PRÁVNICKÁ FAKULTA
MASARYKOVA UNIVERZITA

PRÁVO INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLÓGIÍ

ÚSTAV PRÁVA A TECHNOLÓGIÍ

DIZERTAČNÁ PRÁCA

ELEKTRONICKÝ DÔKAZNÝ PROSTRIEDOK

2019/2020

TOMÁŠ ABELOVSKÝ

Čestné vyhlásenie

Vyhlasujem, že som dizertačnú prácu na tému **Elektronický dôkazný prostriedok** spracoval sám. Všetky pramene a zdroje informácií, ktoré som použil k spísaniu tejto práce, boli citované v poznámkach pod čiarou a sú uvedené v zozname použitých prameňov a literatúry.

V Zürichu, 27. septembra 2020

Tomáš Abelovský

Abstrakt

Dizertačná práca má za cieľ vysvetliť vybrané právne otázky elektronického dôkazného prostriedku ako kľúčového elementu procesného práva v 21. storočí. Práca sa snaží obhájiť platnosť a význam zásady voľného hodnotenia dôkazov vo svetle elektronických dôkazných prostriedkov primárne v občianskom práve procesnom v Českej a Slovenskej republike. Práca ponúka taktiež exkurz do trestného práva procesného a zahraničnej procesnej úpravy.

Kľúčové slová:

elektronický dôkazný prostriedok, dôkaz, dokazovanie, virtualizácia, kyberpriestor, zásada voľného hodnotenia dôkazov, hodnotenie elektronického dôkazného prostriedku, rozhodovanie počítačom

Abstract

The dissertation aims to provide an explanation of the selected legal issues of electronic evidence as a key element of procedural law in the 21st century. The dissertation tries to defend the validity and significance of the principle of free evaluation of evidence in the light of electronic evidence primarily in civil procedural laws of the Czech and Slovak Republic. It offers an excursion into the criminal procedural law and foreign procedural laws.

Keywords:

electronic evidence, evidence, proving, virtualization, cyberspace, principle of free evaluation of evidence, evaluation of electronic evidence, computer decision-making

Ďakujem doc. JUDr. Radimovi Polčákovi Ph.D. za inšpiráciu, usmernenia a cenné rady počas celého môjho doktorandského štúdia.

Ďakujem Lenke. Bez jej podpory a trpezlivosti by táto práca nikdy nevznikla.

Obsah

Poznámky a použité skratky

Všeobecné skratky

ESĽP	Európsky súd pre ľudské práva
NS ČR	Nejvyšší soud České republiky
NS SR	Najvyšší súd Slovenskej republiky
NSS ČR	Nejvyšší správní soud České republiky
NSZ	Nejvyšší státní zastupitelství České republiky
OČTK	Orgány činné v trestnom konaní
SDEÚ	Súdny dvor Európskej únie
ÚS ČR	Ústavní soud České republiky
ÚS SR	Ústavný súd Slovenskej republiky

Právne predpisy

BD	Budapeštiansky dohovor o počítačovej kriminalite z 23. novembra 2001
CŘS	Věcný záměr civilního řádu soudního
CSP	Zákon č. 160/2015 Z.z., Civilný sporový poriadok
DŘ	Zákon č. 280/2009 Sb., Daňový řád
eIDAS	Nariadenie Európskeho parlamentu a rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
FRCP	The US Federal Rules of Civil Procedure (eff. Dec. 1, 2019)
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
Listina	Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod
MAR	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 596/2014 z 16. apríla 2014 o zneužívaní trhu (MAR) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES
NOZ	Zákon č. 89/2012 Sb., Občanský zákoník
OSP	Zákon č. 99/1963 Z.z., Občiansky súdny poriadok (zrušený)
OSŘ	Zákon č. 99/1963 Sb., Občanský soudní řád
SŘ	Zákon č. 500/2004 Sb., Správní řád
TP	Zákon č. 301/2005 Z.z., Trestný poriadok
TŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (Trestní řád)
TZ ČR	Zákon č. 40/2009 Sb., Trestní zákoník
TZ SR	Zákon č. 300/2005 Z. z., Trestný zákon.
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
ZEK	Zákon č. 351/2011 Z. z., o elektronických komunikáciách
ZFEÚ	Zmluva o fungovaní Európskej únie
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (Stand am 1. Juli 2020)
ZSŠ	Zákon č. 191/1950 Sb., Zákon směnečný a šekový

Poznámka
Pokiaľ nie je uvedené inak, citácie z pôvodného zdroja v českom jazyku sú zachované v pôvodnom znení a neprekladané. Citácie zdrojov z anglického a nemeckého jazyka sú preložené do slovenského jazyka autorom. Pokiaľ nie je uvedené inak, právny stav opísaný v práci je ku dňu 1.9.2020.

„I když se nikdo nedívá“- Ján Amos Komenský [1]

Úvod a cieľ práce

Svet elektronických technológií predstavuje v súčasnosti veľkú výzvu pre právnu vedu. Väčšina informácií je uchovávaná a prenášaná výlučne elektronickými prostriedkami. Je zrejmé, že čoraz viac informácií je virtualizovaných a v sústavnom pohybe. [2] Súdny proces, ktorého podstatnou časťou je dokazovanie, pracuje s informáciami. Popri odpovediach na *questio iuris* hľadá súd odpovede na *questio facti.* Dobrý dôkazný prostriedok vysvetľuje minulý dej, je oporou skutkového tvrdenia, má potenciál riešiť spoločenský problém a môže vyvolať zmeny aj v samotnej spoločnosti.[3]

Ako technológia ovplyvňuje tradičný proces dokazovania? Ako zabezpečiť dobrý elektronický dôkazný prostriedok?

Medzi elektronickým nosičom informácie a jeho hmatateľným výstupom, ktorý je nevyhnutný pre praktickú aplikáciu práva, existuje značná priepasť. Na jej prekonanie je potrebné vystavať pomyselný most, ktorého piliere sa opierajú o súčasne platné právo, ako aj o princípy a zásady teórie procesného dokazovania. Podľa Holländera má dokazovanie pre právne rozhodovanie okrem noetickej podstaty aj funkciu presvedčovania a argumentovania. [4] Tá je príslušná elektronickému vykonávaniu dôkazov. Neraz video alebo zvuk, resp. text emailu vo svojej vlastnej podobe vyzerajú ako zrkadlo reality minulých dejov. Preto je možné tiež hovoriť aj o oceňovaní dôkazu,

[1] Výrok Jána Amosa Komenského (Svět mravní, kap. Etika, podkap. O ctižádosti). Zdá sa, že v tomto etickom princípe je okrem ideálneho správania obsiahnutý aj rámec dobrého dokazovania, získavania, navrhovania a vykonávania dôkazných prostriedkov, ako aj ich hodnotenia. Komenského triáda poznať dobré, chcieť dobré a konať dobré, a to aj keď sa nikto nepozerá, je aplikovateľná aj pre súdny systém a jej zásadnú fázu dokazovania. Viď HÁBL, Jan. I když se nikdo nedívá: Fundamentální otázky etického vychovatelství. Pavel Mervart 2015.

[2] Napríklad podiel elektronických dát v podnikovom sektore sa za posledných 15 rokov zvýšil z 20% na 90%. PWC Česká Republika, s.r.o. Forenzní služby: eDiscovery [online]. [cit.1.9.2020]. Dostupné z: http://www.pwc.com/cz/cs/forenzni-sluzby/assets/pwc-vyhledavaci-technologie.pdf

[3] MADLEŇÁK, Ján. Threema, USB, mobily. Aké dôkazy súd nepripustil v prípade vraždy novinára Kuciaka. Týždeň. [online]. 2019 [cit.1.9.2020]. Dostupné z: https://www.tyzden.sk/politika/61159/threema-usb-mobily-ake-dokazy-sud-nepripustil-v-pripade-vrazdy-novinara-kuciaka/

[4] HOLLÄNDER, Pavel. Filosofie práva. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, ISBN 80-868-9896-2, Str.195.

resp. hľadaní jeho sily.[5] Tento proces je síce sfinalizovaný predložením úplného súhrnu dôkazov, avšak v predloženej práci tvrdíme, že správna bonifikácia dôkazných kvalít je o to viac dôležitejšia, ak ide o použitie elektronických dôkazných prostriedkov. Navyše, táto bonifikácia so sebou nesie určité riziká, ktoré je potrebné vyhodnotiť. Ide o riziká dôkazných chýb, justičných omylov a prijímania nespravodlivých rozhodnutí. V našej metafore je pre spojenie dvoch brehov pomyselným mostom nutné postaviť výsledky dokazovania do svetla poznania, ktoré bude založené na úsilí priblížiť sa zhode myšlienky so skutočnosťou (minulým dejom) v takej miere, ktorá zodpovedá požiadavkám overovania, ako aj falzifikovania, ktoré je možné v určitej dobe na túto mieru priblíženia aplikovať.[6] Každé dokazovanie smeruje k overeniu pravdivosti určitého tvrdenia. Každý dobre vykonaný dôkaz by mal predstavovať záruku reflektovania minulých dejov alebo súčasného stavu. Slovami Holländera *„fair spôsob vedenia dôkazného konania (ktoré je v trestnom procese spojené s aplikáciou najmä zásad rovnosti zbraní, prezumpcie neviny, práva na obhajobu, in dubio pro reo) sleduje jednak nachádzanie pravdy v konflikte proti sebe stojacich strán, a jednak snahu o minimalizáciu dôkazných chýb, justičných omylov, a tým aj minimalizáciu prijímania nespravodlivých rozhodnutí.“* [7] Je preto zrejmé, že existuje úzka väzba medzi kategóriou pravdivosti a povahou konania, akým je práve vykonanie dôkazu prostredníctvom elektronického dôkazného prostriedku. V predloženej práci predstavíme teoretickú, ale aj praktickú koncepciu takejto stavby, t.j. pomyselného mosta medzi digitálnym kyberpriestorom a zmyslami vnímateľným svetom.

V predloženej práci tvrdíme, že neexistujú fakty samy o sebe, ale iba fakty, ktoré prešli procesom našej interpretácie.[8] Proces interpretácie je nutné vnímať v kontexte virtualizácie elektronických dôkazných prostriedkov. V prípade dôkazov z technologických stromov,[9] tieto rekonštrukčné procesy a táto subsumpcia môžu trpieť a trpia nedokonalosťou. Na jednej strane existuje suma elektronických informácií,

[5] BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. Teorie práva. Vyd. 1. Praha: Eurolex Bohemia, 2001. ISBN 80-86432-13-0. Str.132.

[6] Ibid. HOLLÄNDER 2006, Str.201.

[7] Ibid. HOLLÄNDER 2006, Str.204.

[8] ŠKOP, Martin. Základní metodologie dokazovaní v právu. In: Dokazovanie v civilnom a trestnom konaní. Pezinok: Justičná akadémia Slovenskej republiky, 2012. ISBN 978-809-7020-743. Str. 13.

[9] Ide o narážku na sovietsku doktrínu opisujúcu „ovocie z otráveného stromu“.

ktoré majú alebo nemajú vlastnosti spôsobilé verifikovať isté tvrdenie, na druhej strane existuje vykonávateľ dôkazu s obmedzeným vnímaním týchto vlastností. Preto sa môže zdať, že limity sú dané nie len personálnou alebo inštitucionálnou nepripravenosťou na elektronické dokazovanie, ale aj tým, že zákonodarca s touto formou vykonania dokazovania doposiaľ priamo nepočítal. Ale je to naozaj tak?

Predložená práca sa snaží obhájiť platnosť a význam zásady voľného hodnotenia získaných elektronických dôkazných prostriedkov primárne v občianskom procesnom práve v českom a slovenskom priestore. Pre tento účel je nutné vykonať aj obmedzený exkurz do trestného procesného práva, najmä v otázkach vybraných druhov elektronických dôkazných prostriedkov. Navyše, na niektorých miestach je naša práca doplnená o komparatívnu analýzu anglo-amerického a švajčiarskeho dôkazného procesu. Ide o priblíženie konceptov, akým je napríklad *e-discovery* a opis elektronického dôkazného prostriedku, ktorý je určovaný kritériami, akými sú spoľahlivosť a integrita, pravdivosť a vierohodnosť, platnosť a zákonnosť.[10]

V tejto práci zastávame názor, že technológia neprináša fundamentálnu zmenu v procese dokazovania. [11] Napriek tomu je možné konštatovať, že jednou zo zaujímavých častí civilného a trestného práva procesného je elektronický dôkazný prostriedok vo svetle každodenného praktického použitia, ktorý sa zdá byť vo svojich výstupoch nejasný, ba dokonca deformovaný a často nepochopený.

Vzhľadom na vyššie uvedené pracujeme s nasledujúcimi piatimi výskumnými otázkami:

1. **Môže virtualizácia slúžiť ako vhodné východisko pri riešení aktuálnych spoločenských problémov v otázkach elektronického dokazovania?**
2. **Aké sú fundamenty a limity elektronického dôkazného prostriedku?**
    - Ako ovplyvňuje kategória kvality elektronického dôkazného prostriedku

[10] District Court of Maryland. Lorraine et al. v. Markel American Insurance Company [online]. 2007 [cit.1.9.2020]. Dostupné z: https://www.govinfo.gov/app/details/USCOURTS-mdd-1_06-cv-01893

[11] Podľa Polčáka sa ukazuje stála nutnosť jeho teoretického skúmania a následnej praktickej reflexie získaných poznatkov. POLČÁK, Radim. Internet a proměny práva. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3. Str.374 an.

proces dokazovania?

- Akú úlohu má zásada voľného hodnotenia dôkazov pri dokazovaní elektronickými dôkaznými prostriedkami?
- Akú úlohu má elektronický súdny spis pri dokazovaní elektronickými dôkaznými prostriedkami?

3. **Oslabuje kyberpriestor teritoriálnu výkonnú moc štátu voči jej virtualizovaným subjektom, a aký to má dopad na súdnu moc, resp. na elektronické dokazovanie?**
4. **Je možné uvažovať o rozhodovaní sudcom-počítačom? Aké sú výhody a východiská?**
5. **Ako nakladať so špecifickými druhmi elektronického dôkazného prostriedku?**
   - Akým spôsobom je možné získať, analyzovať, vykonať a hodnotiť elektronický dôkazný prostriedok pochádzajúci z osobných profilov sociálnych sietí alebo webových stránok na internete?
   - Aký je pohľad trestného procesného práva SR a ČR na zaisťovanie elektronického dôkazného prostriedku v podobe dátového nosiča alebo dát?
   - Kedy má emitent finančného nástroja povinnosť uverejniť informáciu o kyberútoku na jeho informačný systém a aký je proces zdokumentovania tohto útoku?
   - Priniesla by zmenka v elektronickej podobe vyššiu dôkaznú spoľahlivosť?

V 1. kapitole všeobecnej časti predložíme teoretické východiská virtualizácie. Predmetom tejto kapitoly bude proces virtualizácie a jeho vplyv na hodnoty v práve. Ponúkneme odpoveď na to, či môže virtualizácia slúžiť ako vhodná metóda pre nájdenie správnych východísk pri riešení aktuálnych spoločenských problémov, a to aj v čiastkových otázkach elektronického dokazovania. V 2. kapitole sa budeme venovať fundamentom elektronického dokazovania. Od virtualizovania elektronického dôkazného prostriedku prejdeme k všeobecným princípom dokazovania a zameriame sa na limity elektronického dokazovania. Načrtneme informačnú teóriu, ktorá súvisí s kategóriami kvality elektronického dôkazného prostriedku, a ktorá prináša nový

pohľad na predmet dokazovania. Ťažiskom tejto kapitoly bude zamyslenie sa nad zásadou voľného hodnotenia dôkazov. Pokúsime sa predstaviť teóriu rizika a ako je možné hodnotiť elektronické dôkazné prostriedky aj na základe ich rizík. Zameriame sa na elektronický spis, ktorý je praktickým a nevyhnutným prvkom procesu elektronického dokazovania. Predložíme analýzu výhod *e-spisu*. Budeme sa venovať komparatívnemu pohľadu s právom USA a vysvetlíme inštitút *e-discovery*. V 3. kapitole rozoberieme otázky súvisiace s informačnou suverenitou štátu a cezhraničným dokazovaním. Všeobecnú časť uzavrieme 4. kapitolou, v ktorej sa pokúsime načrtnúť teoretické východiská rozhodovania o elektronických dôkazoch počítačom.

V osobitnej časti popíšeme vybrané druhy elektronických dôkazných prostriedkov. Nakoľko táto téma je už pomerne dobre spracovaná existujúcou odbornou literatúrou, zameriame sa na partikulárne a medziodborové otázky, ktoré boli riešené počas nášho doktorandského štúdia. V 5. kapitole vysvetlíme proces dokazovania profilom sociálnej siete, webstránkou a IP adresou z pohľadu trestného práva procesného. V 6. kapitole prinesieme pohľad na procesný úkon zaistenia elektronického dôkazného prostriedku vo svetle rekodifikácie trestného poriadku v ČR. V 7. kapitole popíšeme koncept vnútornej informácie súkromnej spoločnosti o kyberútoku, a prečo všeobecné otázky elektronického dokazovania hrajú dôležitú úlohu pri zaisťovaní tejto informácie. Vysvetlíme povinnosti regulovaných osôb, a to ako s touto informáciou naložiť. Prácu v 8. kapitole ukončíme úvahou o elektronickej zmenke. Tá by mohla predstavovať elektronický dokument a zároveň takmer dokonalý elektronický dôkazný prostriedok v civilnom práve.

Práca má za cieľ predložiť obraz o dôležitosti vybraných právnych otázok elektronického dôkazného prostriedku ako kľúčového elementu súkromného práva procesného v 21. storočí.

