru ochrany, ktorá ide za limity stanovené právom EU."[18] Stanovisko Právneho servisu Európskej komisie o konformite dohody ACTA s právom EU, ktoré konštatuje, že: „*napriek tomu, že musí byť uznané, že rôzne ustanovenia ACTA sú predmetom interpretácie, nezdá sa, že, prima facie, nejaké ustanovenia sú v konflikte s existujúcim EU acquis, alebo že budú vyžadovať prijatie nových právnych aktov EU alebo zmenu už existujúcich*";[19] a publikácia profesora práva duševného vlastníctva Duncana Matthewsa z Queen Mary University of London s dôrazom na jeho analýzu dôsledkov rozhodnutia Súdneho dvoru Európskej Únie o kompatibilite ACTA s právom EU, vzhľadom na základné práva a slobody, ak by k nemu došlo.[20]

Celková kritika spočíva najmä v tom, že ACTA neprimerane výhodne chráni práva duševného vlastníctva a podnikateľské záujmy „veľkého biznisu", zlyháva v rozlišovaní rozvojových a rozvinutých krajín vo vzťahoch medzinárodného obchodu, brzdí inováciu a môže mať nepriaznivý dopad na základné práva a slobody.[21]

1. Rozhodnutie SDEU o súlade ACTA s EU acquis

Po viacerých analýzach a námietkach voči ACTA, naznačujúc jej nesúlad s právom EU, najmä so základnými právami a slobodami, Európska komisia položila 04. apríla 2012 SDEU (Súdny dvor Európskej Únie) nasledujúcu otázku: "*Je Obchodná dohoda o boji proti falšovaniu (ACTA) v súlade so Zmluvami Európskej Únie, konkrétne s Chartou základných práv Európskej Únie*?"[22] Súdny dvor nakoniec túto otázku nezodpovedal, pretože Európsky parlament (ďalej len "EP") 4. júla 2012 väčšinou poslancov odmietol pristúpenie EU k ACTA, využijúc tak prvý krát právo veta v rámci legislatívneho Postupu so súhlasom[23] podľa čl. 218 ZFEU. EP tak urobil napriek žiadosti poslanca EP Christofera Fjellnera (Európska ľudová strana, Švédsko), aby vyčkal s hlasovaním na rozhodnutie SDEU o tom, či je ACTA v súlade so základnými právami a slobodami, zahŕňajúc najmä právo na slobodu prejavu a prístup k informáciám, právo vlastniť majetok v prípade duševného vlastníctva, právo na súkromie a ochranu osobných údajov a právo na spravodlivý súdny proces.[24] Tieto udalosti viedli k tomu, že Európska komisia 19. decembra 2012 stiahla svoju otázku položenú SDEU.

Od Súdneho dvora Európskej Únie sa očakávalo najmä to, že vo svojom rozhodnutí dôvažne stanoví primeranú hranicu medzi spomínanými právami (a niektorými ďalšími ako právo na dostupnú zdravotnú starostlivosť) a cieľom ACTA, explicitne uvedenom v recitáli tejto dohody: „*Majúc v úmysle poskytnúť na presadzovanie práv duševného vlastníctva účinné a vhodné prostriedky dopĺňajúce dohody TRIPS so zreteľom na rozdiely v právnych systé-*

---

18 Viď analýzu EU parlamentu vyššie, pozn. p. č. 3; konkrétne str. 25.

19 The European Commission's Legal Service. *Legal opinion: Anti-Counterfeiting Trade Agreement (ACTA) – Conformity with European Union law* [online]. SJ-0661/11. 2011. [cit. 2013-03-24]. Dostupné na internete: <http://christianengstrom.files.wordpress.com/2011/12/sj-0661-11_legal-opinion.pdf>; konkrétne bod č. 13. str. 3.

20 Viď analýzu od Matthewsa, pozn. p. č. 8.

21 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 1. 3, str. 27.

22 Európska Komisia, Press Release [online]. [cit. 2013-03-24]. Dostupné na internete: http://europa.eu/rapid/press-release_IP-12-354_en.htm.

23 Matthews, D. *The Lisbon Treaty, Trade Agreements and the Enforcement of Intellectual Property Rights* [online]. str. 14-18. Legal studies Research Paper No. 44/2010. Queen Mary University of London, School of Law. [cit. 2013-03-24]. Dostupné na internete: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1542324>.