Všeobecná časť: Elektronický dôkazný prostriedok

V súčasnosti je človek svedkom mnohých technologických vplyvov na spoločenské vzťahy. Stranou neostáva ani proces týkajúci sa rozhodovania súdnych sporov. Je možné uviesť, že súdny proces je jednou z najstarších formalizovaných spoločenských udalostí. Už v starovekom Ríme sa kládol značný dôraz na rôzne technikálie vedenia súdneho sporu. Aj keď v mnohých smeroch išlo o zadosťučineniu tradícii alebo náboženstvu, technologické prvky nikdy neostali na okraji záujmu. Súdny proces, či už súkromný alebo verejný, sporový alebo nesporový, vždy smeruje k formálnemu potvrdeniu alebo vyvráteniu určitých skutočností, čo má zásadný vplyv na práva a povinností zúčastnených. Je dôležité, aby právna veda stíhala technicky pokrok, ale zároveň do oblasti procesného práva implementovala iba tie technologické nástroje, ktoré sú funkčné, udržateľné a účelné.

Nasledujúca časť tejto práce si kladie za cieľ zodpovedať otázku, čo je to elektronický dôkazný prostriedok? Aby táto otázka mohla byť zodpovedaná, je potrebné vytýčiť hranice tejto úvahy. Súdnym procesom pre potreby tejto úvahy bude súkromno-právne sporové konanie podľa OSŘ alebo OSP. Úvaha sa zameria na všeobecné otázky virtualizácie, definuje elektronický dôkazný prostriedok, ktorý je kľúčovým aspektom informatizácie súdneho konania a elektronického dokazovania a popíše otázky informačnej suverenity a cezhraničného dokazovania. Všeobecná časť bude zakončená analýzou teoretickej otázky automatizovaného rozhodovania o elektronických dôkazoch. Predložená úvaha má síce analytické a popisné črty, ale jej záver spočíva v predložení všeobecných odporúčaní vhodných pre akúkoľvek implementáciu technológií do súdneho konania. Pomocou komparatívnej metódy budú predložené postrehy zo súčasných implementácií technologických nástrojov do súdnych procesov alebo alternatívnych konaní, akými sú napr. konania týkajúce sa doménových mien. Stranou neostane ani pohľad na slovenskú právnu úpravu a existujúce riešenia v anglo-americkom systéme práva.

1. Virtualizácia*

1.1. Úvodné poznámky

Virtualizácia ako prítomný fenomén predstavuje jednu z kľúčových a zložitých filozofických otázok okolitého sveta. Delleuze začína svoju slávnu esej tým, že považuje filozofiu za teóriu mnohorakosti, ktorá pozostáva z aktuálnych a virtuálnych častí.[12] Už samotná intuícia bez širšej vedomosti o danej problematike napovedá, že virtualita je všade prítomná, ale zahalená do rúška neznámeho. Často sa nesprávne zamieňa s ilúziou, resp. fikciou. V posledných desaťročiach sa tento pojem začal spájať s viditeľnou vlastnosťou informačných technológii. Slovné spojenia ako „virtuálna realita" alebo „virtuálny" sa stali symbolom úteku človeka pred realitou a jeho novej vízie v populárnych kultúrnych médiách, počnúc fantastickou beletriou až po celosvetové herné simulácie alebo sociálne internetové siete. Dokonca sa začalo hovoriť o *proteusovskom efekte*, kedy jedinec, ktorý ovláda virtuálnu postavu sa stotožňuje a adaptuje s touto postavou – avatarom (t.j. digitálna sebareprezentácia).[13] Je potrebné zdôrazniť, že ani konvenčné sociálne interakcie neostali úplne bez dotyku virtuality.[14] Používatelia rôznych technologických mediátorov[15] sa tak virtualizujú a aktualizujú. Môže sa zdať, že vďaka technológiám je právo postavené pred radikálne zmeny. V skutočnosti však žiadna technológia nemení fundamentálne základy, resp. jeho východiskové hodnoty.[16] Napriek tomu je na mieste si položiť nasledujúcu otázku:

*Táto kapitola vychádza z publikovaného článku ABELOVSKÝ, Tomáš. Virtualizácia ako metóda riešenia spoločenských problémov, Právny obzor, 2015, roč. 98. č. 2., Str. 164-177.

[12] DELEUZE, Gilles; GUATTARI, Felix. A thousand plateaus: capitalism and schizophrenia. London: Athlone Press, 1988. ISBN 0485120585. Str.148.

[13] CAVAGNETTO, Stefano; GAHIR, Bruce. Multiple personalities and the proteus effect in collaborative virtual environments. A. Wittgensteinian viewpoint. Masaryk University Journal of Law and Technology. Brno: Masaryk University. Faculty of Law, 2011, roč. 5, č. 2, Str. 177–197.

[14] Za zmienku stojí „nový" pohľad trestného práva na trestné činy vo virtuálnych svetoch, Viď napr. GŘIVNA, Tomáš. Virtual crimes. Masaryk University Journal of Law and Technology. Brno: Masaryk University. Faculty of Law, 2008, roč. 2, č. 1, Str. 97-104.

[15] V dnešnom ponímaní to môže byť počítač, telefón, TV, tablet, chladnička, automobil, lietadlo alebo akýkoľvek iný technologický artefakt s centrálnou procesnou jednotkou a sieťovým rozhraním s možnosťou konektivity na internet alebo inú sieť s potenciálom virtualizácie.

[16] POLČÁK, Radim. Dokazování elektronickými dokumenty. In: Dokazovanie v civilnom a trestnom konaní. Kolektív autorov. Pezinok, Justičná akadémia Slovenskej republiky, 2012. ISBN 978-80-970207-4-3. Str. 61.

Môže virtualizácia, resp. virtualizovanie,[17] slúžiť ako vhodná metóda pre nájdenie správnych východísk pri riešení aktuálnych spoločenských problémov v otázkach elektronického dokazovania?

1.2. Spoločenský problém

Aby sme pochopili virtualizovanie elektronických dôkazných prostriedkov a procesu dokazovania, bude potrebné osvetliť prečo vizualizácia môže byť metódou riešenia spoločenského problému alebo konfliktu.

S nadnesením je možné povedať, že spoločenský problém je niekedy vec potrebná. Problém alebo ním vyvolaná situácia nás núti premýšľať. Spôsobené nepohodlie nám prináša tlak k aktivite, neinformovanosť vyvoláva otázky a pri ich pochopení nenahraditeľnú skúsenosť. Farbisto, až militantne to opisuje prvý sluha v Shakespearovej tragédii Coriolanus: *„Nie je nad vojnu. Vojna a mier, to je ako deň a noc. Vojna je svižný pohyb, skutočný zvuk a vzrušenie. Mier je umŕtvená, otupená, hluchá, ospalá a hlúpa nuda. Vzíde z nej viac parchantov ako vo vojne pomrie chlapov.“*[18] Tak ako sociálna veda rieši sociálne konflikty, medicína zdravotné neduhy, tak právo pristupuje k lúskaniu niektorých spoločenských problémov a peripetií. Teória práva tu hovorí o entropii, na ktorú reaguje právo s otvorenou náručou bezpečných normatívnych riešení, autoritatívnych príkazov a interpretačných názorov. Podľa Knappa sa spoločnosť vyznačuje tým, že v nej vzniká veľké neusporiadanie konkurujúcich si ľudských záujmov a správaní, ktoré kedysi Hobbes nazval *„vojnou každého proti každému.“*[19] Entropia predstavuje z hľadiska svojej genézy špeciálny pojem, majúci svoje domovské právo vo fyzikálnej vede. Ako pripomínajú niektorí autori, pojem sa používa spravidla v súvislosti s filozofickými implikáciami druhého termodynamického zákona, niekedy označovaného aj ako *entropický*, pretože práve entropia v ňom zohráva kľúčovú úlohu.[20] Entropia má za následok, že systémové vzťahy pokiaľ sú ponechané ladom a skladom, postupom času strácajú svoju

[17] Virtualizovanie je v tejto úvahe chápané ako presun – postup od aktuálneho k virtuálnemu. Rozdiel medzi antonymami aktuálny a virtuálny bude vysvetlený ďalej.

[18] HILSKÝ, Martin. SHAKESPEARE, William. Slovník citátů z Díla Williama Shakespeara. Vyd. 1. Praha: Academia. ISBN 978-80-200-2193-9. Str. 371.

[19] KNAPP, Viktor. Teorie práva. 1. vyd. Praha, 1995. Právnické učebnice (C.H. Beck). ISBN 3406401775. Str. 32.

[20] PAULOV, Ján. Entropia a modelovanie. ORGANON F, 9(1). Filozofický ústav Slovenskej akadémie vied, 2002, Str. 157.

organizovanosť a zákonite dôjde k ich rozpadu.[21] Proces entropie je možné prirovnať k zvetrávaniu piva (prepadnutie peny po jeho načapovaní), ku chátraniu stavby alebo ku korózii plechu.[22] Entropia v práve preto značí mieru ambivalencie – protichodných postojov, resp. neusporiadanosti právnych vzťahov. Prečo však táto entropia existuje, resp. je na mieste sa spýtať, kde sú jej príčiny?

Polčák považuje tento stav neorganizovanosti za stav, ktorý je vyvolaný nedostatkom informovanosti, resp. v informácii hľadá protipól entropie.[23] Antidotum na entropiu je informácia s vlastnosťou pravdivosti. Na druhú stranu za entropiu nie je možné považovať len úplné bezprávie. Totiž každý pohyb, chvenie alebo napnutie spôsobuje disbalanc s rôznym výsledným efektom. Ten vyústi alebo má v sebe potenciál vyústiť do problému, ktorý nie je zväčša statický, ale pokračuje v dynamickom reťazení ďalších interakcií, pnutí a praskaní. Výsledkom sú neorganizované systémové vzťahy.

Podľa Knappa potreba sebazáchovy spoločnosti plodí nielen moc (regulátor ľudského správania), ale aj silnú trojicu motívov ľudského správania regulovaného mocou – potreba, účel a záujem. Preto ľudské záujmy, ktoré sa identifikujú s touto triádou motívov môžu vyvolávať konflikty, čo má za následok, že v spoločnosti vzniká potreba záväzného riešenia konfliktných situácií.[24] Riešeniu sporov, či už v civilnom alebo trestnom práve, predchádza proces dokazovania. Ide o vyhľadanie, navrhnutie a vykonanie dôkazov. Je to právom stanovený procesný postup, ktorý pomáha súdu (alebo inému rozhodovaciemu orgánu) získať poznatky o rôznych skutočnostiach dôležitých pre rozhodnutie sporu - spoločenského problému. Avšak pred tým než pristúpime k objasneniu procesu dokazovania vo svetle moderných technológií, je potrebné odpovedať na základnú otázku, aká je to potreba, ktorá ženie subjekty práva k riešeniu neusporiadanosti?

[21] POLČÁK. Právo a evropská informační společnost. vyd. Brno: Masarykova univerzita, 2009. Spisy Právnické fakulty Masarykovy univerzity v Brně, sv. 344. ISBN 9788021048850. Str. 13.

[22] KÜHN, Zdeněk, Michal BOBEK a Radim POLČÁK. Judikatura a právní argumentace: teoretické a praktické aspekty práce s judikaturou. Vyd. 1. Praha: Auditorium, 2006. ISBN 80-903786-0-9. Str. 143.

[23] Ibid. POLČÁK, Právo a evropská informační společnost. Str. 15.

[24] Ibid. KNAPP, Str. 31.

1.3. Potreba riešenia entropie a hodnoty

Einsteinovi je pripisovaný výrok, že „*nie je možné vyriešiť problém takým spôsobom myslenia, aký bol použitý v čase jeho vytvorenia.*“[25] Potreba identifikácie a regulácie spoločenských konfliktov je imanentná ľudskému pokoleniu od nepamäti. Avšak prítomnosť tejto potreby vo vedomí človeka nezaručuje správny smer jeho konania. Ide skôr o determinované motívy, ktoré sú svojou podstatou rôzne. Je možné konštatovať, že spoločným spojivom ostáva strach pred chaosom a vôľa stabilizovať pomery pred ich deštrukciou. A to aj s vedomím, že dosiahnuť všeobecnú absolútnu rovnováhu je neuskutočniteľné. Totiž pre naplnenie tohto ambiciózneho plánu by sa musela metóda harmonizovania (ak si pod ňou predstavíme čokoľvek v rámci výkonu štátnej moci, proces dokazovania, normotvorby alebo rozhodovania) kvalitatívne stotožniť s požadovaným cieľom. Musela by s ním takpovediac splynúť, čím by zanikol problém, ale aj metóda riešenia, ktorá by sa stala obsolentnou. Avšak to nevylučuje rozhodnutie priblížiť sa k tomuto majáku ideálu. Dôležité je identifikovať svetlo, ktoré vyžaruje kvalitná právna legislatíva, resp. dobrý kód, [26] dobrá rozhodovacia činnosť, dobré dokazovanie, koherentné a predvídateľné fungovanie súdnej moci a v neposlednom rade neustále zdokonaľované právne vedomie zúčastnených.[27] Preto právo a jemu vlastný regulatívny normatívny systém predstavuje silný nástroj riešenia spoločenských problémov. Právo ako sociálny fenomén je jedným z najvýznamnejších prostriedkov stabilizácie sociálnych vzťahov. Právo je považované za synonymum pojmu poriadok.[28]

Ak hovoríme o virtualizovanom riešení spoločenských problémov, je potrebné zdôrazniť, že virtualizácia sama o sebe podľa Lévyho nemá hodnotovú vlastnosť. Nie je dobrá, ani zlá a nie je dokonca ani neutrálna. Virtualizácia (čohokoľvek v spojení

[25] CALAPRICE, A., ed. The New Quotable Einstein, Princeton University Press; 2000, Str.317.

[26] Myšlienka kódu ako zákona internetu pochádza z pera Lawrenca Lessiga. Viď LESSIG, Lawrence. Code: version 2.0. New York: Member of the Perseus Books Group, 2006. ISBN 04-650-3914-6.

[27] Polčák hovorí o unikátnej funkcii informácie, ktorá dokáže organizovať systémy a čeliť rastu entropie, preto potom predpokladom organizovanej spoločnosti je jej informovanosť. Viď Ibid. POLČÁK. Internet a proměny práva. Str. 274.

[28] BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. Teorie práva. Vyd. 1. Praha: Eurolex Bohemia, 2001. ISBN 8086432130. Str. 274.

s človekom) demonštruje najzakladanejšiu schopnosť človeka odlišovať sa od okolia a svojich blízkych, tzv. heterogenézu. [29] Virtualizácia ako metóda riešenia spoločenských konfliktov však môže pootvoriť bránu axiologických otázok informačnej spoločnosti. Ide o spoločnosť, ktorá prirodzeným spôsobom využíva výdobytky informačných a komunikačných technológií za účelom dosiahnutia vyššej informovanosti, a to do takej miery, aby bola schopná odstraňovať neusporiadanosť vlastných sociálnych vzťahov. Je prirodzené, že vývoj ľudstva napĺňa svoj apetít po väčšej informovanosti. S tým súvisí jeho neustále informačno-technologické napredovanie, vývoj technológii a neustály posun k metódam, ktoré uľahčujú proces virtualizovania (napr. elektronický spis). Polčák tu zdôrazňuje aspekt prirodzenosti, nakoľko veda o kybernetike už dávno predpovedala, že ide o jeden z najzakladanejších prejavov života.[30] Je možné vidieť, že táto rapídne naštartovaná evolúcia so sebou nesie aj znovuobjavovanie existujúcich hraníc základných práv a slobôd človeka. Spoločnosť si postupne nasadzuje nové okuliare pre čítanie starého *Textu*.[31] Opäť a opäť zisťuje, že základné hodnoty ostávajú nemenné. [32] Ako Polčák uvádza, premenami v skutočnosti prechádzajú len partikularity. Avšak táto skutočnosť zdôrazňuje nutnosť ďalšieho teoretického skúmania fundamentu práva.[33] Miestami je cítiť dopyt po spomalení technologických krokov a počuť hlasy volajúce po návrate. Nové dioptrie na okuliaroch a súvisiace procesy sú podrobované odbornej kritike, skúmaniu a hľadaniu interpretačných korelácii s fundamentom práva. Objavuje sa otázka, ako dlho budú slúžiť nové okuliare a či nepokazia náš zrak, resp. nesedeli staršie pohodlnejšie? Avšak pozorný čitateľ pochopí, že správne sa je pýtať, k čomu vlastne tie okuliare slúžia a aká je podstata videného *Textu*.

---

[29] LÉVY, Pierre. Becoming virtual: reality in the Digital Age. New York, c1998. ISBN 0306457881. Str.16.

[30] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 274.

[31] Za *Text* považujeme nemenné hodnoty, princípy a fundamenty dobrého fungovania spoločnosti a spoločenského zriadenia.

[32] Abstraktné a hodnotové právne normy, resp. hodnotovo zameraná právna interpretácia je svojou podstatou veľmi blízka právnemu smeru, ktorý sa snaží identifikovať hranice hodnôt. Príkladom môže byť v Nemecku prevládajúca hodnotová jurisprudencia (Wertungsjurisprudenz), ktorá sa orientuje najmä na teleologický výklad. „*Hodnotová jurisprudence vychází ze samozřejmého (?) předpokladu, že zákonodárce není jenom loutka, která je manipulovaná nějakými zájmy, ale že on sám k nim zaujímá určité hodnotící stanovisko a podle toho pak fixuje právní normu.*“ Viď SOBEK, Tomáš. Nemorální morálka. In: Jiné právo [online]. [cit.1.9.2020]. Dostupné z: http://jinepravo.blogspot.sk/2010/07/tomas-sobek-nemoralni-moralka.html

[33] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 374.

Z pohľadu analytickej filozofie v prípade hodnôt Wittgenstein hovorí o limite ľudského jazyka, resp. jeho logickej štruktúry. Podľa neho je tu stále niečo vonkajšie, „*nad múrmi,*" o ktoré je opretý náš rebrík, po ktorom sa šplháme, niečo nevysloviteľné. Jeho slovami o hodnotách „*to sa ukazuje, ale nevyslovuje.*" Preto ľudská logika jazyka tu neumožní hovoriť o veciach etických či náboženských. Jednoducho nemajú čo zobrazovať.[34] Veda sa zaoberá svetom a rišou faktov. Ako sa majú veci na svete je úplne náhodné, a preto nepodstatné. Veci na svete sa majú tak, ako sa práve majú, a mohli by sa mať aj inak.[35] Môže sa zdať, že prísnou logikou by bolo možné odsunúť všetky metafyzické otázky na bok. Avšak podľa názoru samotného Wittgensteina, o čom svedčí aj jeho hádka na jednom zo sedení viedenského krúžku, záležitosti hodnôt nemôžu byť nepodstatné, sú totiž „*príliš dôležité.*"[36] Svet faktov a hodnôt je absolútne odlišný. Výroky o svete faktov by sa nemali používať k popisu sveta hodnôt. Podľa Wittgensteina na hodnoty je možné pozerať tak, že sú transcendované svetom faktov. Totiž ležia za jeho hranicami. Aj keď dielo v kantovskom duchu s názvom *Tractatus logico-philosophicus* a v ňom obsiahnutý predmetný argument je už prekonaný (sám autor ho odvrhol vo svojej neskoršej práci), jedno z možných ponaučení toho, o čo Wittgensteinovi išlo v jeho rannom diele je možné vidieť v tom, že sa snažil vybudovať obranný val na ochranu práve týchto hodnôt pred devastujúcimi zásahmi vedy. Komentátori Wittgensteina tu hovoria o príťažlivej negatívnej definícii.[37] Takáto negatívna definícia ako jediná môže kontúrami opísať hranice vyššie spomínaného *Textu.* Je si možné povzdychnúť, škoda že tu Wittgenstein nepoužil radšej kresbu, ako to urobil Antoine de Saint-Exupéry v prípade nakreslenej debničky s ovečkou pre Malého princa. Pre lepšiu funkciu ochranného valu, ktorý bude obraňovať *Text*, môže informačnej spoločnosti slúžiť práve racionálne zvolená virtualizácia jednotlivých častí spoločenských vzťahov. Či už pôjde o virtualizáciu zverejňovania právnych predpisov, judikatúry a súvisiacich právnych komentárov alebo o lepšiu virtualizáciu

[34] WITTGENSTEIN, Ludwig. Tractatus logico-philosophicus. Kalligram, Bratislava, 2003. Str. 171. bod 6.522.

[35] Ibid. WITTGENSTEIN. Str. 167. bod 6.41.

[36] A j keď ide o parafrázovaný komiksový príbeh, priama reč Wittgensteina k členom Viedenského krúžku, ktorí odsudzujú „metafyziku" vystihuje jeho názor na vec: *„The meaning of the „Tractatus" has completly escaped you."* DOXIADES. Logicomix. 1st U.S. ed. New York: Bloomsbury, 2009. ISBN 1-59691-452-1. Str. 222

[37] GRAYLING.Antohny. Wittgenstein: průvodce pro každého. 1. vyd. v českém jazyce. Praha: Dokořán, 2007. ISBN 9788073630775. Str. 61.

procesu dokazovania, vždy je prvoradým cieľom lepšie pochopenie podstaty samotného *Textu.*

1.4. Virtualizácia ako metóda

Právna teória rozoznáva spôsoby, akými dochádza k vyrovnaniu alebo zníženiu entropie spoločenských vzťahov. Prostriedkami môže byť voľný trh alebo autoritatívny a zároveň efektívny systém záväzných pravidiel ľudského správania alebo efektívne vyhľadávanie a hodnotenie elektronických dôkazných prostriedkov. Jednou z metód na dosiahnutie tohto prostriedku je metóda už uvedenej vedomej virtualizácie spoločenských vzťahov v nadväznosti na procesy aplikácie práva.

Ak hovoríme o virtualizácii alebo virtualite, nie je možné rozmýšľať len o digitálnom svete. Pojem *virtuálny* sa používa v počítačovom žargóne pre popísanie situácie, kedy určitá skutočnosť má svoj pomyselný a neuchopiteľný obraz takmer totožnej náhrady. Príkladom môže byť virtuálna pamäť, ktorá supluje fyzickú RAM pamäť počítača tým, že vytvára kvázi súbor priamo na jeho harddisku.[38] Schields vysvetľuje význam pojmu virtuálny na slovnom príklade, kde je možné popísať budúcu úlohu ako „*virtuálne dokončenú*“ s cieľom presvedčiť adresáta našej odpovede o tom, že je „skutočne“, ale nie „aktuálne (súčasne)“ dokončená.[39] Je nutné poukázať na to, že sa často tento pojem nestretne s úplným pochopením ani u odbornej verejnosti.[40] Virtualizácia totiž nemôže byť redukovaná len na zmiznutie alebo nejakú dematerializáciu objektu alebo osoby. Je potrebné si uvedomiť, že pravým opakom virtuálneho nie je reálne, ale aktuálne. Podľa Deleuza *„aktualizácia prislúcha vždy k virtuálnemu. Aktualizácia virtuálneho je singularita, kde aktuálne je samo o sebe konštituovanou individualitou. Aktuálne padá z roviny (imanencie) ako ovocie, kým*

[38] Viď POSTER, Mark. Postmodern Virtualities. In: Personal web page: UCI History Department Faculty [online]. 1995 [cit. 1.9.2020]. Dostupné z: http://www.csun.edu/~snk1966/Pomovirt.htm

[39] SCHIELDS, Rob. The Role of the Virtual in Knowledge-Based Economies, Organizations, and Localities. In: SEED Journal Semiotics, Evolution, Energy, and Developmen [online]. 2020 [cit.1.9.2020]. Dostupné z: http://see.library.utoronto.ca/SEED/Vol2-4/shields.html

[40] Viď napr. ZOUBKOVÁ, Ivana a Jana FIRSTOVÁ. Kriminologie: aktuální problémy. Vyd. 1. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-395-6. Str. 33.

aktualizácia ho uvádza späť do tejto roviny ako do niečoho, čo obracia objekt späť do subjektu.“[41]

Lévy považuje virtuálne jestvovanie za plodný a silný mód bytia, ktorý rozširuje proces kreativity. Tento mód z filozofického pohľadu mení chápanie samozrejmosti okamžitej fyzickej prítomnosti. Proces virtualizácie, postup od aktuálneho módu do módu virtuálneho, sa dá chápať ako reverzná aktualizácia. Čo je však najdôležitejšie a pre túto prácu osobitne podstatné, virtualizácia v sebe zahŕňa zmenu identity, prechod od konkrétneho riešenia ku všeobecnej nevyriešenej problematike.[42] Pojem virtuálneho priestoru si môžeme priblížiť na praktickom príklade tak, že sa zamyslíme nad otázkou, kde konkrétne sa uskutočňuje telefonický hovor?[43] Podľa názoru Ehrentrautovej človek nemôže jestvovať v zmiešanej realite, resp. vo virtuálnom priestore naveky – *„v istom bode telefónna konverzácia skončí a jeho mód prechádza do stavu offline.“*[44] Môžeme konštatovať, že sme svedkami virtualizačnej vlny. More, po ktorom sa plavíme za pomyselným majákom je plné týchto vĺn. Preto je logické sa pýtať, či môže existovať svet bez virtualizácie?

Prísne v duchu wittgensteinovskej logiky by virtualizácia nemusela byť nevyhnutne prítomná. Išlo by však len o myšlienkový konštrukt, v ktorom by nejestvoval život. Virtualizácia, ale aj aktualizácia, sú prejavom života a nevyhnutnou súčasťou konštruovania reality. Otázkou by bolo, či o takomto svete – myšlienkovom konštrukte je vôbec možné zmýšľať. Preto najdôslednejšie bude skúmať virtualizáciu z praktického hľadiska s prihliadnutím k všeobecnej otázke o jej úspešnosti. Virtualizácia podľa Polčáka predstavuje zmenu vonkajších znakov určitej štruktúry (predmetu virtualizácie) pri zachovaní jej elementárnej podstaty. Úspešnosť akéhokoľvek procesu virtualizácie bude determinovaná dynamikou (rýchlosťami) v organizácii virtualizovaných štruktúr. Tento proces spôsobuje odpadnutie niektorých

[41] Ibid. DELEUZE, Gilles; GUATTARI, Felix. Str. 150.

[42] Ibid LÉVY, Pierre. Str. 44.

[43] Lévy popisuje „virtuálne“ ako doslovne „nie tam (not there)“, čo značí, že nejde o rovnaký fyzický priestor, na aký sme zvyknutý v prvom digitálnom veku. Viď Ibid LÉVY, Pierre. Str. 27.

[44] EHRENTRAUT, Judy. Mark Poster's "Postmodern Virtualities" and Pierre Levy's "Becoming Virtual". In: Simulation Space: Cyberspace, Critical Theory, Gaming [online]. [cit.1.9.2020]. Dostupné z: http://thesimulationspace.wordpress.com/2013/07/05/mark-posters-postmodern-virtualities-and-pierre-levys-becoming-virtual/

problematických aspektov fungovania príslušného systému, pričom však iné problémy pribúdajú.[45]

Vráťme sa na chvíľu k už spomenutým determinovaným motívom konajúcich a zúčastnených pri riešení spoločenských problémov (napr. vo forme podanej žaloby, alebo návrhu na vykonanie dôkazu). Ak tvrdíme, že virtualizácia je pohyb od aktuálneho k virtuálnemu (tzv. reverzná aktualizácia) objavuje sa otázka, akú kvalitu bude mať takéto konanie a či sa vôbec hodnotový rámec konania zmení, resp. bude sa automaticky vzťahovať na lepšie vyriešenie entropie spoločenských vzťahov?

Pre demonštráciu si predstavme nasledujúci myšlienkový experiment s Platónovym mýtickým príbehom *Gýgovho prsteňa.*[46] Pripusťme, že takýto prsteň s ohromujúcou mocou efektu prsteňu princeznej Arabely je naozaj skutočný. Chudobný a jednoduchý pastier Gýges, ktorý si nažíval v úplnom pokoji, objaví takýto prsteň. Otočením kameňa na prsteni sa stane neviditeľný. V extrémnej polohe je tu možné nájsť paralelu s virtualizáciou, s vlastným procesom ľudského odlišovania sa, tak ako ju popísal Lévy. Pastier od aktuálneho módu (jestvuje tu a teraz) bytia prešiel do virtuálneho módu (jestvuje kdekoľvek a akokoľvek). Nejde len o nadobudnutie novej vlastnosti, neviditeľnosti. Nehľadajme príčiny tejto technológie, ktorá by bola bezo sporu ekonomicky úspešná. Sústreďme sa na kvalitu konania. Gýges využil túto skutočnosť, nepozorovane sa premiestnil (teleportoval) do panovníckeho sídla, zviedol manželku miestneho kráľa a následne kráľa aj zavraždil (zabíjal so značnou výhodou nepoznanej premeny). Aktualizoval tak svoj virtuálny mód jestvovania, ktorý mu umožnil nové druhy funkcionalít, t.j. vyriešiť ním videné konflikty, problémy a spolu s jeho „tajnou podobou“ mu inicioval novú dynamickú spoluprácu medzi aktuálnym a virtuálnym.

Predložený myšlienkový experiment spočíva opäť na hodnotách. Glaucon si v dialógu so Sokratom kladie rečnícku otázku s odpoveďou *„keby boli také prstene dva a jeden z nich by si nastrčil človek spravodlivý, druhý nespravodlivý, nebol by asi ako sa zdá, nikto z takého železa, aby zotrval v spravodlivosti a mal dosť síl zdržovať sa cudzieho majetku, nedotýkať sa ho, aj keby by mu bolo voľno brať si napríklad z trhu*

[45] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 258.

[46] PLATO., G. GRUBE a C. REEVE. Republic. Indianapolis: Hackett Pub. Co., xx, 300 p. ISBN 08-722-0136-8. Str. 31.

bez bázne všetko čo by chcel, vchádzať do domov a obcovať s kýmkoľvek by chcel, ale aj zabíjať a z pút vyprosťovať kohokoľvek by chcel, ale aj ostatné veci na svete konať ako nejaký boh. Takto konajúci nekonal by nič iné než ten druhý, ale práve obaja by smerovali k rovnakému cieľu.“ [47] Inak povedané, spravodlivý človek koná spravodlivo, spravodlivý neviditeľný človek nekoná spravodlivo.[48] Možno je na mieste spomenúť vyššie uvedený výrok – imperatív J. A. Komenského, *„aj keď sa nikto nepozerá.“* Príbeh v nás vyvolá zaujímavú reakciu, značný odpor ku kvalite konania Gýgesa. Pýtame sa, prečo s nami tak otrasie? Je to aspekt príbehu v podobe virtualizácie, ktorého imanentným znakom je neviditeľnosť? Žeby Gýges nahradil morálne ospravedlnenie praktickou účinnosťou? Gýges dokonal zločin a nie je potrestaný a ani odsúdený, spáchal ho totiž bez ťažkostí a v najvyššej možnej technologickej dokonalosti. Navyše mu ani neprebehlo hlavou, či je jeho konanie vôbec správne. Avšak ako poznamenávajú niektorí autori, účelnosť nemusí byť cnosť.[49]

Odpoveď hľadajme v súčasnom svete. S prípadom virtualizácie sa môžeme stretnúť aj v prípade nasadenia systému bezpilotných bojových lietadiel, tzv. dronov.[50] Človek – vojak prostredníctvom hardvéru a jeho softvéru využíva virtualizované bojové prostriedky ovládané globálnou vojenskou počítačovou sieťou. Deteritorializácia ako jeden z primárnych znakov virtualizácie je v tomto príklade úplne zrejmý. [51] Zbraň v ruke vojaka nahradzuje riadená technológia s ovládačom

[47] PICHA, Marek. 100 myšlenkových experimentů ve filozofii. Vyd. 1. Praha: Dybbuk, 2013. ISBN 978-80-7438-096-9. Str.128.

[48] Ibid. PICHA, Marek. Str.128.

[49] KAAG, John a Sarah KREPS. Morálne riziká dronov: Preklad ŠKODA, Rastislav. In: Zošity humanistov [online]. 2012. vyd. [cit.1.9.2020]. Dostupné z: http://www.zosity-humanistov.sk/2012/08/moralne-rizika-dronov/

[50] Napriek tvrdej kritike dronov existujú aj ich zástancovia, a to aj z radov právnikov. Viď napr. CALO, Ryan. Bad laws would hurt good drones. In: CNN.COM: Special to CNN [online]. [cit.1.9.2020]. Dostupné z: http://edition.cnn.com/2013/03/05/opinion/calo-drones/ alebo CALO, Ryan. The drone as privacy catalyst, Stanford Law Review, Vol. 64, 2011. Str.29.

[51] Deteritorializácia je filozofický pojem predstavený Deleuzom a Guattarim, ktorý môže značiť prevzatie kontroly a poriadku mimo krajinu alebo územie pôvodu. *„Against the Oedipal and oedipalized territorialities (Family, Church, School, Nation, Party), and especially the territoriality of the individual, Anti-Oedipus seeks to discover the "deterritorialized" flows of desire, the flows that have not been reduced to the Oedipal codes and the neuroticized territorialities, the desiring-machines that escape such codes as lines of escape leading elsewhere.“* Viď DELEUZE, Giles; GUATTARI,Félix. Anti-Oedipus: capitalism and schizophrenia. University of Minnesota. Humanities Press Inc. 2000. ISBN 0-8166-1225-0. Str.17.

v ruke informatika experta na simulačné hry.[52] Musíme pripustiť, že nejde len o obyčajné riadenie na diaľku. Totiž ak je v boji nasadených dronov viac, existuje tu možnosť prepínania kontroly medzi jednotlivými zariadeniami. Je to otázka rozhodnutia operátora podľa jemu dostupných aktuálnych informácií, resp. inteligencii algoritmu softvéru na strane ovládajúceho a na strane drona. Každé rozhodnutie operátora virtualizuje zamýšľaný bojový úkon, s ktorým ďalej pracuje softvér a ovládajúci hardvér. Paže operátora, jeho pohyby tela a manévre s bojovou technikou sú vďaka virtuálnej technológii prolongované do nepoznaného terénu. Zdá sa, že nový mód jestvovania je na svete. Hra sa odohráva vo virtualite a ovplyvňuje realitu, ktorá je na míle vzdialená operátorovi dronu. Napriek „deteritorializácii", virtualita je stále nejakým spôsobom naviazaná a prítomná vo vzťahu k fyzickému subjektu (vojakovi) a skôr či neskôr sa vždy aktualizuje (vojak vidí kontrolné panely, živú kameru, kontroluje svoj pohyb a pohyb dronu atď.).[53]

Súvislosť s Gýgovým príbehom je možné vidieť v tom, s akou nesmiernou ľahkosťou prináša metóda virtualizácie bojových prostriedkov riešenie ozbrojených konfliktov. Štát prostredníctvom armády zabúda na medzinárodné dohovory o vedení vojen[54] a zneužíva virtualizáciu na ním definované účely, ktoré by pomocou konvenčných zbraní nikdy nedosiahol. Ide o takmer úplnú Gýgovu neviditeľnosť so všetkými súvisiacimi následkami. Zdá sa, že *„technologická výhoda prsteňa sa stáva ospravedlnením jeho použitia,"* a že *„technológia dolieha na zmenu fundamentu práva."* Napriek tomu, že môžeme čeliť dileme, či popraviť nebezpečného teroristu bez akéhokoľvek súdneho procesu selektívnym útokom na diaľku alebo čeliť ďalšiemu teroristickému útoku do vlastných radov, takúto konfúziu je nevyhnutné striktne

[52] V polovici roka 2012 bola zverejnená náborová televízna reklama americkej armády zameraná na cieľovú skupinu hráčov počítačových hier. Viď US Army Commercial Targets Video Gamers. In: YouTube [online]. [cit.1.9.2020]. Dostupné z: http://www.youtube.com/watch?v=HU1y1G6uzAI

[53] Ibid LÉVY, Pierre. Str. 29.