24 Viď analýzu od Matthewsa, pozn. p. č. 8.

moch a v právnej prax."[25] Negatívne stanovisko SDEU by spôsobilo následky podľa Článku 218 (11) druhá veta ZFEU, ktorý stanovuje: "*Ak je stanovisko Súdneho dvora záporné, zamýšľaná dohoda nemôže nadobudnúť platnosť, pokiaľ nie je zamenená alebo doplnená, alebo pokiaľ nie sú zmluvy revidované.*"[26]

V nedávnej dobe SDEU rozhodol v dvoch prípadoch o vyvážení práv zakotvených v Charte základných práv Európskej Únie a opatreniam na ochranu PDV. Predmetné rozhodnutia SDEU sa týkali ochrany osobných informácií, ich filtrovania a vydávaniu stranám s poškodenými právami z duševného vlastníctva, a v kontexte dohody ACTA sú dôležité, lebo viacerí európski odborníci v oblasti PDV sa zhodujú,[27] že Článok 11 ACTA, "*Informácie týkajúce sa porušenia*", posilňuje už existujúce právo na informácie zakotvené v Článku 47 Dohody TRIPS[28] (predchodca a základ pre dohodu ACTA), pretože v súlade s ACTA sa toto právo stáva obligatórnym (na rozdiel od fakultatívnosti podľa TRIPS), a v druhom rade je rozšírený zoznam informácií, ktoré možno požadovať, pričom ich možno požadovať už od obvineného porušiteľa PDV (podľa TRIPS len od súdom uznaného porušiteľa). ACTA taktiež neobsahuje žiadne ustanovenia proti zneužívaniu získaných informácií (na rozdiel od Čl. 8. 3(c) Smernice 2004/48/EC), a chýba v nej požiadavka proporcionality (na rozdiel od Čl. 47 TRIPS a Čl. 8.1 Smernice 2004/48/EC). Dodatočne, Článok 27.4 ACTA reguluje sprístupnenie informácií o predplatiteľovi, pričom je vágnejší ako článok 47 TRIPS, ktorý toto právo upravuje ako fakultatívne na rozdiel od ACTA. Dôležitejším je však predmetná úprava ACTA umožňujúca tieto informácie požadovať tak o porušiteľoch, ako aj o tých predplatiteľoch, čo neporušili PDV (na rozdiel od TRIPS, kde informácie môžu byť získané len o porušiteľoch PDV). ACTA v tejto oblasti všeobecne odkazuje na ochranu práva na slobodu prejavu, spravodlivý súdny proces a súkromie, no neobsahuje žiadne presnejšie ustanovenia efektívnej ochrany predmetných práv (na rozdiel od detailných ustanovení ochrany súkromia v Smernici 1995/46/EC, 2002/58/EC a 2006/24/EC). Ak by SDEU rozhodoval o súlade ACTA a EU acquis, mohol by jasne rozhodnúť, či sú niektoré vágne ustanovenia ACTA v súlade s právom EU, resp. ako ich treba vykladať a vykonávať. Urobil tak aj v nasledujúcich rozhodnutiach.

V prípade Scarlet Extended SDEU uviedol, že právo EU zakazuje, vzhľadom na požiadavky vyplývajúce z ochrany základných práv, vydanie súdneho príkazu, ktorý by poskytovateľovi internetového pripojenia ukladal povinnosť zaviesť systém filtrovania celej elektronickej komunikácie prebiehajúcej v rámci jeho služieb, ktorý sa bude preventívne uplatňovať na všetkých jeho zákazníkov, výlučne na náklady tohto poskytovateľa, bez časového obmedzenia, a bude spôsobilý identifikovať na sieti tohto poskytovateľa obeh elektronických súborov obsahujúcich hudobné, kinematografické alebo audiovizuálne dielo, o ktorom navrhovateľ tvrdí, že k nemu má práva duševného vlastníctva, s cieľom blokovať prenos súborov, ktorých výmena porušuje autorské právo.[29]

---

25 Viď. oficiálny text ACTA uvedený vyššie, pozn. p. č. 1, str. 2.

26 Konsolidované znenie zmluvy o fungovaní Európskej Únie [online]. Článok 218 (11). [cit. 2013-03-24]. Dostupné na internete: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:sk:PDF.

27 European academics. Opinion of European academics on Anti-Counterfeiting Trade Agreement [online]. str. 5-6. 2011. [cit. 2013-03-24]. Dostupné na internete: <http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_110211_DH2.pdf>; Ďalšie informácie dostupné na internete: http://www.iri.uni-hannover.de/acta-1668.html.

28 Agreement on Trade-Related Aspects of Intellectual property rights (TRIPS). [online]. [cit. 2013-03-24]. Dostupné na internete: http://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

29 Rozhodnutie SDEU vo veci C-70/10 Scarlet Extended [online]. [cit. 2013-03-24]. Dostupné na internete: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10.

V druhom dôležitom rozhodnutí SDEU konštatoval, že právo EU (smernica 2006/24/ES o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí) sa má vykladať v tom zmysle, že nebráni uplatneniu vnútroštátneho ustanovenia, ktoré povoľuje, aby bolo poskytovateľovi internetových služieb na účely identifikácie konkrétneho účastníka alebo používateľa internetu nariadené oznámiť majiteľovi alebo držiteľovi autorských práv informácie o identite účastníka, ktorému bola pridelená určitá IP adresa, ktorá bola údajne použitá pri porušení uvedeného autorského práva, lebo taká právna úprava nepatrí do pôsobnosti *ratione materiae* predmetnej smernice; pričom smernica 2002/58/ES o spracovaní osobných údajov a ochrany súkromia sa má vykladať v tom zmysle, že nebráni vnútroštátnej právnej úprave, ktorá umožňuje vnútroštátnemu súdu, aby v závislosti od okolností každého samostatného prípadu a s náležitým prihliadnutím na požiadavky vyplývajúce zo zásady proporcionality zvážil jednotlivé protichodné záujmy.[30]

Tieto posledné rozhodnutia SDEU ukazujú hranicu medzi ochranou základných práv a sledovaním záujmov oprávnených osôb z práv duševného vlastníctva, pričom ak by SDEU dostal šancu zodpovedať vyššie položenú otázku o súlade ACTA s právom EU, mohol by autoritatívne špecifikovať aj medze, výkon a ochranu predmetných práv v súvislosti s ochranou práv duševného vlastníctva.

Poučením z procedúry uzatvárania dohody ACTA na Úniovej úrovni je najmä to, že Európsky parlament mal vzhľadom na procedurálne hľadisko počkať, kým SDEU rozhodne, či je ACTA v súlade s Úniovým právom, najmä základnými právami a slobodami a až potom hlasovať o uzavretí samotnej dohody, a to bez ohľadu na fakt, že nič v Článku 218 ZFEU mu nebránilo vysloviť nesúhlas s ACTA pred rozhodnutím SDEU. Nedá sa taktiež definitívne povedať, či ACTA dodržiava primeranú hranicu medzi ochranou predmetných práv a dosahovaním svojich cieľov, alebo ju porušuje, keďže k rozhodnutiu SDEU fakticky ani nedošlo. V nasledujúcich kapitolách budú rozobrané najviac dotknuté práva a rôzne názory na ich potencionálne porušenie dohodou ACTA.

2. Právo vlastniť majetok

Právo vlastniť majetok bolo zahrnuté už do prvých prameňov zakotvujúcich ľudské práva a to vo Francúzskej deklarácii práv človeka a občana (1789), a vo Všeobecnej deklarácii ľudských práv (1948). V súčasnosti je toto právo upravené v článku 17 Charty a v článku 1 Dodatkového protokolu Dohovoru, a nepochybne zahŕňa aj práva duševného vlastníctva. Doslovne je to vyjadrené v článku 17 (2) Charty, pričom práva duševného vlastníctva sa vzťahujú aj na vlastníkov elektronických zariadení a softvéru, programov, hudby, audio alebo video súborov na nich uloženom, alebo uschovanom v tzv. "*cloud-e*".

Ak má byť toto právo legitímne obmedzené, musí byť splnená požiadavka tzv. „*fair balance*" testu, ktorý používa Európsky súd pre ľudské práva (ďalej len „ESĽP") pri ochrane práv podľa Dohovoru a takmer rovnakým spôsobom aj SDEU pri ochrane práv v súlade s Chartou. V rámci tohto *fair balance* testu sa veľkou mierou spolieha na procedurálne garancie. V prvom rade, aby bolo do vlastníckeho práva legálne zasiahnuté, musí existovať možnosť nápravy riadnym opravným prostriedkom voči rozhodnutiu o obmedzení / po-

---

[30] Rozhodnutie SDEU vo veci C-461/10 Bonnier Audio [online]. [cit. 2013-03-24]. Dostupné na internete: http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=61956.

zbavení vlastníckeho práva vydanom národným orgánom na základe zákona. V druhom rade, pri zasiahnutí do práva musí dôjsť aj k primeranému protiplneniu ako kompenzácii za tento zásah.[31] Pri posudzovaní vyváženosti práv a povinností dvoch strán v náležitých vzťahoch sa berie do úvahy aj interpretatívny princíp proporcionality, ktorý v sebe neobsahuje hmotnoprávne práva a povinnosti, ale slúži na vyváženie a balansovanie noriem za účelom stanovenia presného obsahu základných práv a slobôd.[32]

Môžeme konštatovať, že takmer všetky opatrenia v ACTA v súvislosti s porušením práv duševného vlastníctva majú za cieľ ochranu vlastníkov/držiteľov PDV, no tieto opatrenia môžu mať vážny dopad na vlastnícke práva užívateľov a spotrebiteľov. Keďže sa neprimeraný zásah do vlastníckych (aj tých ostatných) práv posudzuje najmä podľa procesných opatrení, budeme sa im venovať v 6. kapitole tejto práce, „Právo na účinný prostriedok nápravy a na spravodlivý súdny proces."