[54] Ide o Ženevské a Haagské dohovory, ktoré tvoria základné právne piliere medzinárodného vojnového a humanitárneho práva. Medzi základné povinnosti patrí *„povinnosť útočníka rozlišovať medzi civilným obyvateľstvom a kombatantmi s cieľom ušetriť civilné obyvateľstvo a civilný majetok. Útok môže byť vedený iba proti vojenským cieľom. Ďalej to je nemožnosť neobmedzeného práva voliť spôsoby a prostriedky vedenia vojny príslušníkmi ozbrojených síl a stranami v konflikte."* Viď Právo ozbrojeného konfliktu a jeho uplatňovanie vo vojenských operáciách. In: Ozbrojené sily Slovenskej republiky: Konferenční príspevok [online]. [cit.1.9.2020]. Dostupné z: www.mil.sk/data/att/11772_subor.ppt

odmietnuť.[55] Obratom sa dostávame nepriamo k myšlienke Wittgensteina, ktorý sa nás snaží presvedčiť tiež o tom, že *„rozlišovanie medzi faktom a hodnotou znamená, že konštatovanie faktu si neslobodno mýliť s konštatovaním hodnoty.“*

Možné ponaučenie z Gýgovho podobenstva a vyššie uvedeného vojnového dobrodružstva je, že bez ohľadu na metódu riešenia spoločenských problémov, či už to bude virtualizácia právnych predpisov, judikatúry alebo procesu dokazovania,[56] resp. inej formy právnych nástrojov, dobré konanie zúčastnených je vždy výsledkom spoločenských vplyvov a determinované silou ich vlastných rozhodnutí a nikdy sa netýka zásadnej zmeny hodnôt (fundamentu v práve) z dôvodu novších alebo vyspelejších dioptrií, ktoré tu predstavujú informačný alebo technologický pokrok ľudstva.

Na druhej strane, metóda virtualizácie ponúka radu zaujímavých možností ako nastaviť niektoré procesy riešenia problémov. Pre Wittgensteina bola zmenou paradigmy v hľadaní logiky jazyka situácia, kedy si uvedomil, že modelové figúrky pri opise autonehody sa na stole v súdnej sieni usporadúvajú podľa skutočných vzťahov, ako sú sprostredkované jazykom. To znamená, že jazyk je modelom - obrazom skutočnosti.[57] Zdá sa, že v tomto príbehu išlo o virtualizáciu a následnú aktualizáciu minulých dejov prostredníctvom hovoreného jazyka. Totiž rozhodovanie o hľadaní príčin vo väzbách umiestnených modelov (figúrky, automobily atď.) predstavuje interpretáciu v podobe aktualizácie súčasného stavu. Práve tieto myšlienky pomohli postaviť Wittgensteinovi mohutný základ jeho analytickej filozofie.

Hoci nie je možné tvrdiť, že virtualita je zrkadlo reality alebo dokonca jej protikladom, istá analogická súvislosť tu nepochybne je. Ak hovoríme o virtuálnom

[55] Ibid. KAAG, John a Sarah KREPS.

[56] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 202.

[57] Hovorí sa, že túto myšlienku sformuloval behom prvej svetovej vojny, keď v novinách čítal o súdnom konaní v Paríži, ktoré sa týkalo dopravnej nehody a kde bola použitá kriminalistická technika zmenšených figurín a modelov. Viď BUCKINGHAM, Will. Kniha filozofie. Vyd. 1. Praha: Knižní klub, 2013. Universum (Knižní klub). ISBN 978-80-242-3912-5. Str. 249. Avšak fiktívná literatúra ponúka úsmevnejší pohľad a táto myšlienka sa mala zjaviť Wittgensteinovi pri jeho asistencii na hlavnom armádnom štábe monarchie počas prvej svetovej vojny, kde na modelovom bojisku podával zmenšený model ním vyrobeného kanónu príslušným nadriadeným podľa ich slovných pokynov. Ibid. DOXIADES. Logicomix. Str. 241.

jestvovaní, jeho znakom je skôr potenciálne ako aktuálne jestvovanie.[58] Každá evolúcia invenciou nových rýchlostí (napr. dopravných prostriedkov alebo internetovej konektivity) prináša nové a nepoznané problémy, avšak umožňuje aj nový pohľad a bezpochyby požadovanú úpravu niektorých partikularít. Čo je dôležité, nový pohľad a čiastkové úpravy však musia prevažovať nad nevýhodami opustených problémov.[59]

Pozitívnym príkladom môže byť dopad aspektov virtualizácie procesu autoritatívnej aplikácie práva v podobe systému riešenia on-line sporov (ODR). Vzhľadom na zvyšujúcu sa početnosť nehmotných elektronických dôkazných prostriedkov je povinnosťou každého praktikujúceho právnika brať na zreteľ kvalitu elektronických dôkazov (viď podkapitolu: 2.7 Elektronický súdny spis). Preto virtualizácia spisu a elektronických dôkazov predstavuje stabilnú konštrukciu ochrany týchto základných povinností a napomáha pri zachovaní elementárnej podstaty tohto inštitútu zvyšovať dynamiku prístupu k informáciám pre zúčastnených. Zaujímavým príkladom virtualizácie ako nástroja riešenia spoločenských problémov môže byť už spomenuté všeobecné zvyšovanie informovanosti spoločnosti, a to v podobe neukončených projektov eZbierka / eLegislatíva[60] alebo v podobe publikovania právnych vedomostí v laicky dostupných hypertextových a interaktívnych komentároch a článkoch. Za zmienku stojí aj samotný výkon právnickej profesie - advokácie prostredníctvom internetu. Aj keď niektorí autori dokonca rozmach takýchto technológií (označovaných ako *online legal guidance*) zaraďujú k príčinám budúceho zániku právnikov, je potrebné zdôrazniť, že výhody online advokácie v tuzemských pomeroch zatiaľ neprevažujú nad výhodami klasického prístupu kamenných advokátskych kancelárii.[61]V neposlednom rade je potrebné spomenúť virtualizovanie peňažnej sústavy *Bitcoin* alebo iných ekonomických prostriedkov v informačnej spoločnosti. Zdrojový kód projektu *Bitcoin* postavený na formáte *MIT* licencie a jeho technológia umožnili vznik ďalších zaujímavých projektov so zameraním na

[58] Lévy hovorí o príklade potencionálneho jestvovania, keď "strom je virtuálne prítomný v semiačku". Viď Ibid LÉVY, Pierre. Str. 23.

[59] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 258.

[60] Důvodová zpráva Návrhu zákona o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv [online]. [cit.1.9.2020]. Str.3. Dostupné z: https://apps.odok.cz/kpl-detail?pid=KORN999FKLW5. Ekonomický deník. [online]. [cit.1.9.2020]. https://ekonomickydenik.cz/esbirka-a-elegislativa-nejdrive-v-roce-2021

[61] SUSSKIND, Richard E. The end of lawyers?: rethinking the nature of legal services. New York: Oxford University Press, 2008. ISBN 978-0-19-954172-0. Str.121.

virtualizáciu niektorých častí spoločenských vzťahov. Za zmienku tu stojí virtualizovaný systém dokazovania časovej pečiatky a časovo uzavretého súboru.[62] Ide o úplne nový koncept, ktorý využíva skúsenosť zo šírenia a zdieľania *torrentov* a súvisiacich súborov, avšak kde sa zdieľaný (tzv. seedovaný) súbor nahradzuje obsahom časovej schránky. Totiž takýto obsah zdieľaný v sieti je v pravom slova zmysle všadeprítomný a jeho čiastočky sú roztrúsené medzi jednotlivými s*eedermi.* Systém je vybudovaný na Dumasovkom princípe jeden za všetkých, všetci za jedného. Otázne je, či táto technológia zatiaľ neprospieva viac skupinám využívajúcim anonymné a netransparentné prostredie ako skupinám hlásiacim sa k princípom a hodnotám usporiadanej spoločnosti.[63]

1.5. Zhrnutie kapitoly

V predloženej kapitole boli predstavené možnosti virtualizácie vo svetle súčasnej potreby riešenia spoločenských problémov prostredníctvom práva a právnej vedy. Ako bolo uvedené, virtualizácia je síce uchopiteľný koncept, ktorý posúva hranice chápania spoločenských problémov, automaticky sa však nedotýka základného fundamentu práva a nie vždy vytvára bezpečnejšie a účinnejšie riešenie. Ba naopak, často od vyriešeného problému posúva známy stav k rade nových problematických situácií.[64] Na druhej strane predstavuje proces plný invencie, ktorý ponúka nový pohľad na vec a jeho pochopenie dáva istotu o tom, že sa človek bude vedieť pohybovať aj na území, ktoré sa nečakane vynorilo na videnom horizonte v dôsledku jeho nekončiaceho blúdenia časom a priestorom. Ak je tento horizont zaujímavejší, dáva to motiváciu opustiť pôvodný problém a pristúpiť k riešeniu nových výziev, ktoré vykazujú vyššiu kvalitu a sľubujú efektívnejší rast.

Virtualizácia predstavuje nové rýchlosti a nové výzvy. Aj keď sa môže zdať, že virtualizácia si nárokuje na zásadne zmeny podstaty virtualizovaného predmetu, snahou tejto úvahy bolo vysvetliť, že virtualizácia je len koncept (technologický alebo systémový), ktorý sám o sebe negarantuje lepšie a hodnotnejšie spoločenské vzťahy.

[62] Twister: Peer-to-peer microblogging [online]. [cit. 1.9.2020]. Dostupné z: http://twister.net.co/

[63] Príkladom môže byť projekt Tor, anonymizér IP adries a poskytovateľ anonymných VPN pripojení, ktorý je podľa kriminalistických štúdii veľmi obľúbený u rôznych delikventov. Viď Tor: Anonymity Online. [online]. [cit. 1.9.2020]. Dostupné z: https://www.torproject.org/index.html.en

[64] Ibid. POLČÁK, Radim. Právo a evropská informační společnost. 1. Str.118.

Je zrejmé, že neuvážená virtualizácia každej sféry spoločenského života (vrátane elektronického dokazovania) za pomoci informačných a telekomunikačných technológii spôsobuje vo finále z pohľadu právnej kybernetiky zbytočnú preinformovanosť. Preto je počuť hlasy volajúce po tichu, ktoré sú vo svojom jadre veľmi hlboké a pravdivé.[65] Vystihujú podstatu problému. Slovami Shakespeara *„blíži sa doba, myslím, kedy najlepším prejavom múdrosti bude ticho. Džavotanie bude tak akurát len pre papagájov.“*[66] Avšak fakt samotnej preinformovanosti by v nás nemal zanechať pachuť po technológiách a spôsobiť neschopnosť rozlišovať *Text* od balastu alebo dezinformácie. Preto virtualizácia predstavuje dobré okuliare, ale tie ešte nedávajú záruku plného pochopenia samotného *Textu.* Exupérovsky je možné na záver dodať už len to, že *„dobré vidíme aj tak iba srdcom. To hlavné je očiam neviditeľné.“*[67]

[65] Ibid. POLČÁK, Radim. Internet a proměny práva. Str.378. alebo Viď POLČÁK, Radim. Pět tichých minut za Viktorem Knappem. Právník, Praha: AV ČR, Ústav státu a práva, 2013, roč. 152, č. 12, Str. 1231-1244. ISSN 0231-6625.

[66] Replika Lorenza, ktorí v hre Kupec benátsky hovorí k Lancelotovi. Viď HILSKÝ, Martin. SHAKESPEARE, William. Slovník citátů z Díla Williama Shakespeara. Vyd. 1. Praha: Academia. ISBN 978-80-200-2193-9. Str. 356.

[67] SAINT-EXUPÉRY, Antoine. Malý princ. Gardenia Publishers, Bratislava, 2000. Str. 70.

2. Fundamenty elektronického dôkazného prostriedku*

2.1. Úvodné poznámky

V predloženej kapitole sa zameriavame na virtualizované dôkazné prostriedky, t.j. elektronické dôkazné prostriedky a ich podstatu. Naším primárnym záujmom je inštrumentárium a proces okolo dokazovania v občianskom sporovom konaní. V tomto konaní je dokazovanie ako postup súdu a účastníkov konania upravený právnymi normami a procesnými zvyklosťami, ktorých účelom je zadováženie poznatkov pre meritórne alebo iné rozhodnutie súdu alebo orgánu. Je vecou strán, aby svoje tvrdenia opreli o vierohodné dôkazy.[68]

V českom civilnom konaní sú to vždy strany sporu, ktoré navrhujú vykonanie dôkazov, a to až na výnimky.[69] Slovenský civilný súd môže z úradnej moci (*ex officio)* vykonať len taký dôkaz, ktorý vyplýva z verejných registrov a zoznamov, ak tieto registre alebo zoznamy nasvedčujú, že skutkové tvrdenia strán sú v rozpore so skutočnosťou. Napríklad švajčiarsky civilný súd vykonáva dôkazy *ex officio* vždy, keď musí zistiť skutočnosti e*x officio* a ak existujú vážne pochybnosti o pravdivosti nespornej skutočnosti.[70]

V trestnom konaní právo obstarávať dôkazy majú aj procesné strany, avšak postavenie procesných strán v civilnom konaní je značne silnejšie.[71] Z procesného

---

* Táto kapitola vychádza z publikovaného článku ABELOVSKÝ, Tomáš. Elektronický dôkazný prostriedok vo svetle práva duševného vlastníctva. 1. vydání. Brno: Spisy Právnické Fakulty MU, 2014. 1033 s. ISBN 978-80-210-7211-4. Str. 185-205.

[68] V trestnom konaní na rozdiel od civilného konania vyvíjajú súdy a OČTK samostatnú iniciatívu k zadováženiu dôkazných prostriedkov (zásada vyhľadávacia, zásada riadneho zistenia skutkového stavu bez dôvodných pochybností).

[69] V civilnom konaní môže český súd zaistiť alebo vykonať aj iné ako navrhnuté dôkazy. Napríklad za účelom overenia skutočnosti, ktorú žiadna zo strán netvrdí. Súd tak môže brať do úvahy len dôkazy do okamihu koncentrácie konania alebo tie dôkazy, u ktorých sa uplatní výnimka z koncentrácie. K režimu koncentrácie sa vyjadril NS ČR tak, že *„i v režimu zákonné koncentrace řízení podle § 118b odst. 10 o. s. ř. není soud zbaven povinnosti provésti jiné než účastníky navržené důkazy, jestliže potřeba jejich provedení vyšla v řízení najevo (§ 120 odst. 3 o. s. ř.). Zákonná koncentrace řízení omezuje soud v rozsahu těchto aktivit potud, že může brát v úvahu jen takové důkazy, jejichž potřeba provedení vyšla najevo do skončení prvního jednání, které se ve věci konalo.“* Rozsudek NS ČR ze dne 27. 3. 2008, sp. zn. 29 Odo 1538/2006 (Rc 28/2009 civ.).

[70] Porovnaj § 120 ods. 2 OSŘ, § 185 ods. 2 CSP a čl. 153 ZPO alebo Viď HROMADA, Miroslav. § 120 [Důkazní povinnost]. In: SVOBODA, Karel, SMOLÍK, Petr, LEVÝ, Jiří, ŠÍNOVÁ, Renáta. Občanský soudní řád. 2. vydání. Praha: Nakladatelství C. H. Beck, 2017, Str. 526.

[71] Viď § 2 ods. 5 TŘ a § 2 ods. 10 TP.

hľadiska prostredníctvom dokazovania súd alebo vyšetrovací orgán získava hmotnoprávne, ale aj procesnoprávne poznatky. Ide o skutočnosti, ktoré sú dôležité aj pre iné než meritórne rozhodnutie.[72] Súdy alebo iné orgány postupujú tak, aby bol zistený skutkový stav veci v určitej kvalite v rozsahu nevyhnutnom na rozhodnutie veci samej (napr. neexistuje dôvodná pochybnosť).

Na rozdiel od anglo-americkej právnej tradície,[73] proces dokazovania pomocou elektronického dôkazného prostriedku vo vyššie uvedených civilných súdnych poriadkoch nemá ucelenú osobitnú úpravu (výnimkou sú ustanovenia o vedení elektronického spisu alebo nakladanie s elektronickými podaniami). Môžeme sa pýtať, do akej miery ovplyvňujú pravidla súdneho konania podstatu elektronického dôkazného prostriedku, ak zákonodarca nepočítal s takou samostatnou úpravou? Ako ďalej vysvetlíme, sme toho názoru, že súčasná procesná úprava dokazovania v SR a ČR je dostatočne použiteľná aj pre elektronický dôkazný prostriedok. Ide o to, aby bola použitá s prihliadnutím na podstatu elektronického dôkazného prostriedku, pochopeniu jeho limitov a rizík, jeho informačného obsahu a kategórie kvality.

2.2. Podstata elektronického dôkazu

Aby sme mohli prikročiť k definícii elektronického dôkazného prostriedku, je nutné ozrejmiť rozdiel medzi *dôkazným prostriedkom* a *dôkazom*. Za dôkazný prostriedok považujeme procesný nástroj, postup, pomôcku, nosič alebo inštrument, z ktorého môžeme získať, resp. vyťažiť dôkaz. Ide o sprostredkovateľa alebo nosič informácie. Inak povedané, za dôkazný prostriedok môžeme považovať všetko čím sa dá zistiť stav veci o dokazovanej skutočnosti.[74] Typickým dôkazným prostriedkom je svedecká výpoveď. Procesný úkon v podobe vypočúvania svedka je dôkazný prostriedok, pričom dôkazom je získaná informácia, respektíve obsah výsluchu svedka. Akými prostriedkami má byť navrhnutý dôkaz vykonaný je základná procesná otázka na odlíšenie dôkazu a dôkazného prostriedku.[75] Tieto pojmy sa často v odbornej

[72] SVOBODA, Karel, Dokazovaní, Praha: ASPI – Wolters Kluwer, 2009, Str. 12.