3. Právo na slobodu prejavu a prístup k informáciám

Toto právo, upravené v Článku 11 Charty a v Článku 10 Dohovoru, v sebe zahŕňa viac ako len *právo vyjadriť svoj názor*. Jeho význam chápeme aj ako *právo mať názor* a *právo dostať, šíriť a vyhľadávať názory a informácie*. Podľa názoru ESĽP je to pre demokratickú spoločnosť základné a nevyhnutné právo, často dôležitejšie ako právo na ochranu vlastníctva.[33] V kontexte ACTA je tieto práva dôležité analyzovať z troch hľadísk.[34] Prvé hľadisko sa týka aplikácie ACTA na banálne a malé prípady technických porušení PDV, bez účelu zisku, alebo na šírenie informácií chránenými právom duševného vlastníctva bez súhlasu vlastníka tam, kde je na to oprávnený prevažujúci verejný záujem. Tu autori Korff a Brown dochádzajú k viacerým konštatovaniam. Článok 23(1) ACTA,

„ČLÁNOK 23

Trestné činy

1. *Každá zmluvná strana ustanoví trestnoprávne postupy a sankcie minimálne v prípadoch úmyselného falšovania ochranných známok alebo porušenia autorského práva a súvisiaceho pirátstva práv v komerčnom rozsahu. Na účely tohto oddielu medzi skutky vykonávané na obchodnej úrovni patria prinajmenej tie, ktoré sú vykonávané ako komerčné aktivity za priamu alebo nepriamu hospodársku alebo obchodnú výhodu.*"[35]

požaduje strany dohody, aby znížili kritéria pre trestnosť pri porušení PDV. To sa prejavuje používaním pojmov, ktorých výklad je sporný a nejasný. Jedná sa o pojmy *„komerčný rozsah"* a *„nepriama hospodárska alebo obchodná výhoda"*. Nejasnosť týchto pojmov spôsobuje obavy z kriminalizácie obyčajných situácií, ktoré by inak trestnými neboli (väčšinou

---

31 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 2.2, str. 20.

32 Christoffersen, J. *Fair Balance – A Study of proportionality, Subsidiarity and Primarity in the European Convention on Human Rights* [online]. bod 2.8 str. 185-213. ISBN 978-87-89091-01-3 [cit. 2013-03-24]. Dostupné na internete: http://www.humanrights.dk/files/pdf/Disputats%20_Endelig%202008%2004%2017_%20(2).pdf.

33 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 2.3., str. 22.

34 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 3., str. 57.

35 Viď oficiálny text ACTA, pozn. p. č. 1, Článok 23 Trestné činy.

sa vyžaduje len priamy prospech). Jedná sa napríklad o situáciu, keď fyzická osoba A vlastní CD s hudbou a urobí z neho kópiu, ktorú potom dá fyzickej osobe B bez odplaty. Neskôr si fyzická osoba B kúpi CD a dá ho osobe A bez odplaty. Na túto situáciu sa môže hľadieť ako na nepriamu hospodársku výhodu osoby A z činnosti kopírovania CD. Pre tieto situácie taktiež nie sú v ACTA uvedené žiadne *de minimis* výnimky, bežné v právnych poriadkoch členských štátov EU.

Tieto obavy potvrdzujú aj európski akademici, keď poukazujú na pozíciu Európskeho parlamentu, ktorý v apríli 2007 výslovne vylúčil z trestnoprávnej zodpovednosti činy vykonané súkromnými užívateľmi na súkromné účely bez účelu profitu. EP zároveň vyhlásil, že spravodlivé užívanie diela chráneného právom duševného vlastníctva, zahŕňajúc reprodukciu akýmkoľvek spôsobom, za účelom kritiky, komentáru, reportovania správ, vyučovania, akademickej práce a výskumu, nekonštituuje trestný čin. Podľa názoru viacerých odborníkov na duševné právo však ACTA tieto závery nepotvrdzuje.[36]

Samotný pojem *komerčný rozsah*, nie je, ako sa zdá podľa štúdie EP, ani v súlade s doterajšími rozhodnutiami WTO (World Trade Organization), ktoré tento pojem používajú na určenie záporného dopadu danej protiprávnej aktivity na trh, oproti ACTA, ktorá ho skôr chápe v súlade s *priamou alebo nepriamou hospodárskou výhodou* ako nástroj na určenie úmyslu porušovateľa PDV.[37]

Podľa Čl. 23(4),

„ČLÁNOK 23

Trestné činy

4. *V súvislosti s trestnými činmi uvedenými v tomto článku, pre ktoré zmluvná strana ustanovuje trestnoprávne postupy a sankcie, táto zmluvná strana zabezpečí, že v jej právnych predpisoch bude ustanovená trestnoprávna zodpovednosť za napomáhanie a navádzanie.*"[38]

ACTA pridáva nové skutkové podstaty, „*napomáhanie a navádzanie*", ktoré sú taktiež vágne a v kombinácii s nepriamym hospodárskym prospechom môžu opäť viesť ku kriminalizácii bežne legálnych obyčajných činností. Bez *de minimis* výnimiek („*fair rules*" a „*fair comment*" pravidiel podľa U. S. práva) bude vynucovanie PDV neprimerane reštriktívne obmedzovať právo na slobodné vyhľadávanie, prijímanie a šírenie informácií a ideí. Nemierni to ani fakt, že strany dohody môžu získať určité hmotnoprávne výnimky z PDV, keďže *de minimis* výnimky majú procedurálny a nie hmotnoprávny charakter.

Ďalším dôležitým kontextuálnym znakom ACTA je to, že z jej znenia je zrejmé, že držitelia práv duševného vlastníctva môžu porušiteľom týchto práv uložiť takmer akýkoľvek typ obmedzení, pričom ACTA predpokladá, že sú vždy v súlade s právom, v zmysle spotrebiteľského a kontraktačného práva bez ohľadu na to, ako prísne sú. V niektorých prípadoch budú takéto opatrenia však neproporcionálne (aj vzhľadom na chýbajúce *de minimis* ustanovenia, najmä v Článku 27(5)(6)(7)), a budú predstavovať obmedzenie práva na prístup k informáciám podľa Charty a Dohovoru.

---

36 Viď *Opinion of European* academic, pozn. p. č. 27, bod. 7 Scope, str. 4.

37 Viď analýzu EU parlamentu vyššie, pozn. p. č. 3; konkrétne str. 22-23.

38 Viď oficiálny text ACTA, pozn. p. č. 1, Článok 23 Trestné činy.

Posledným hľadiskom, ktoré treba brať do úvahy pri práve na slobodu prejavu a prístup k informáciám sú rozšírená zodpovednosť poskytovateľa internetových služieb a pravidlo „trikrát a dosť" (ďalej len „three strikes"). Napriek tomu, že ustanovenia o zodpovednosti a three strikes sa už vo finálnom texte v Článku 27 ACTA nenachádzajú vo svojej pôvodnej drakonickej forme, boli, tak ako na to jasne poukázal EDPS (European Data Protection Supervisor), v jasnom rozpore s právom EU.[39] Článok 27 má však stále vágny charakter.

„ČLÁNOK 27

Presadzovanie v digitálnom prostredí

1. *Každá zmluvná strana zabezpečí, že v jej právnom poriadku budú postupy presadzovania práva v rozsahu uvedenom v oddiele 2 (Občianskoprávne presadzovanie) a v oddiele 4 (Trestnoprávne presadzovanie) vrátane rýchlych opravných prostriedkov na zabránenie porušovania a opravných prostriedkov, ktoré odrádzajú od ďalšieho porušovania, aby bol možný účinný postup voči skutkom porušenia práv duševného vlastníctva, ku ktorému dochádza v digitálnom prostredí.*

2. *Nad rámec ustanovení odseku 1, postupy presadzovania práva každej zmluvnej strany platia pre porušenie autorského práva alebo súvisiacich práv cez digitálne siete a môžu zahŕňať neoprávnené používanie prostriedkov rozsiahleho rozširovania na účely porušovania. Tieto postupy sa vykonávajú spôsobom, ktorý zabraňuje vzniku prekážok pre zákonné činnosti vrátane elektronického obchodu, a v súlade s právom strany zachováva základné zásady, ako sú sloboda prejavu, spravodlivý proces a súkromie."*[40]

Vágnosť ustanovení Článku 27(1) spočíva najmä v použití pojmov *„účinný postup"* a *„rýchle opravné prostriedky"*, bez ďalšieho špecifikovania týchto konaní a prostriedkov. Článok 27(2) stanovuje, že postupy podľa ods. (1) *„platia pre porušenie autorského práva alebo súvisiacich práv... a môžu zahŕňať neoprávnené používanie prostriedkov rozsiahleho rozširovania..."*, no je jasné, že dané postupy nie sú limitované len *neoprávneným používaním*. Badať aj opäť chýbajúce *de minimis* výnimky. Tieto vágne ustanovenia o postupoch presadzovania práv PDV sú kritizované spolu s krátkym odkazom v ods. (2) *„postupy sa vykonávajú spôsobom, ktorý... v súlade s právom strany zachováva základné zásady, ako sú sloboda prejavu, spravodlivý proces a súkromie"* ako nedostatočné, najmä s chýbajúcim odkazom na medzinárodné dokumenty zakotvujúce predmetné práva. Poznámka pod čiarou pri Čl. 27(2) taktiež naznačuje, že napriek odstráneniu ustanovení o rozšírenej zodpovednosti poskytovateľov internetu, zmluvným stranám sa len povoľuje obmedziť predmetnú zodpovednosť, a teda napriek úprave textu ostáva zámer neprimerane rozšíriť danú zodpovednosť. Nakoniec, odkaz na dodržiavanie v súlade s právom strany naznačuje, že v EU by sa tieto ustanovenia museli dodržiavať v súlade s judikatúrou ESĽP a SDEU, no zdá sa, že štáty mimo EU môžu tieto práva porušovať oveľa jednoduchšie.