[73] Viď napr. pre USA procesnú úpravu FRCP

[74] Tuzemské procesné poriadky nerozlišujú dôsledne medzi týmito pojmami.

[75] Viď rozhodnutie ÚS ČR, podľa ktorého *„orgány činné v trestním řízení jsou povinny vždy pečlivě posuzovat, zdali důkazní prostředek, z něhož plyne usvědčující důkaz, byl opatřen způsobem, jenž nezpochybňuje spolehlivost v něm obsažené informace, a v případě pochybností o spolehlivosti takto opatřeného důkazu byl následně objektivním způsobem prověřen.“* Nález ÚS ČR ze dne 15. 2. 2016, sp. zn. I. ÚS 368/15.

literatúre zamieňajú a používajú ako synonymá.[76] Doktrína ešte rozoznáva *prameň dôkazu*, za čo považuje samostatný nosič informácie.[77] Môže ísť o napríklad o osoby a veci.[78] Pri elektronickom dôkaznom prostriedku to bude napríklad email a získaným dôkazom jeho obsah po vykonaní dokazovania emailom. Prameňom dôkazu v tomto prípade bude najčastejšie zaistený emailový server, pevný disk, dáta v podobe súboru emailového klienta (napr. súbor vo formáte *Personal Storage Table* pre *Microsoft Exchange a Outlook*), resp. iný dátový nosič schopný uchovávať dokazovanú skutočnosť v elektronickej podobe.

Vo všeobecnosti teória dokazovania rozoznáva dôkazné prostriedky *priame* a *nepriame.* Priame sa vyznačujú tým, že prinášajú priame a bezprostredné oboznámenie sa so skutočnosťou. Typicky medzi priame dôkazné prostriedky patria prehliadka osôb, veci alebo miesta. Medzi priame elektronické dôkazne prostriedky môže patriť prehliadka hardwaru, ktorého fyzický stav je priamym výsledkom dokazovanej skutočnosti. Nepriame dôkazné prostriedky podávajú informácie len sprostredkovane (napr. listina alebo dátový zápis o určitej skutočnosti ako indícia).[79] K podobnému deleniu dochádza aj u dôkazných prostriedkov, kde priamym dôkazným prostriedkom bude konkrétna informácia na profile webovej sociálnej siete a nepriamym dôkazným prostriedkom bude potvrdené alibi v podobe číselného kódu zariadenia u mobilného operátora zaznamenaného v danom čase a mieste, ktoré sa zhoduje so skúmaným zariadením. Presvedčivosť nepriamych dôkazov (indícií) vyvoláva rôzne sporné otázky

[76] Podľa Mařádeka „hovořím-li o důkazním prostředku, nemyslím jím procesní činnost, kterou soud získává informace o *skutkovém stavu (výslech svědka, ohledání věci), nýbrž pramen informace o skutkovém stavu (který někteří autoři nazývají pramenem důkazu – např. listina).“* Viď MAŘÁDEK, David. Soukromě pořízený zvukový a zvukově obrazový záznam jako důkazní prostředek a důkaz v civilním soudním řízení. Právní rozhledy. 2015, č. 20, Str. 705-710.

[77] Obhajoba v trestnom konaní je oprávnená predovšetkým dôkazy vyhľadať, tzn. pátrať po prameňoch dôkazov a ich nositeľa identifikovať tak, aby bolo možné dôkaznú hodnotu vyhľadaných dôkazov využiť v procese dokazovania. VANTUCH, Pavel. Kdy může obhajoba důkaz vyhledat, kdy předložit a kdy jen navrhnout jeho provedení? Bulletin advokacie. 2013, č. 7-8, Str. 27-32

[78] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. 2015. Str. 57.

[79] Napríklad dôkaz vykonaný metódou pachovej identifikácie je nepriamym dôkazným prostriedkom, ktorý ako jediný spravidla k uznaniu viny v trestnom práve postačovať nebude a je potrebná ucelená reťaz nepriamych dôkazov. Ako uvádza Havelková a Jirásko *„abychom tedy mohli v konkrétním případě mluvit o tzv. uceleném řetězci nepřímých důkazů, musí v dané věci existovat ucelená, logická a ničím nenarušená uzavřená soustava vzájemně se doplňujících a na sebe navazujících nepřímých důkazů, přičemž tyto musí ve svém celku shodně a spolehlivě prokázat určitou skutečnost (v trestním řízení zpravidla to, že se stal konkrétní skutek naplňující znaky trestného činu a že jej spáchal zcela jednoznačně obžalovaný) a musí jasně vyloučit možnost jiných závěrů.“* Viď HAVELKOVÁ, Renata, JIRÁSKO, Vojtěch. Využití metody pachové identifikace v trestním řízení. Trestněprávní revue. 2019, č. 9, Str. 192-195.

v aplikačnej praxi.[80] Je preto potrebné zhrnúť, že elektronický dôkazný prostriedok a elektronický dôkaz môžu mať povahu priameho, ale aj nepriameho dôkazného prostriedku, respektíve dôkazu, čo vždy závisí od kontextu skúmanej situácie a jeho správneho posúdenia.

Ak pristúpime ku charakteristike elektronického dôkazného prostriedku, je zvyčajne v odbornej literatúre uvádzaný v dvoch podobách:[81]

(i) „záznam skutočností ako úplný obraz minulých dejov (napr. počítačový model, digitálna fotografia, audiovizuálna nahrávka);

(ii) elektronické dáta (napr. dátový nosič, záznam telekomunikačnej prevádzky, odpočúvanie elektronickej komunikácie).“

Medzi týmito dvoma skupinami sa ťažko hľadá jasná hranica, nakoľko často splývajú a ich rozdelenie je len otázkou pohľadu na inštrumentárium nakladania s elektronickým dôkazným prostriedkom v jednotlivom prípade.

Jasnejšiu definíciu je možno nájsť v zahraničnej literatúre u Masona, ktorý za elektronický dôkazný prostriedok (*electronic evidence, digital evidence*) považuje všetky *„dáta (zahrňujúce výstup analógových alebo digitálnych zariadení alebo dáta v digitálnom formáte), ktoré sú vytvorené, manipulované, ukladané alebo komunikovaná akýmkoľvek zariadením, počítačom alebo počítačovým systémom alebo prenášané cez komunikačný systém, ktoré sú relevantné pre proces rozhodovania.“*[82] Podobnú definíciu je možné nájsť aj u Caseya. Avšak tá je prísne viazaná na elektronický dôkazný prostriedok len v súvislosti s počítačom alebo počítačovým systémom.[83]

[80] Česká súdna prax o nepriamom dôkaze konštatovala, že poukázanie sťažovateľa na miesto výskytu SIM karty poškodeného v čase jeho vraždy nie je presvedčivý dôkaz, pretože len vypovedá o tom, ktorá bunka mobilného operátora zachytila výskyt SIM karty poškodeného, nie to, že priamo na tomto mieste sa poškodený pohyboval. Viď Usnesení ÚS ČR ze dne 12. 9. 2017, sp. zn. III. ÚS 2977/16.

[81] KYNCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. In: Revue pro právo a technologie. Brno: Masarykova univerzita, č.3, 2011. ISSN 1805-2797. Str. 5.

[82] MASON, Stephen. Electronic evidence. 2nd ed. London: LexisNexis, 2010. ISBN 978-140-5749-121. Str. 24.

[83] CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the Internet. 3rd ed. Amsterdam: Elsevier, 2011. ISBN 978-0-12-374268-1. Str.7.

Na základe vyššie uvedeného považujeme elektronický dôkazný prostriedok pre účely civilného konania za taký dôkazný prostriedok, ktorého interpretácia je vždy závislá od využitia elektronických a digitálnych technológií, a ktorými možno v procese dokazovania zistiť stav veci.

V odbornej literatúre sa je možné stretnúť s názorom, že neexistuje žiaden dôvod na rozlišovanie špeciálnych typov dôkazných prostriedkov, nakoľko vo všeobecnosti k vykonaniu dôkazu možno použiť akékoľvek dôkazné prostriedky (ak sú k tomu vhodné), a to za predpokladu, že neboli získané alebo vykonané v rozpore s platnými právnymi predpismi.[84] Avšak domnievame sa, že aspoň v priebehu interpretácie (hodnotenia) je potrebné diferencovať elektronický dôkazný prostriedok z dôvodu jeho špecifických technických vlastností, ktoré môžu spôsobovať praktické problémy s jeho obstaraním, vykonaním a hodnotením. Takáto diferenciácia pomôže lepšie elektronický dôkazný prostriedok popísať, zaradiť ho do kontextu a logicky vyhodnotiť.

Odborná prax rozlišuje najčastejšie nasledujúce typy elektronického dôkazného prostriedku (demonštratívny výpočet):

- Dáta alebo dátový záznam vrátane elektronických dokumentov a podpisov;
- Dáta z mobilných komunikačných zariadení;
- Dáta z cloudu alebo serverových úložísk;
- Dáta z dohľadových systémov kybernetickej bezpečnosti;
- E-mail, instantné správy alebo iný elektronický komunikačný formát pre textové alebo audiovizuálne správy (messenger);
- Osobný profil a webová prezentácia (webstránka);
- IP adresa alebo identifikátor sieťového rozhrania;
- Prevádzkové a lokalizačné údaje;
- Odpočúvanie, audio-vizuálne nahrávanie, informačno-technické prostriedky v trestnom konaní.

[84] MORÁVEK, Jakub. Kdy lze jako důkazní prostředek připustit záznam z kamerového systému. Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 2011. č. 13. ISSN 1210-6410.

2.3. Limity elektronického dokazovania

Dokazovanie ako jedna z najdôležitejších súčastí procesného práva, pri ktorej sa dokazuje (verifikuje) určité tvrdenie, často predstavuje myšlienkový proces zrekonštruovania minulých dejov alebo verifikácie určitých skutočností, či už minulých alebo súčasných. Niekedy sa zdá, že nový fenomén elektronického dôkazného prostriedku posúva paradigma vnímania procesu dokazovania do úplne novej roviny. Pri každom dokazovaní po získaní požadovanej informácie pristupuje logická operácia súdu podradenia skutkovej (dejovej) podstaty pod zodpovedajúcu právnu normu. Podľa Knappa môžeme hovoriť, že súčasťou aplikácie práva je práve táto operácia, t.j. *„ako priliehavo bude zvolená právna norma.“* [85] Táto musí zodpovedať tomu, čo sa udialo a čo bolo preukázané, teda existujúcej skutkovej podstate. Ideálnym výsledkom by mala byť vždy správna aplikácia práva a následne spravodlivé rozhodnutie súdu. Poznanie v podobe zistenia materiálnej pravdy, ktoré dosahuje súd v rámci súdneho konania, nie je a ani nemôže byť absolútnym poznaním. Má pravdepodobnostný charakter kvalitatívnej úrovne, ktorá je totožná s praktickou istotou.[86] Hovoríme o miere dôkazu. Dosiahnutie praktickej istoty je napríklad v súčasnosti negatívnym spôsobom vyjadrené ako zásada zistenia skutkového stavu bez dôvodných pochybností priamo v trestnom poriadku ČR alebo SR. Súdy sa snažia zistiť skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie.[87] Holländer v nadväznosti na Weinbergera, chápe pojem praktickej istoty ako psychologicko-praktickú hranicu poznania. [88]

S nadnesením je možné uviesť, že elektronický dôkazný prostriedok pripomína rozohranú šachovú partiu, kde súd v postavení Sherlocka Holmesa musí pomocou retrográdnej analýzy zodpovedať množstvo otázok ohľadom predošlých ťahov a odhaliť tak „páchateľa šachového zločinu.“ [89] Prirovnanie demonštruje, že častým

[85] KNAPP, Viktor. Teorie práva. Praha: C.H.Beck, 1995. ISBN 80-7179-028-1. Str. 187.

[86] MACUR, J. Dokazovaní a procesní odpovědnost v občanském soudním řízení. Spisy Právnické fakulty University J.E.Purkyně v Brně; svazek 56, Brno. 1984, Str. 69.

[87] Ustanovenie o základných zásadách trestného konania v § 2 ods. 5 TŘ alebo § 2 ods. 10 TP.

[88] HOLLÄNDER, Pavel. Filosofie práva. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, Str. 201.

[89] Pre bližšie zoznámenie sa s retrográdnou analýzou, ktorá zohrala dôležitú rolu v príbehu a živote beletrickej postavy Sherlocka Holmesa. Viď SMULLYAN, Raymond. Šachové záhady Sherlocka Holmese, aneb, Padesát úloh šachové dedukce, které vám nedají spát. 1. vyd. Praha: Mladá fronta, 2005. ISBN 80-204-1233-6.

limitom je nepochopenie pravidiel šachu a nedostatočné logické uvažovanie, čo vidíme aj pri elektronickom dokazovaní. Medzi súčasne limity využívania elektronického dôkazného prostriedku práve tak, ako ho poznáme v tuzemskej a zahraničnej odbornej literatúre, patrí v prvom rade nepochopenie samotnej podstaty tohto inštitútu a použitej technológie. Elektronický dôkazný prostriedok a vyťažený dôkaz by nemal len vyrozprávať príbeh o dokazovanej skutočnosti, ale mal by byť aj ľahko pochopiteľný a čitateľný laickej verejnosti.[90] S touto prekážkou úzko súvisí absencia teoretickej definície elektronického dôkazného prostriedku. Pri bližšom skúmaní sa zdajú byť problematické najmä otázky samostatnej procesnej úpravy a otázky metodologických usmernení ako správne elektronický dôkazný prostriedok identifikovať, vyťažiť (*soft-law*), ale aj ako ho vykonať (súdny poriadok). Navyše v neposlednom rade elektronický dôkazný prostriedok svojimi nárokmi na technické vlastnosti predmetov dokazovania spôsobuje roztrieštenosť a náhodilosť vo výbere postupov ohľadom nakladania s takýmito dôkazmi. Žiadna teória dôkazu by nemala zabudnúť na osobné presvedčenie sudcu, ktoré je zo svojej povahy vždy subjektívne.[91] Preto môžeme zhrnúť, že pre dokazovanie elektronickým dôkazným prostriedkom bude priliehavosť voľby právnej normy súdom okrem iného závislá aj na tom, ako bude pochopená technológia týchto prostriedkov (subjektívna stránka) a ako dobre bude tento postup v objektívnej podobe kontrolovateľný alebo verifikovateľný (objektívna stránka). Táto priliehavosť môže byť ovplyvnená technológiou, resp. vedeckým spracovaním dôkazov a aplikáciou zásady voľného hodnotenia dôkazov.

2.4. Informačná teória elektronického dôkazného prostriedku

Ako už bolo uvedené vyššie, informácia je stavebným kameňom právneho systému.[92] Podľa Knappa kybernetické metódy v práve sú o inovatívnom chápaní práva, t.j. ako informačného systému.[93] V prípade procesu dokazovania, či už civilnom alebo v trestnom práve, na strane vykonávateľa dôkazného prostriedku prevláda

[90] Ibid. MASON, Stephen. Str. 167.

[91] GAZDA, Viktor. Míra důkazu a úloha pravděpodobnosti v důkazním právu. Právní rozhledy. 2019, č. 3, Str. 77-78.

[92] POLČÁK, Radim. PÚRY, František, HARAŠTA, JAKUB a kolektiv. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015, Spisy Právnické fakulty MU č. 542 (řada teoretická, Edice Scientia). ISBN 978-80-210-8073-7MUNI/A/1296/201. Str. 16.

[93] Podľa Polčáka *„ide o jeho analýzu a spracovanie ako dokonalého objektu kybernetického skúmania.“* Viď POLČÁK, Radim. Pět tichých minut za Viktorem Knappem. Právník. 12/2013. ÚSP AV ČR. Ročník: 152 Str. 1231-1244.

informačný deficit. Ten je daný nedostatkom priameho, resp. bezprostredného poznania skutočnosti, ktorá sa dokazuje. Ak právny poriadok pracuje s informáciou ako predmetom dokazovania, nepostihuje jej ideálnu existenciu, ale stanoví jej vonkajšiu formu a potom jej priradzuje príslušné následky. Podľa Šámala ide o nutnú formalizáciu informácie.[94] Domnievame sa, že práve táto formalizácia kompenzuje informačný deficit medzi skutočným stavom a dokázaným stavom.

Základný princíp kybernetiky, podľa ktorého miera informovanosti systému zodpovedá jeho usporiadanosti, je možné objaviť aj v procese dokazovania. Informačný efekt v podobe približovania sa k informačnej symetrii je závislý na kvalite elektronického dôkazného prostriedku a na tom, ako táto kvalita dokáže presvedčiť vykonávateľa dôkazu, resp. súd. Slovami Weinbergera *„v pragmatickom pohľade nejde len o to, aby argumenty [boli] objektívne platné, ale hlavne o to, aby účastníci rozhovoru nadobudli presvedčenie o váhe argumentov.“* [95] Podľa Škopa ide o pragmatické poňatie procesu dokazovania. Logická a empirická pravda môže byť nahradená argumentačnou rovinou, ktorá sa spája s presvedčením a nie pravdou.[96] Inak povedané, informačný efekt u elektronického dôkazného prostriedku bude umocnený interpretáciou jeho kvality. Ide o vyjadrenie hodnoverného príbehu o minulej skutočnosti a technológií pomocou ľahko pochopiteľného jazyka.[97] Informačnú hodnotu elektronického dôkazného prostriedku je možné prirovnať k vitamínom. Informácie získané z elektronického dôkazného prostriedku nie sú vždy v dokazovaní potrebné. Často predstavujú doplnkové a nepriame dôkazy, ale v samotnom závere rozhodovania môžu chýbať. Ale ak sú osamote a bez kontextu, nepomáhajú znížiť informačný deficit. Napriek tomu, vďaka informačnej hodnote, ktorá môže byť objektívne merateľná (napr. v oblasti dátovej analýzy *Big data* pomocou matematických a štatistických postupov), elektronický dôkazný prostriedok môže

[94] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. 2015. Str. 17.

[95] WEINBERGER, Otto. Základy právní logiky. Brno: MU, 1993. ISBN 80-210-0827-X. Str.221.

[96] Ibid. ŠKOP, Martin. Základní metodologie dokazovaní v právu. In: Dokazovanie v civilnom a trestnom konaní. Str. 20.

[97] Podľa Škopa je právnik podobný Don Quijotovi, nakoľko svet praxe, správania a teórie sú oddelené. *„I v jeho případě je nutné mezi nimi udržet zdání vztahu. Aby se slova příliš nevzdálila věcem, aby se interpretace norem příliš nevzdálily praxi. Nebo aby si naopak praxe za každou cenu přizpůsobovala slova.“* ŠKOP, Martin, 2013. --právo, jazyk a příběh. Praha: Auditorium. ISBN 978-80-87284-37-7. Str. 39.

zohrať rolu viac presvedčivejšieho prostriedku než je klasický dôkazný prostriedok v procese dokazovania. Príkladom môže byť porovnanie vlastnoručného podpisu s elektronickým zaručeným podpisom. Pri vlastnoručnom podpise musí súd vychádzať zo záverov znaleckého dokazovania, ktoré je založené na expertnom skúmaní materiálov, fyzikálnych vlastností papiera a atramentu, vlastností písma a jeho charakteristík. Čo do rozsahu ide vždy o expertné skúmanie založené na pravdepodobnosti. Pri skúmaní autenticity elektronického dôkazného prostriedku akým môže byť elektronický dokument podpísaný zaručeným elektronickým podpisom, stačí prepočítať jeho číselné hodnoty v počítačovom programe na základe vopred definovaných hodnôt (napr. overenie kľúča alebo podpisového certifikátu podpisujúcej osoby). Preto informačná hodnota elektronického dôkazného prostriedku môže byť pomerne vysoká, ale je závislá na jeho kvalite. V nasledujúcej podkapitole si vysvetlíme jednotlivé príklady kvalít elektronického dôkazného prostriedku.

2.5. Kategória kvality elektronického dôkazného prostriedku

2.5.1. Potencionálna ubiquita a volatilita

Tak ako predmety práva duševného vlastníctva, tak aj elektronické dôkazné prostriedky sú charakteristické materiálnou vlastnosťou, ktorá sa popisuje ako *potencionálna ubiquita*.[98] Ide o pojmový znak predmetu, ktorý je v nehmotnej podobe a ktorý sa vyznačuje schopnosťou byť všadeprítomný. Môže byť kedykoľvek a kdekoľvek vnímaný.[99] Teoreticky ho môže užívať neobmedzený počet ľudí. Čo je zásadné, toto užívanie neovplyvňuje jeho podstatu a funkciu. Ostáva tak nedotknutý a nemenný.[100]Za určitých okolností predmety dokazovania vo virtualizovanej podobe

[98] Podľa Krištúfeka *„dostávame sa tak k jednému z kľúčových znakov ideálnych objektov - potenciálnej ubiquity (možná všadeprítomnosť), ktorá znamená, že ideálne objekty môže používať ktokoľvek, kdekoľvek a kedykoľvek a pritom sa nezhoršuje ich podstata ani funkcie.“* Viď KRIŠTÚFEK, M. Základy práva duševného vlastníctva – autorské právo, jemu príbuzné právo a s ním súvisiace práva. In. Ochrana duševného vlastníctva. Zborník. Bratislava: Vydavateľské oddelenie Právnickej fakulty Univerzity Komenského, 2001, Str. 11.

[99] KYSELOVSKÁ, Tereza. Procesní a kolizní problematika práv k duševnímu vlastnictví se zaměřením na judikaturu Soudního dvora EU. Revue pro právo a technologie. 2013, č. 8, Str. 19-27.

[100] Podľa Telca nehmotný statok je *„povahovo nadaný potencionálnou ubikvitou, tzn. potencionálnou časovou a územnou všadepritomnosťou, bez toho aby sa spotreboval alebo akokoľvek opotreboval. V tom spočíva hospodárska výhoda všetkých nehmotných statkov a poťažmo aj práv k nim, označovaných, podľa svojich predmetov, tiež ako práva nehmotné.“* Viď TELEC, Ivo. Šíření děl a výkonů v telekomunikačních sítích, zvláště v Internetu, In: Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 1997. č.4. ISSN 1210-6410.

(napr. existencia pesničky v digitálnom formáte MP3) pomocou elektronického dôkazného prostriedku (napr. dátový nosič, obsah *cloudu* alebo iného úložiska) majú vlastnosť potencionálnej ubiquity. Táto vlastnosť sa vzťahuje na obsah zaisteného elektronického dôkazného prostriedku (napr. dáta). Ten je dôležitý pre svoj informačný potenciál. Potencionálna ubiquita značí, že zadovážením alebo použitím dôkazu by sa nemal dôkazný prostriedok automaticky spotrebovať, resp. úplne fyzicky zničiť (napr. stiahnutie fotografie neovplyvní pôvodný publikovaný súbor fotografie na webe).

Avšak v prípade elektronického dôkazného prostriedku je potrebné brať do úvahy aj jeho druhú materiálnu vlastnosť, t.j. *volatilitu*. Volatilita alebo volatilnosť (z angl. *volatility*) je v ekonomických vedách pojem užívaný pre kolísavosť, nestálosť, prchavosť, resp. premenlivosť hodnôt (najmä cien). Táto vlastnosť však výstižne popisuje základnú črtu elektronických dát. Totiž elektronické alebo digitálne dáta sa môžu automaticky modifikovať alebo zmeniť. Takáto zmena je spôsobená častou povahou alebo okolnosťami, za ktorých bolo s nimi nakladané. Inak povedané, už len samotným kopírovaním záznamu dát sa môže kontaminovať alebo pozmeniť ich obsah.

Kľúčom k elektronickému dokazovaniu je práve pochopenie týchto dvoch vlastností, t.j. potencionálnej ubiquity a volatility elektronického dôkazného prostriedku v počiatočnej fáze procesu elektronického dokazovania. Aj keď ide o pomerne náročné technické vedomosti o spôsobe zberu, nakladania a uchovávania dát výpočtovej techniky, už samotná vedomosť o možnej potencionálnej ubiquite a rovnako aj volatilite napovie o správnej voľbe technických postupov na vyťaženie a uchovávanie dôkazu. V prípade elektronického dokazovania je potrebné nenechať sa zmiasť ich automatickou schopnosťou byť všadeprítomný (potencionálnou ubiqitou), ale dôsledne strážiť ich volatililtu. Ako jednoduchý príklad je možné uviesť metódu použitia vytlačeného *printscreenu* (grafického otlačku) obsahu webovej stránky. Takýto dôkazný prostriedok, ktorý má sprostredkovať informáciu o obsahu webu (napr. záznam v prípade sporu o doménové meno alebo obsah diskusného fóra) má veľmi malú výpovednú hodnotu a navyše samotná tlač (konverzia) na papier často deformuje popisovanú skutočnosť (napr. metadáta, chýbajúca hlavička, päta a obrázky,

neukončená URL adresa).[101] Tieto technické problémy je možné odbúrať využitím vhodných technologických nástrojov, ktoré vytvoria elektronický záznam požadovaných webových stránok so všetkými dostupnými súvisiacimi informáciami (napr. s metadátami v podobe WHOIS výpisu) s využitím bezpečného šifrovania a podpisových politík (napr. elektronický podpis, časová pečiatka). Takýto záznam v elektronickej podobe môže predstavovať hodnotnejší elektronický dôkaz o existencii obsahu webovej stránky v konkrétnom čase a v ideálnom prípade by mal byť autorizovaným spôsobom vložený do elektronického úložiska (*e-spis*) v predmetnom civilnom spore na príslušnom súde, a to tak, aby každá zo súdnych strán mala k nemu plný a zabezpečený prístup vo forme elektronického nazerania do súdneho spisu, čím sa zabráni jeho volatilite (viď podkapitolu: 2.7. Elektronicky súdny spis).

2.5.2. Dôkazná spoľahlivosť a integrita

Kategória spoľahlivosti elektronického dôkazného prostriedku je vzájomne závislá na formálnych vlastnostiach dôkazného prostriedku (napr. kvalitatívnych znakoch dôkazu, akými sú spôsob získania a uchovávania elektronického nosiča), na objektívnej možnosti kontroly vzniku, zmeny a zániku tejto informácie a tiež na nestrannom vykonaní tohto dôkazu. Ide najmä o jeho prevedenie do formy, ktorá je vnímateľná zmyslami človeka a bezprostredným vykonaním takéhoto dôkazu, ak to jeho podstata umožňuje. Resp. jeho fyzickou ohliadkou alebo delegovaním tejto činnosti na oprávnený subjekt (napr. súdny znalec, expert), ktorý môže zodpovedať odbornú otázku bez rozhodnutia o aplikácii práva. Dôkazná spoľahlivosť bola definovaná a potvrdená ÚS ČR v trestnom práve procesnom. OČTK sú totiž vždy povinné vždy starostlivo posudzovať, či dôkazný prostriedok, z ktorého plynie usvedčujúco dôkaz, bol získaný spôsobom, ktorý nespochybňuje spoľahlivosť v ňom obsiahnutej informácie, a v prípade pochybností o spoľahlivosti takto získaného dôkazu bol následne objektívnym spôsobom preverený.[102] Pre posúdenie spoľahlivosti elektronického dôkazného prostriedku je nevyhnutné zachovať kvalitu dôkaznej spoľahlivosti tak, aby bola zabezpečená najmä jeho integrita. Elektronický dôkazný prostriedok by mal byť zabezpečený a prechovávaný takým spôsobom, o ktorom nie

[101] Prax prináša takýto *printscreen* často ako prílohu notárskej zápisnice o osvedčovaní právne významných skutočností, t.j. o tom ako notár otvoril webstránku a prezeral si jej obsah v zmysle § 56 ods.1 písm. i) zákona č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok).

[102] Nález ÚS ČR ze dne 15. 2. 2016, sp. zn. I. ÚS 368/15.

sú pochybnosti o tom, že by mohol byť akokoľvek, úmyselne, z nedbanlivosti alebo obyčajnou náhodou upravený, pozmenený alebo zamenený za iný. Navyše ak sa pri vykonávaní a hodnotení dôkazov vyskytnú vážne pochybnosti o spoľahlivosti použitých dôkazov, je povinnosťou súdu sa s nimi spoľahlivo a presvedčivo vysporiadať v odôvodnení rozsudku. Aby bola dôkazná spoľahlivosť a integrita objektivizovateľná, majú súdy povinnosť vyčerpávajúcim spôsobom popísať dôkazný postup a presvedčivo odôvodniť svoje skutkové závery.[103]

Je možné si položiť otázku, do akej miery je skúmanie dôkaznej spoľahlivosti elektronických dôkazných prostriedkov možné v konkrétnych prípadoch nahradiť formálne akceptovanou deklaráciou o dôveryhodnosti zdroja pôvodu?[104] Môže sa zdať, že takáto akceptácia „brzdí" zásadu voľného hodnotenia dôkazov a hrozí zavedením zákonnej dôkaznej teórie, čo prináša hrozbu pre účinnú súdnej ochrany.[105] Avšak súdna prax v súčasnosti ukázala, že v partikulárnych otázkach sa s podobnou formou už stretáva. V uvedenom príklade dôkazu obsahu webovej stránky je možné odkázať na § 78a OSŘ, podľa ktorého môže dôkaz byť zaistený tiež notárskym alebo exekútorským zápisom.[106] V praxi sa často na súd ako dôkaz prináša práve notárska zápisnica o existencii obsahu, resp. iných skutočností na webových stránkach. Nakoľko zabezpečenie takéhoto dôkazu bolo vykonané verejnou listinou, súd pri zisťovaní skutkového stavu považuje osvedčenia notára alebo súdneho exekútora za pravdivé, ak nie je v konaní preukázaný opak.[107] Zásadný rozdiel spočíva práve v dôkaznej sile verejnej listiny v porovnaní s dôkaznou silou súkromnej listiny

[103] Nález ÚS ČR ze dne 10. 8. 2017, sp. zn. I. ÚS 615/17.

[104] Napr. v USA ide o tzv. „pravidlo 902" v podobe dôkazu, ktorý je samostatne autentifikovateľný (*Evidence That Is Self-Authenticating*). Ide o certifikované záznamy generované elektronickým procesom alebo systémom a certifikované údaje kopírované z elektronického zariadenia, pamäťového média alebo súboru. Viď Rule 902. (13), (14) FRCP.

[105] Stanovisko generálního advokáta - Wahl - 11 září 2014. - CA Consumer Finance proti Ingrid Bakkaus a další - Věc C-449/13.

[106] Podľa § 78a OSŘ: *„Důkaz může být zajištěn také notářským nebo exekutorským zápisem o skutkovém ději nebo o stavu věci, jestliže se skutkový děj udál v přítomnosti notáře nebo soudního exekutora nebo jestliže notář nebo soudní exekutor osvědčil stav věci."* Takéto ustanovenie o zaistení dôkazu priamo v slovenskom občianskom súdnom poriadku chýba, napriek tomu sa jeho obsah plne uplatňuje v súlade so zákonom č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) – viď vyššie poznámku pod čiarou.

[107] Podľa § 134 OSŘ: *„Listiny vydané soudy České republiky nebo jinými státními orgány v mezích jejich pravomoci, jakož i listiny, které jsou zvláštními předpisy prohlášeny za veřejné, potvrzují, že jde o nařízení nebo prohlášení orgánu, který listinu vydal, a není-li dokázán opak, i pravdivost toho, co je v nich osvědčeno nebo potvrzeno."*

(súkromným *printscreenom*).[108] Aj keď pojem dôkazná sila je spájaný s povahou predloženej listiny, stojí za zamyslenie, či by si pojem dôkaznej spoľahlivosti v prípade elektronických dôkazných prostriedkov nezaslúžil väčšiu pozornosť a širší spoločenský konsenzus. Podľa Polčáka pojem *„dôkaznej spoľahlivosti je v našej právnej kultúre relatívne nový a mohol by sa postupne presadiť ako univerzálna kategória namiesto terajších nepríliš prakticky použiteľných kategórií pravosti a pravdivosti listinného dôkazu.“*[109] Význam tohto pojmu sa dá ilustrovať na príklade dôkazu o obsahu webovej stránky. Ak ide o súkromný záznam (napr. v podobe súborov s obsahom HTML kódu na dátovom nosiči), jeho dôkazná spoľahlivosť je nízka, nakoľko miera volatility tohto elektronického dôkazného prostriedku je pomerne vysoká. Ak pôjde o verejnú listinu v podobe notárskej zápisnice o osvedčení právne významnej skutočnosti – obsahu webstránky, pôjde o dôkaz s významnou dôkaznou silou, avšak z technického pohľadu veľmi limitovanou schopnosťou vypovedať širšie informácie o kóde, vzniku alebo veľkosti dát.

Istý náznak riešenia ponúka ustanovenie § 562 ods. 2 NOZ, podľa ktorého sa má za to, že *„záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý.“* Aj keď jeho pôvodným zámerom bolo ošetrenie (ne)platnosti záznamov v elektronických účtovných evidenciách, je ho možné podľa Polčáka použiť aj na *„kontraktačné platformy a iné dôveryhodné systémy generujúce elektronické písomnosti.“*[110] Napriek tomu, že je v mnohých otázkach súvisiacich s týmto ustanovením nutné ešte počkať na konštantnú judikatúru,[111] je

[108] Viď § 565 až 569 NOZ.

[109] POLČÁK, Radim. Elektronické právní jednání - změny, problémy a nové možnosti v zákoně č. 89/2012 SB. Bulletin Advokacie: www.cak.cz [online]. 2013. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-pravni-jednani-zmeny-problemy-a-nove-moznosti-v-zakone-c.-892012-sb

[110] POLČÁK, Radim. Dokazovaní elektronickými dokumentami změny, problémy a nové možnosti v zákoně č. 89/2012 Sb. Bulletin advokacie. 2014, č. 13, Str. 34–41.