---

39 European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)* [online]. 2010. (2010/C 147/01). [cit. 2013-03-24]. Dostupné na internete: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:FULL:EN:PDF.

40 Viď oficiálny text ACTA, pozn. p. č. 1, Článok 27 Presadzovanie v digitálnom prostredí.

Korff a Brown na záver konštatujú, že bez jasnej stipulácie, že zmluvné strany ACTA neprijmú three strikes pravidlo a neprimerane prísne pravidlá o zodpovednosti poskytovateľov internetových služieb, ACTA zlyháva v garantovaní dodržiavania európskych a medzinárodných ľudskoprávnych štandardov. Navyše, explicitné *de minimis* výnimky a ustanovenia o ochrane verejného záujmu sú nevyhnutné pre súlad Článku 23 s Dohovorom, Chartou a právom EU. No po odstránení drakonických opatrení (three strikes, neprimeraná zodpovednosť poskytovateľov) zo skoršej verzie textu ACTA, a pri vykladaní ustanovení ACTA vo svetle judikatúry a uplatňovania práv podľa Charty a Dohovoru, Články 23 a 27 ACTA nie sú v priamom rozpore s Chartou a Dohovorom *prima facie*, no stále sú veľmi vágne a podporujú štáty mimo EU, aby prijali opatrenia ohrozujúce základné práva a slobody v prospech U.S. a EU korporácií. A práve to je presný opak toho, čo vyžadujú tieto dokumenty v relácii k tretím krajinám.

Doplňujúco, analýza Právneho servisu Európskej komisie v danej problematike konštatuje, že ACTA nezahŕňa všetky garancie, ktoré EP zahrnul do predmetných smerníc, no nezakazuje a neoponuje takým opatreniam, ak by boli prijaté zmluvnými štátmi. Bude tak na každom členskom štáte EU, aby sa rozhodol, či tieto opatrenia v súlade s domácim právom a právom EU zavedie.[41]

4. Právo na súkromie a ochranu osobných údajov

Právo na súkromie a ochranu osobných údajov je upravené v článkoch 7 a 8 Charty a v článku 8 Dohovoru, pričom vo vzťahu k nim sú podstatné ustanovenia Článku 11 a 27(3)(4) ACTA, ktoré majú viaceré dôsledky.[42] Jedná sa (i) o možné neohlásené sledovanie internetových aktivít veľkého množstva jednotlivcov bez podozrenia páchania ilegálnej činnosti,[43] systematické zaznamenávanie takto získaných informácií; (ii) sprístupnenie takto získaných informácií držiteľom práv duševného vlastníctva, napriek tomu že tieto informácie nemusia byť spoľahlivé ako indikátor ilegálneho konania, bez akýchkoľvek právnych záruk, že len nevyhnutné informácie budú poskytnuté tretím stranám; (iii) na základe nejasných štandardov (v zásade bude postačovať vyhlásenie držiteľa PDV); (iv) rozhodnutím súdnych a iných orgánov (teda aj orgánmi bez záruky nestrannosti a neutrálnosti); (v) v cezhraničných vzťahoch, teda aj z štátov EU do štátov mimo EU, bez adekvátnej kontroly dodržiavania základných práv a slobôd; (vi) v konaniach bez práva obvineného jednotlivca byť vypočutý.

Tieto opatrenia by za určitých podmienok mohli byť v súlade s EU právom a štandardmi. Museli by byť limitované na jasné prípady podstatného porušenia PDV a len s predošlým súhlasom príslušného štátneho orgánu. Osobné údaje a informácie by mohli byť sprístupnené len tým tretím stranám mimo EU, ktoré dodržiavajú adekvátne štandardy ochrany osobných dát, s predošlým súhlasom príslušného štátneho orgánu v krajine EU.

Záverom analýzy Korffa a Browna teda je, že absencia striktných podmienok v ACTA v spojení s predchádzajúcimi závermi znamená nekompatibilitu s Dohovorom, Chartou a právom EU v oblasti ochrany osobných údajov.[44]

Európsky dozorný úradník pre ochranu údajov (vo svojej analýze ACTA dochádza k podobným záverom na základe štúdie Článkov 27(3) a 27(4). V prvom rade treba uviesť, že predmetné ustanovenia ACTA dávajú signatárom dohody len možnosť prijať predmetné

---

41 Viď analýzu Právneho servisu Európskej komisie, pozn. p. č. 19, bod. 32, str. 9.
42 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 3., str. 57.
43 Porovnaj s rozhodnutím SDEU vo veci *C-70/10 Scarlet Extended*, pozn. p. č. 29.
44 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 3., str. 57.