[111] Napr. v minulosti NS ČR uviedol, že e-mail, ktorý nebol podpísaný elektronickým podpisom nemôže naplniť písomnú formu. Toto rozhodnutie bolo kritizované odbornou verejnosťou nakoľko neodpovedalo na to, čo je to elektronický podpis. Viď Usnesení NS ČR ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019. Domnievame sa, že súd mal zisťovať povahu „jednoduchého“ elektronického podpisu. Už v tom prípade by dané naplnilo podmienku podpisu. Viď LOUTOCKÝ, Pavel. Ochrana spotřebitele při uzavírání smluv na internetu a možnost řešení vzniklých sporů online. In: POLČÁK, Radim et al. Právo informačních technologií. 2018. Praha: Woltes Kluwer. Str. 307.

možné sa zamyslieť nad tým, akú dôkaznú spoľahlivosť má napr. elektronické potvrdenie o dôveryhodnosti zdroja pôvodu poskytnuté vrcholovým registrátorom CZ.NIC z.s.p.o. (česká doména) alebo SK.NIC (slovenská doména) v prípade zisťovania držiteľa doménového mena alebo histórie doménových prevodov? To isté platí v prípade ak sa dokazuje obsah profilu sociálnej siete na internete. Aký význam by malo nahradenie úplného súboru informácií na dátovom nosiči o profile skúmaného subjektu na sociálnej sieti formálne akceptovanou deklaráciou o dôveryhodnosti zdroja pôvodu (napr. spoločnosťou Facebook, Inc.)? Potenciál takého potvrdenia je zrejmý, avšak v súčasnosti je problém tieto elektronické záznamy v konkrétnom prípade získať.[112] Nahradili by komplikovaný proces vykonávania elektronického dôkazného prostriedku, akým môže byť obsah získaný zo zaisteného (dožiadaného) dátového nosiča, resp. notárskej zápisnice o existencii webovej stránky (najmä v prípade slovenskej domény). Čo je však dôležitejšie, zachovali by si dôkaznú spoľahlivosť, a to bez ohľadu na svoju formu. Išlo by však o prelínanie verejnoprávnej úpravy procesu dokazovania a súkromných úkonov definičných autorít (súvisiaca úvaha je predložená v osobitnej časti, v 8. kapitole: Zmenka ako elektronický dôkazný prostriedok).

2.5.3. Pravdivosť a vierohodnosť

Skúmanie pravdivosti a vierohodnosti elektronického dôkazného prostriedku predstavuje jednu z najnáročnejších častí procesu dokazovania. Pravdivosť a vierohodnosť sú previazané kategórie.[113] Pri ich hodnotení sa skúma obsah vykonaných dôkazov a či je tento obsah pravdivý a vierohodný. Len pravdivé a vierohodné elektronické dôkazné prostriedky môžu slúžiť ako *„gnozeologický základ pre vytvorenie úsudku o existencii konkrétnej skutočnosti dôležitej pre rozhodnutie vo*

[112] Úprava elektronických systémov v § 562 ods. 2 NOZ by mohla vypustiť zbytočnú požiadavku uznávaného elektronického podpisu vyžadujúceho neustále využívanie a udržiavanie kvalifikovaného certifikátu. Viď KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan, AMLER, Pavel. Elektronická identita při elektronickém (hmotně)právním jednání. Právní rozhledy. 2019, č. 18, Str. 626-632.

[113] Slovami Weinbergera: *„Dokázať tvrdenie t znamená presvedčiť sa o pravdivosti výroku t vyvodením t z iných pravdivých výrokov. Výrok t, ktorý sa má dokazovať, sa nazýva tvrdenie (téza, tiež predmet dôkazu čiže probandum). Pri dokazovaní musíme nájsť také zrejmé alebo už skôr dokázané výroky, tzv. dôkazové prostriedky čiže argumenty dôkazu, z ktorých tézy logicky vyplýva."* Viď WEINBERGER, O., ZICH, O. Logika. Praha 1965, Str. 49. alebo KŘÍSTEK, Lukáš. Jak má vypadat znalecký posudek. Soudce. 2017, č. 2, Str. 9.

veci. "[114] Pravdivosť hovorí, ktoré okolnosti možno považovať za preukázané v súlade so skutočnosťou. Miera pravdivosti určuje vierohodnosť dôkazu.[115]

Ako už bolo uvedené, tuzemské dokazovanie v súdnom konaní a následné rozhodovanie je vystavané na zásade voľného hodnotenia dôkazov. Táto zásada vyjadruje, že sudca si urobí o pravdivosti či nepravdivosti tvrdených skutočností vzhľadom na získané informácie z vykonaných dôkazov vlastný záver.[116] Táto zásada v moderných procesných poriadkoch nahradila zásadu formálneho hodnotenia dôkazov (zákonná dôkazná teória), ktorá vychádzala z toho, že určitá skutočnosť bola považovaná za dokázanú, ak ju dokazovalo určité množstvo, stupeň alebo kvalita dôkazov predpísaných v zákone alebo inej právnej norme (pozitívna forma) alebo vychádzala z toho, že ak súd nemal zákonom predpísanú kvalitu dôkazov, nesmel určitú skutočnosť považovať za dokázanú (negatívna forma).

Pravdivosť je kvalita dôkazného prostriedku, ktorou dôkaz informuje o miere závažnosti okolností. Pravdivosť predstavuje pravdepodobnostnú mieru, podľa ktorej je možné považovať určité okolnosti za dokázané a v súlade so skutočnosťou. Táto miera určuje zároveň jeho vierohodnosť.[117] Poznanie súdu je obmedzené a jeho závery majú charakter pravdepodobnostných úvah o pravdivosti dôkazu. Totiž absolútna pravda je nedostupná. Priradenie hodnoty pravdivosti ako určitého stupňa pravdepodobnosti vyústi do jeho presvedčenia či nepresvedčenia o dokazovanej skutočnosti. Súd hľadá rozumný stupeň subjektívnej istoty na základe relevantných dôvodov.[118]

Pravdivosť konania ako povinnosť strán bola v minulosti zakotvená v civilnom súdnom konaní v § 79 ods. 1 OSŘ, podľa ktorého návrh na začatie konania mal

[114] ZÁHORA, Jozef a kol. Dokazovanie v trestnom konaní. 1.vydanie. Praha: Leges, 2013, Str. 117.

[115] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Str. 67.

[116] Podľa § 132 OSŘ: *„Důkazy hodnotí soud podle své úvahy, a to každý důkaz jednotlivě a všechny důkazy v jejich vzájemné souvislosti; přitom pečlivě přihlíží ke všemu, co vyšlo za řízení najevo, včetně toho, co uvedli účastníci."* Bližsie viď DRÁPAL, BUREŠ a kol. Občanský soudní řád I, II. Komentář. 1. vydání. Praha: C. H. Beck, 2009, ISBN 978-80-7400-107-9. Str. 914.

[117] ŠÁMAL, Pavel. Provádění dokazování v hlavním líčení a úprava absolutní a relativní neúčinnosti důkazů ve věcném záměru trestního řádu. Trestněprávní revue. 2008, č. 12, Str. 349-357.

[118] GAZDA, Viktor. Míra důkazu a úloha pravděpodobnosti v důkazním právu. Právní rozhledy. 2019, č. 3, Str. 77-84.

obsahovať pravdivé opísanie rozhodujúcich skutočností. Neskôr ustanovenie § 101 ods. 1 OSŘ ukladalo účastníkom konania povinnosť pravdivého a úplného opísania všetkých potrebných skutočností. [119] V súčasnosti je pravdivosť obsiahnutá v ustanoveniach OSŘ o svedeckej výpovedi, výsluchu účastníkov, pri listinách vydaných súdmi alebo inými štátnymi orgánmi a prehlásení majetku.[120] Povinnosť pravdivosti konania ako princíp je prevzatý v slovenskom civilnom procese, kde *„strany majú povinnosť pravdivo a úplne uvádzať podstatné a rozhodujúce skutkové tvrdenia týkajúce sa sporu“* a rovnako v náležitostiach žaloby, kde žalobca má povinnosť uviesť *„pravdivé a úplné opísanie rozhodujúcich skutočností.“* [121] V českom trestnom poriadku sa skúma pravdivosť zo zákona, najmä ak ide o inštitút prehlásenia o majetku, dočasného odloženia trestného stíhania, v dohode o vine a treste, pri inštitúte spolupracujúceho obvineného a pri čítaní protokolu výsluchu z prípravného konania súdom.[122] V švajčiarskom civilnom procese vystupuje otázka pravdivosti dôkazu do popredia ak ide o nelegálne získaný dôkaz. Ten sa pripustí v spore iba vtedy, ak existuje prevažujúci záujem súdu na nájdení pravdy.[123] Rovnako švajčiarsky civilný súd môže navrhovať a vykonávať dôkazy *ex officio* vtedy, ak existujú vážne pochybnosti o pravdivosti nespornej skutočnosti.[124]

Ako je uvedené vyššie, súdy počítajú s posudzovaním pravdivosti, ale normotvorca nedefinuje tento pojem. Macur uviedol, že dokazovanie pravdivej skutočnosti ako prostriedok poznania je otrasený postmodernizmom. Tento smer chápania súčasného sveta vidí skutočnosť ako nepoznateľnú a za pravdu považuje tie tvrdenia, na ktorých sa zhodne spoločnosť. [125] Ako uviedol NSS ČR *„správní orgán rovněž nemůže provedení důkazů odmítnout s odůvodněním, že od důkazu nelze očekávat, že by potvrdil pravdivost tvrzené skutečnosti, např. u navržených svědků s poukazem na ekonomickou či personální propojenost s daňovým subjektem, neboť správní orgán*

[119] MACUR, Josef. Povinnost pravdivosti a její legislativní úprava v civilním soudním řádu. Právní rozhledy. 1999, č. 4, Str. 172 – 176.

[120] § 126 ods. 1, § 131 ods. 2, § 134 a § 260e OSŘ.

[121] § 150 ods. 1 a § 132 ods. 1 CSP.

[122] § 7a ods. 4, § 159c ods. 1, § 175a ods. 3, § 178a ods. 1 písm. a), § 212 ods. 1 TŘ.

[123] Článok 152 ods. 2 ZPO.

[124] Článok 153 ods. 2 ZPO.

[125] Ibid. SVOBODA, Karel. 2009. Str. 12 alebo MACUR, Josef. Postmodernizmus a zjišťování skutkového stavu v civilním řízení. Brno: Masarykova univerzita, 2001.

nemůže předem hodnotit pravdivost a věrohodnost důkazů, aniž vůbec tyto důkazy provedl.“[126] Preto pravdivosť je kategória kvality, ktorá môže byť braná na zreteľ až po vykonaní dôkazov.

Pravdivosť a vierohodnosť elektronického dôkazného prostriedku je závislá najmä od obsahu vykonaného dôkazného prostriedku, resp. od toho, aké poznatky sú získané o tomto prostriedku a o skutočnosti, ktorú popisuje. Môže ísť o skutkové (faktické) tvrdenia, ale aj o hodnotiace súdy (napr. kritické poznámky na diskusnom fóre). Ako uviedol NS ČR v prípade hodnotiacich súdov síce nemožno počítať s možnosťou preukázania ich „pravdivosti“, je však potrebné trvať na tom, aby sa odvíjali od rozoznateľného racionálneho skutkového základu.[127] Hodnotením dôkazov z hľadiska ich pravdivosti súd dochádza k záveru, ktoré skutočnosti, o ktorých dôkazy (pre rozhodnutie významné a zákonné) vypovedajú, možno považovať za pravdivé (dokázané) a ktoré nie. Vyhodnotenie dôkazov z hľadiska pravdivosti predpokladá tiež posúdenie vierohodnosti dôkazom poskytovanej výpovede podľa druhu dôkazného prostriedku a spôsobu, akým sa podľa zákona vykonáva.[128] Je nutné pripomenúť, že aj pri elektronických dôkazoch platí, že vo všeobecnosti dôkaz neslúži na zistenie materiálnej pravdy, ale len na preukázanie pravdivosti skutkového tvrdenia.[129] ÚS ČR sa v tomto duchu vyjadril, že *„absolutní jistota je tedy důkazní standard, který není možno v soudním řízení aplikovat, neboť by při tom důkazní břemeno prakticky nebylo možno unést.“*[130] Nesmieme zabúdať, že v súkromnom práve procesnom pravdivosť tvrdenia závisí do značnej miery od aktivity procesných strán. Navrhovateľ dôkazu musí preukázať jeho tvrdenie a protistrana ho môže vyvrátiť.[131] Preto otázku pravdivosti a vierohodnosti vykonaných elektronických dôkazov je nutné posudzovať aj vzhľadom na ostatné priame a nepriame dôkazy, okolnosti prípadu a konzistentnosť tvrdenia strán o existencie či neexistencii rozhodných skutočností.

[126] Rozsudek NSS ČR ze dne 26. 6. 2003, č. j. 22 Ca 427/2002-35.

[127] Rozsudek NS ČR ze dne 10. 1. 2013, sp. zn. 30 Cdo 2591/2011-I.

[128] Rozsudek NS ČR ze dne 20. 3. 2008, sp. zn. 21 Cdo 3075/2006.

[129] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Str. 10.

[130] Nález ÚS ČR ze dne 20. 8. 2014, sp. zn. I. ÚS 173/13.

[131] V zásade dôkazné bremeno v civilnom sporovom konaní leží na strane sporu ktorá tvrdí určitú skutočnosť. Viď MACUR, Josef. Důkazní břemeno v civilním soudním řízení. Brno: Masarykova univerzita, 1995.

Právna prax hovorí aj o *miere dôkazu*, ktorá určuje, ako vysoký musí byť stupeň vnútorného presvedčenia súdu o pravdivosti či nepravdivosti skutkového tvrdenia, aby bol dôkaz vierohodný. Tuzemské procesné právo sa neuspokojuje s prevažujúcou pravdepodobnosťou zistenia skutočností (tak, ako je tomu napr. v USA), ale nežiada ani absolútnu istotu.[132]

Pre potreby tejto práce môžeme z pohľadu načrtnutej kategórie pravdivosti a vierohodnosti rozdeliť elektronické dôkazné prostriedky na dve skupiny:

- Otvorené elektronické dôkazné prostriedky
    - Verejne dostupné elektronické dáta na sieti internet alebo inej verejne dostupnej sieti, avšak nejde o notoriety[133] (napr. otvorené webstránky, elektronické publikácie, audio-vizuálne diela, metadáta verejných technických informácií ako sú záznamy WHOIS, verejné profily sociálnych sietí, vyhľadané záznamy vo vyhľadávači, obsah informácie v databázach systému *blockchain* ako je napr. krypto mena Bitcoin, články na Wikipedii).
    - Vďaka technológií je ich dostupnosť a obsah možné overiť nezávislé na procesných stranách alebo súde,[134] preto pravdivosť a vierohodnosť môže byť skúmaná len z ich obsahového hľadiska.

- Uzavreté elektronické dôkazné prostriedky
    - Neverejné elektronické dáta, ktoré sú uzamknuté alebo šifrované alebo prístupné len určitému okruhu osôb (napr. cloudové úložiská, súkromné servery, dátové nosiče, mobilné zariadenia, osobné počítače, USB

[132] KANDOVÁ, Katarína. Pojem pravdy (nejen) v trestním řízení a některé související instituty. Právník, Praha: AV ČR, Ústav státu a práva, 2017, roč. 156, č. 10, ISSN 0231-6625. Str. 842-857.

[133] Notorieta je skutočnosť, ktorú nie je potrebné dokazovať, lebo sa pokladá za všeobecne známu (napr. 2 x 2 = 4) alebo právne predpisy uverejnené v zbierke zákonov. Viď 127 OSŘ. V trestnom konaní notoriety nie sú priamo definované, avšak nedokazujú sa skutočnosti, ktoré sa podľa všeobecnej skúsenosti, logiky a ustálených pravidiel myslenia považujú za pravdivé, ak o nich nevznikli pochybnosti, alebo skutočnosti, ktoré štátny zástupca a obvinený označili za nesporné (§ 314d ods. 2 TŘ). PÚRY, František. Notorieta. In: HENDRYCH, Dušan, BĚLINA, Miroslav, FIALA, Josef, ŠÁMAL, Pavel, ŠTURMA, Pavel, ŠTENGLOVÁ, Ivana, KARFÍKOVÁ, Marie. Právnický slovník. 3. vydání. Praha: Nakladatelství C. H. Beck, 2009.

[134] Aj keby išlo o článok publikovaný procesnou stranou na internete, ktorý dotknutá strana stiahla alebo zmazala, v dnešnej dobe je možné dopátrať jeho obsah pomocou služieb ako je web archív (napr. http://web.archive.org).

kľúče, prevádzkové a lokalizačné údaje, dohľadové systémy kybernetickej bezpečnosti).

- Existenciu nie je možné overiť nezávislé od procesných strán, tretích osôb alebo súdu.
- Pravdivosť a vierohodnosť je skúmaná z obsahového hľadiska, ale aj z technického hľadiska (formálna stránka). Ide o súvislosť so spoľahlivosťou a integritou elektronického dôkazného prostriedku. Je preto možné sa pýtať, či bol daný elektronický dôkazný prostriedok technicky manipulovaný tak, aby budil dojem pravdivosti a vierohodnosti?

Vzhľadom na to, že pri uzavretých elektronických dôkazných prostriedkoch je pravdivosť a vierohodnosť často skúmaná aj z technického hľadiska, miera dôkazu sa pri jednotlivých dôkazoch zdá byť vyššia ako pri otvorených elektronických dôkazných prostriedkoch. Preto miera dôkazu pri vyťaženom USB kľúči alebo mobilnom telefóne bude vyššia ako pri prečítaní dostupného komentáre na verejnom diskusnom webfóre, kde navyše môže byť jeho autenticita potvrdená alebo vyvrátená treťou stranou (prevádzkovateľom).

Všeobecne platí, že súd vychádza zo zhodných tvrdení strán, ak neexistuje dôvodná pochybnosť o ich pravdivosti.[135] Zaujímavou otázkou je dôkaz negatívnej skutočnosti, resp. neexistencie skutočnosti. NS ČR uviedol, že dôkazné návrhy nie je možné zamietnuť iba z toho dôvodu, že by snáď bolo vylúčené preukázať neexistenciu skutočnosti. Totiž súčasná civilistická doktrína pripúšťa, že aj negatívnu skutočnosť možno dokazovať.[136] Toto rozhodnutie vyvolalo civilistickú diskusiu o obrátení dôkazného bremena s dokazovaním negatívnych skutočností. Zdá sa totiž, že ak nemožno negatívum dokázať, môže sa dôkazné bremeno za určitých okolností javiť ako nespravodlivé a priečiace sa spravodlivému procesu.[137] V takýchto prípadoch by malo byť dôkazné bremeno výnimočne otočené. Strana, ktorá popiera negatívum, musí dokázať pozitívum. Podľa Pulkrábeka *„historická negativní teorie dělení důkazního*

[135] § 186 ods. 2 CSP.