ustanovenia, nie je teda použitý obligatórny jazyk. Namietanými sú teda (i) mechanizmus, na základe ktorého môže byť poskytovateľ on-line služieb nariadený, aby urýchlene oznámil držiteľovi práva informácie postačujúce na identifikáciu podozrievaného predplatiteľa, a (ii) usilovanie sa o podporovanie spolupráce v rámci podnikateľských kruhov, aby sa účinne riešili porušovanie ochranných známok a autorských práv. Toto druhé opatrenie treba vykladať s úvodným ustanovením ACTA, kde zmluvné strany vyjadrili podporu spolupráce medzi poskytovateľmi služieb a držiteľmi práv, aby sa riešili príslušné porušenia v digitálnom prostredí. Mnoho kontraktačných strán k ACTA už totiž má určité fungujúce mechanizmy dobrovoľnej spolupráce, napríklad three strikes pravidlo, ktoré už boli vyššie kritizované. Predmetné mechanizmy musia byť podľa tejto analýzy implementované v súlade so zásadou nevyhnutnosti a proporcionality, pričom opäť, nejasné sú pojmy ako *komerčný rozsah*, *kompetentné autority.* Zároveň bolo poukázané na to, že pri širokom monitorovaní užívateľov internetu, ACTA nemá dostatočné ochranné ustanovenia, najmä vzhľadom na implementáciu monitorovania, ochranu osobných údajov, spravodlivý proces a iné.[45]

5. Právo na účinný prostriedok nápravy a na spravodlivý proces

Tieto práva upravuje Charta v článku 47 a Dohovor v článkoch 6 a 13, pričom ESĽP a SDEU ich zvykne vnímať ako vzájomne prepojené. Situácie vznikajúce v súvislosti s ACTA dotýkajúce sa predmetných práv predstavujú najmä určovanie vlastníckych práv (na strane vlastníka alebo spotrebiteľa) chránených článkom 1 Dodatkového protokolu Dohovoru a článkom 17 Charty, a vyúsťujú do trestných obvinení, pričom by mali byť neustále zachovávané štandardy spravodlivého procesu. V kontexte dohody ACTA je dôležité odlíšiť trestné a civilné vynucovanie dodržiavania ustanovení ACTA a tzv. privatizáciu PDV.[46]

V súvislosti s trestným vynucovaním nie je podľa Korffa a Browna problematickým dodržanie podmienok spravodlivého procesu, aspoň nie v rámci EU, ale už nimi vyššie spomenuté zníženie hranice trestnosti a rozšírenie skutkových podstát, bez *de minimis* výnimiek, aj na bežné situácie, ktoré nevyžadujú trestné vynucovanie. V kontexte Dohovoru a Charty sú takéto opatrenia neproporcionálne. Uviedol to aj ESĽP v prípade *Vo v. Francúzsko*, ktorý sa týkal neúmyselného pôrodu, keď sa vyjadril, že trestné stíhanie nie je jediné nevyhnutné riešenie pre daný prípad a ako účinný prostriedok nápravy môže stačiť napríklad náhrada ujmy v civilnom konaní.[47]

V ustanoveniach upravujúcich občianskoprávne vynucovanie, ACTA ohýba klasické pravidlá bez adekvátnych ochranných opatrení. Excesívne sa spolieha na využívanie súdnych príkazov a dočasných opatrení, ako zhabanie majetku a zariadení, v konaniach bez toho, aby bola dotknutá strana riadne vypočutá. Konkrétne, Čl. 12 ACTA stanovuje konania *inaudita altera parte,* no neobsahuje žiadne procedurálne ochranné opatrenia. Tieto boli napríklad zavedené Smernicou 2004/48/EC on the enforcement of intellectual property

---

45 European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor on the proposal for a Council on the Conclusion of the Anti-Counterfeiting Trade Agreement* [online]. 2012. (2010/C147/01). [cit. 2013-03-24]. Dostupné na internete: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-24_ACTA_EN.pdf.

46 Viď analýzu od Korffa a Browna vyššie, pozn. p. č. 6, bod 3., str. 57.

47 Rozhodnutie ESĽP vo veci *Vo. v. France, 53924/00, 08.07.2004* [online]. bod. 90 [cit. 2013-03-24]. Dostupné na internete: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61887.

rights,[48] v jej článkoch 9 (4)(5). Z toho dôvodu sú konania *inaudita altera parte*, kde nie je dotknutá strana vypočutá, len veľmi výnimočné, pričom musia byť stanovené dostatočné záruky ochrany dotknutej strany. Tu sa zdá, že ACTA takéto konania využíva neprimerane, bez ich nevyhnutnej potreby a bez dostatočných prostriedkov ochrany dotknutej strany.

Korff a Brown konštatujú, že vynechanie *de minimis* výnimiek z mandatórneho a drakoniánskeho režimu vynucovania trestnými sankciami predstavuje neadekvátnu ochranu práva na informácie, zákazu nezákonnej a bezdôvodnej prehliadky a zatknutia, práva na domovú slobodu a práva na pokojné užívanie majetku, a teda tieto práva porušuje. Bez jasných ustanovení v rámci civilnej ochrany PDV; zaručujúcich to, že súdne príkazy a predbežné opatrenia sa použijú len vo výnimočných a odôvodnených prípadoch, a že musia existovať dostatočné záruky na zabezpečenie princípu rovnosti v konaniach na ochranu PDV; je ACTA v rozpore s Dohovorom, Chartou a právom EU. Doplňujúco ako už bolo povedané, ACTA má charakter dohody, ktorá znižuje mieru dodržiavania ľudských práv a slobôd mimo krajín EU, a účasť EU na vykonávaní takých ustanovení ACTA by malo za následok porušenie princípu zakladajúcich zmlúv EU. Európski akademici konkrétne namietajú konflikt ACTA so Smernicou 2004/48/EC, keď Čl. 8(1) ACTA požaduje od zmluvných strán, aby ich súdy boli oprávnené nariadiť strane, aby upustila od porušovania PDV, resp. aby nariadili zákaz vstupu tovarov do obchodných kanálov, pričom predmetná smernica dáva štátom možnosť, aby umožnili nariadenie finančnej kompenzácie poškodenej strane namiesto predbežných opatrení. Tu sa ACTA zdá prísnejšia, resp. môže nastať konflikt práva pri jej uplatňovaní s právom EU.[49]

Problém je aj s výkladom ustanovení o náhrade škody upravenej v Čl. 9 ACTA. Je namietané, že niektoré z kritérií pre určenie výšky škody, napr. „*trhová cena porušovaného tovaru*" v Čl. 9(1), nemajú oporu v práve EU, konkrétne v Smernici 2004/48/EC, a nepresne reflektujú škodu spôsobenú porušenej strane. Zároveň nie sú jasné pravidlá stanovenia alternatívnej náhrady škody podľa Čl. 9(4), čo môže eventuálne viesť k ustanoveniu neprimerane vysokej škody kombinovaním Čl. 9(1) a Čl. 9(4).[50]

Tieto závery ukazujú na používanie neprimeraných opatrení namiesto miernejších a postačujúcich, nejasné rátanie výšky náhrady škody a iné nezrovnalosti na základe vágnych ustanovení ACTA, ako poukazujú viaceré analýzy.

Záver

Ako bolo v tejto práci analyzované, viaceré kompetentné štúdie sú znepokojené vágnosťou, nejasnosťou dohody ACTA. Tie následne znamenajú nejasnú interpretáciu podstatných pojmov, čo môže pri ich aplikácii v praxi spôsobiť nepredvídané následky, často porušujúc základné ľudské práva a slobody, ako bolo naznačené na viacerých miestach tejto práce. Je pravdepodobné, že táto vágnosť ostala v dohode po tom, čo komercializácii tajných rokovaní o ACTA na verejnosti spôsobila, že strany dohody museli niektoré ustanovenia o neproporcionálnych opatreniach odstrániť, no urobili tak bez riadneho vypracovania nových, koherentných ustanovení, možno i úmyselne. ACTA pravdepodobne nie je *prima facie*

---

48 European Parliament and The Council, *Directive 2004/48/EC of The European Parliament and The Council of 29 April 2004 on the enforcement of intellectual property rights* [online]. [cit. 2013-03-24]. Dostupné na internete: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF.

49 Viď *Opinion of European* academic, pozn. p. č. 27, bod. 1 Injunctions, str. 2.

50 Viď *Opinion of European* academic, pozn. p. č. 27, bod. 2 Damages, str. 2.

v rozpore s právom EU, Chartou a Dohovorom, keďže by sa musela implementovať aj v svetle predmetných noriem a judikatúry, no zlyháva v riadnom zabezpečení ochrany základných práv a slobôd vo svojom texte. Samozrejme, objasňujúce stanovisko by v tomto mohol dať Súdny dvor Európskej Únie, ak by poslanci Európskeho Parlamentu hlasovali o ACTA až po jeho rozhodnutí.

Informačná spoločnosť a medzinárodné právo

Zborník príspevkov zo VI. študentského sympózia konaného v dňoch 21. - 22. apríla 2013 v učebno-výcvikovom zariadení UPJŠ v Danišovciach

Zostavovatelia: Mgr. Adam Giertl
Mgr. Ľubica Gregová Širicová

Vydavateľ: Univerzita Pavla Jozefa Šafárika v Košiciach
Odborné poradenstvo: Univerzitná knižnica UPJŠ v Košiciach
http://www.upjs.sk/pracoviska/univerzitna-kniznica
Rok vydania: 2013
Náklad: 100 ks
Rozsah strán: 136
Rozsah: 9,8 AH
Vydanie: prvé
Tlač: EQUILIBRIA, s. r. o.

ISBN 978-80-8152-021-1 (tlačená verzia publikácie)
ISBN 978-80-8152-022-8 (e-publikácia)

ISBN 978-80-8152-027-3