[136] Rozsudek NS ČR ze dne 26. 7. 2017, sp. zn. 22 Cdo 1479/2017.

[137] PULKRÁBEK, Zdeněk. O dokazování negativních skutečností v civilním soudním řízení (a o některých zásadách zjišťování skutkového stavu vůbec). Právní rozhledy. 2013, č. 17, Str. 573-580.

břemena se snažila o důkladnou argumentaci, je dnes jediným argumentem intuitivní a nesprávný názor, že nelze prokázat neexistenci, resp. – v mírnější verzi – „trvající neexistenci.“[138] Na mieste je otázka, či forma elektronické dôkazného prostriedku v súkromnom práve prispeje k lepšiemu dôkazu o neexistencii skutočnosti? Negatívnu skutočnosť je možné dokázať často pomocou inej skutočnosti (nepriamym dôkazom, resp. indíciou). Ako príklad je možné uviesť dokazovanie skutočnosti o nedodaní elektronického súboru protistranou. Ak si strany dohodli technologický postup plnenia (napríklad zdieľané úložisko v podobe cloudu), je na dokazujúcej strane, aby zaobstarala alebo navrhla zaobstarať elektronický záznam prístupov, zmien súborov a ich časový prehľad (*log file*).[139] Tento záznam musí vykazovať dôkaznú spoľahlivosť a integritu. V ideálnom prípade bude potvrdený prevádzkovateľom úložiska. Takýto záznam by mohol priniesť informáciu o tom, že protistrana v rozhodnom období nepristúpila alebo nenahrala požadovaný súbor do dátového úložiska podľa dohody. Vyjadrenie tretej strany je vhodné. Tá je totiž v postavení svedka, ktorý dáva výpoveď o aktivitách na svojom systéme a dokáže priniesť vyjadrenie o možnostiach svojho systému. Ak vyjadrenie nie je možné alebo cloud je v správe protistrany, potvrdenie prevádzkovateľa je možné nahradiť znaleckým dokazovaním. Tu však pristupuje otázka vykonateľnosti takéhoto znaleckého skúmania. V neposlednom rade je potrebné dodať, že v procesnom práve je otázka pravdivosti a vierohodnosti pojmovo oddeliteľná od kategórie platnosti a zákonnosti, ktorá bude vysvetlená v nasledujúcej časti.[140]

2.5.4. Platnosť a zákonnosť

Proces dokazovania a jeho teória má interdisciplinárny a medziodborový charakter. Na úvod je v otázkach kategórie platnosti a zákonnosti možné uviesť tri kľúčové

[138] PULKRÁBEK, Zdeněk. Znovu a trochu jinak o dokazování negativních skutečností. Právní rozhledy. 2018, č. 1, Str. 17-20.

[139] Napr. pred zahájením konania môže súd zaistiť dôkaz podľa § 78 alebo § 78a OSŘ. Na Slovensku ide o § 345 ods. 1 CSP podľa ktorého *„pred začatím konania, počas konania a po skončení konania vo veci samej možno na návrh zabezpečiť dôkaz alebo dôkazný prostriedok, ak je obava, že neskôr ho nebude možné vykonať vôbec alebo len s veľkými ťažkosťami.“*

[140] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Str. 21.

zásady dokazovania rešpektované v trestnom procesnom práve, ktoré predstavujú typickú nezákonnosť dôkazov:[141]

- *Dôkaz nesmie byť získaný a vykonaný v rozpore s platným právnym poriadkom.*
- *Dôkaz nesmie byť získaný donútením alebo hrozbou takého donútenia.*
- *Nik nesmie usvedčovať sám seba, preto obvinený má právo odoprieť výpoveď.*

Tieto zásady sú odrazom princípu zákonnosti, resp. legality.[142] Dokazovanie musí byť v súlade s ústavným poriadkom (zriadením) a platným právom. To predstavuje základný pilier a garanciu práva na spravodlivý proces. Súdne konanie a každá jeho časť vrátane znaleckého dokazovania sa riadi určitými pravidlami, ktoré majú najmä zabezpečiť to, aby bol výsledný súdny proces spravodlivý.[143]

Princíp zákonnosti má svoj odraz aj v civilnom konaní. Za dôkaz vo všeobecnosti môžu slúžiť všetky dôkazné prostriedky, ktorými možno zistiť stav veci. Ide najmä o *„výsluch svedkov, znalecký posudok, správy a vyjadrenia orgánov, fyzických a právnických osôb, notárske alebo exekútorské zápisy a iné listiny, ohliadka a výsluch účastníkov.“* [144] Elektronický dôkazný prostriedok ako samostatný typ prostriedku tak nie je uvedený ani v českom alebo slovenskom súdnom poriadku.[145] Nakoľko ide často len o zákonom uvedený demonštratívny výpočet typov dôkazných prostriedkov, nespôsobuje to automaticky neplatnosť alebo nezákonnosť procesného úkonu

[141] Ibid. ZÁHORA, Jozef a kol. Dokazovanie v trestnom konaní. Str. 19., alebo REPÍK, B. Procesní důsledky porušení předpisů o dokazování v trestním řízení, Bulletin advokacie, 1982, Str. 125-126.

[142] ÚS ČR o princípe legality uviedol, že *„podle čl. 1 Ústavy je Česká republika demokratickým právním státem. Ústavní soud již dříve uvedl, že Česká republika se hlásí k principům nejen formálního, nýbrž především materiálního právního státu. Ústava akceptuje a respektuje princip legality jako součást celkové koncepce právního státu, neváže však pozitivní právo jen na formální legalitu, ale výklad a použití právních norem podřizuje jejich obsahově materiálnímu smyslu.“* Nález ÚS ČR ze dne 27. 9. 2006, sp. zn. Pl. ÚS 51/06.

[143] TOMOSZEK, Maxim. Jaké zásady pro znalecké dokazování vyplývají z práva na spravedlivý proces? Časopis pro právní vědu a praxi. 2020, č. 1, Str. 55-70.

[144] § 125 veta prvá OSŘ.

[145] V zmysle § 185 ods. 1 CSP *„za dôkaz môže slúžiť všetko, čo môže prispieť k náležitému objasneniu veci a čo sa získalo zákonným spôsobom z dôkazných prostriedkov“ a podľa § 185 ods. 1 CSP „dôkazným prostriedkom je najmä výsluch strany, výsluch svedka, listina, odborné vyjadrenie, znalecké dokazovanie a obhliadka. Ak nie je spôsob vykonania dôkazu predpísaný, určí ho súd.“*

vykonania elektronického dôkazného prostriedku. Zákon ponecháva na súde rozhodnutie o tom, ako bude zisťovať *questio facti*.[146] Otázkou ostáva, čo spôsobuje neplatnosť alebo nezákonnosť elektronického dôkazného prostriedku, resp. ovplyvní táto forma nároky toho ktorého súdu na jeho vykonanie?

V prvom rade, v civilnom konaní elektronický dôkazný prostriedok a dôkaz musí byť získaný, ale aj vykonaný v súlade so zákonom. Ide o kumulatívne podmienky. Ak by tieto dve podmienky neboli naplnené, súd by k nemu nemal prihliadnuť, čo by predstavovalo jeho neplatnosť.[147] To potvrdil NS ČR vo svojom rozhodnutí, keď uviedol, že *„při hodnocení důkazů po stránce jejich zákonnosti zkoumá soud, zda důkazy byly získány (opatřeny) a provedeny způsobem odpovídajícím zákonu nebo zda v tomto směru vykazují vady (zda jde o důkazy zákonné či nezákonné); k důkazům, které byly získány (opatřeny) nebo provedeny v rozporu s obecně závaznými právními předpisy, soud nepřihlédne.*“[148] V praxi však existujú situácie, kedy elektronický dôkazný prostriedok nebol získaný v súlade s platným právom a môže porušovať práva a právom chránené záujmy protistrany, avšak má silný potenciál objasniť dokazovanú skutočnosť. Takýto prostriedok je často navrhnutý z dôvodu ochrany iného práva alebo záujmu ako toho, do ktorého zasahuje. Súd tak bude stáť pred otázkou, ako vyrieši stret záujmov dvoch alebo viacerých protichodných práv, t.j. ako aplikovať test proporcionality.[149]

[146] V zmysle § 125 veta druhá OSŘ, pokiaľ nie je spôsob vykonania dôkazu predpísaný, určí ho súd.

[147] WINTEROVÁ, Alena a kol. Civilní právo procesní. 6. aktualiz. vyd. Praha. Linde. 2008. Str. 273.

[148] Rozsudek NS ČR ze dne 20. 3. 2008, sp. zn. 21 Cdo 3075/2006.

[149] Slovenský CSP priamo počíta s takýmto dôkazom v čl. 16, keď stanoví že „súd pri prejednávaní a rozhodovaní veci nezohľadňuje skutočnosti a dôkazy, ktoré boli získané v rozpore so zákonom, ibaže vykonanie dôkazu získaného v rozpore so zákonom je odôvodnené uplatnením čl. 3 ods. 1.“ Čl. 3 ods. 1 CSP hovorí, že *„každé ustanovenie tohto zákona je potrebné vykladať v súlade s Ústavou Slovenskej republiky, verejným poriadkom, princípmi, na ktorých spočíva tento zákon, s medzinárodnoprávnymi záväzkami Slovenskej republiky, ktoré majú prednosť pred zákonom, judikatúrou Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie, a to s trvalým zreteľom na hodnoty, ktoré sú nimi chránené.“*

Test proporcionality pozostáva z troch krokov.[150] Súd posudzuje:

1. Účelnosť

    - Súd posudzuje účelnosť (vhodnosť) zásahu, t.j. vykonania dôkazu a či navrhnutý elektronický dôkazný prostriedok naozaj osvetlí zisťovanú skutočnosť. Ak nezákonne získaný elektronický dôkazný prostriedok, ktorý predstavuje zásah do práv a právom chránených záujmov, nie je spôsobilý sledovaný účel dosiahnuť, išlo by o prejav svojvôle zo strany súdu, ak by ho vykonal.[151] Účel by dozaista nebol naplnený v prípade, ak by sa žalujúca strana sporu snažila navrhnúť vykonať elektronický dôkazný prostriedok v podobe emailového archívu (dátového nosiča) obsahujúceho viaceré emailové účty aj nezainteresovaných strán, ktorý by bol protiprávne získaný, avšak bol by technologicky uzamknutý (zašifrovaný) tak, že nie je spôsobilý byť interpretovaný cudzími osobami vrátane forenzných expertov (napr. súdny znalec).

2. Potrebnosť

    - Súd skúma či je navrhnutý elektronický prostriedok vôbec potrebné vykonať a či nemožno sledovaný účel dosiahnuť aj inými dôkaznými prostriedkami. Preferenciu ma vždy taký prostriedok, ktorý zasahuje do práv a právom chránených záujmov procesných strán v čo najmenšej miere. Zdá sa, že ide o požiadavku minimalizácie zásahu, resp. preukázania dôkaznej núdze na strane navrhovateľa dôkazu. Ak súd môže vypočuť svedkov o dokazovanej skutočnosti s primeraným a vierohodným výsledkom, nepripustí vykonanie obrazovo-zvukového záznamu, ktorý by zasahoval do práv protistrany a bol získaný v rozpore s platným právom.

[150] Vučka formuloval zjednodušenú nerovnosť pri aplikácií testu proporcionality pre každú osobu, do ktorej práv sa pri zabezpečovaní dôkazov priamo zasahuje: *„(i) závažnost činu x pravděpodobnost, (ii) zajištění důkazu x významnost důkazu, (iii) ≥ intenzita zásahu do práv.“* Viď VUČKA, Jan. Test proporcionality při zajišťování důkazů. Trestněprávní revue. 2010, č. 9, Str. 290-293.

[151] Ibid. VUČKA, Jan. Test proporcionality při zajišťování důkazů.

3. Primeranosť[152]

- Ide o najdôležitejší a najkomplexnejší krok. Súd skúma primeranosť v užšom zmysle. Zvažuje sa proporcionalita medzi ujmou na právach a verejným záujmom na zásahu do týchto práv. Ujma nesmie byť neprimeraná vo vzťahu k zamýšľanému účelu.[153] Súd skúma, či je záujem na unesení dôkazného bremena vyšší ako záujem na ochrane práva porušeného nezákonne získaným a vykonaným elektronickým

[152] Česká judikatúra k otázkam primeranosti zásahu do práv pri použití nezákonného zásahu je pomerne bohatá. NS ČR v otázke **zvukového záznamu** judikoval, že *„zvukový záznam zachycující projevy, ke kterým dochází při výkonu povolání, při obchodní či veřejné činnosti, zpravidla nelze považovat za zaznamenání projevu osobní povahy; důkaz takovým záznamem v občanském soudním řízení proto není nepřípustný.“* (Viď Rozsudek NS ČR ze dne 11. 5. 2005, sp. zn. 30 Cdo 64/2004) V ďalšom prípade ohľadom **nahrávania obchodných telefonických rozhovorov**, ÚS ČR uviedol, že *„hovory fyzických osob, ke kterým dochází při výkonu povolání, obchodní či veřejné činnosti, zpravidla nemají charakter projevů osobní povahy. Zvukový záznam takového hovoru pořízený navíc po předchozím upozornění, že hovor je zaznamenáván, může soud použít jako důkazní prostředek v občanském soudním řízení, jímž lze zjistit skutkový stav věci, poté, co zvážil, zda měl účastník uplatňující informace ze záznamu k jejich získání jiné, z hlediska zásahu do soukromí druhé osoby šetrnější možnosti.“* (Viď Nález ÚS ČR ze dne 27. 2. 2018, sp. zn. II. ÚS 2299/17) V inom prípade **nahrávania súkromných rozhovorov** ÚS ČR sa vyslovil, že *„za běžných okolností je svévolné nahrávání soukromých rozhovorů bez vědomí jejich účastníků hrubým zásahem do jejich soukromí. Takový postup s rysy záludnosti je ve velké většině případů morálně i právně nepřijatelný, zejména je-li veden záměrem nahrávanou osobu poškodit. ÚS se rozhodně staví proti nekalým praktikám vzájemného elektronického sledování a skrytého nahrávání při soukromých i profesionálních jednáních, jež zpravidla jsou nejen v rozporu s právem, ale také šíří ve společnosti atmosféru podezíravosti, strachu, nejistoty a nedůvěry. Zcela odlišně je však třeba posuzovat případy, kdy je tajné pořízení záznamu rozhovoru součástí obrany oběti trestného činu proti pachateli nebo jde-li o způsob dosažení ochrany výrazně slabší strany významného občanskoprávního a zejména pracovněprávního sporu. Zásah do práva na soukromí osoby, jejíž mluvený projev je zaznamenán, je zde ospravedlnitelný zájmem na ochraně slabší strany právního vztahu, jíž hrozí závažná újma (např. ztráta zaměstnání). Opatření jediného nebo klíčového důkazu touto cestou je analogické k jednání za podmínek krajní nouze či dovolené svépomoci.“* (Viď Nález ÚS ČR ze dne 9. 12. 2014, sp. zn. II. ÚS 1774/14) Otázka proporcionality v dokazovaní bola riešená aj v prípade použitia **testu DNA**, keď NS ČR sa vyslovil, že majetkový záujem žalovanej nemožno považovať za dostatočný dôvod na zásahu do nastolených rodinných väzieb. *„Test DNA vyhotovený na základě vzorku DNA odebraného z těla zemřelého, aniž by k tomu dal souhlas před smrtí sám zemřelý, nebo po jeho smrti osoby oprávněné k pietní ochraně osobnosti podle § 15 obč. zák., je nezákonně získaným důkazem a jako takový je v řízení nepřípustný.“* (Viď Rozsudek NS ČR ze dne 24. 9. 2014, sp. zn. 30 Cdo 1982/2012) NS ČR rovnako odmietol protiprávne vyhotovenie **protiprávnych obrazových záznamov** poisťovne na svoju obranu. Uviedol, že „*jestliže pojistitel jako soukromá osoba při zjišťování rozsahu škody pořídil vizuální záznamy pojištěného v okolí jeho bydliště a na jiných veřejných prostranstvích svémocně (konspirativně) bez jeho souhlasu, přestože nahrávku sám nešířil a pouze ji v řízení o náhradu škody na zdraví vzniklé pojištěnému nabídl jako důkaz k možnému provedení, porušil tím právo pojištěného na ochranu podoby. Nelze připustit, že by záznamy takto nelegálně pořízené bylo možno dále legálně používat, resp. využívat, byť k důkazům u soudu.“* (Viď Rozsudek NS ČR ze dne 27. 5. 2015, sp. zn. 30 Cdo 5216/2014).

[153] Viď konštantnú judikatúru o otázke primeranosti v teste proporcionality ÚS ČR: Nález ÚS ČR ze dne 1. 3. 2007, sp. zn. Pl. ÚS 8/06, Nález ÚS ČR ze dne 13. 8. 2002, sp. zn. Pl. ÚS 3/02, Nález ÚS ČR ze dne 3. 9. 2009, sp. zn. III. ÚS 346/09, Nález ÚS ČR ze dne 3. 9. 2009, sp. zn. III. ÚS 346/09, Nález ÚS ČR ze dne 15. 1. 2009, sp. zn. IV. ÚS 1554/08.

dôkazným prostriedkom.[154] Ak sa súd rozhodne vykonať nezákonne získaný elektronický dôkazný prostriedok (napr. nelegálne získaný výpis sociálneho profilu z účtu LinkedIn), je povinný vo svojom rozhodnutí zdôvodniť, prečo dal právo na ochranu osobnosti dotknutej osoby na druhú koľaj. Musí uviesť prečo uprednostnil iné právo alebo právom chránený záujem, ktorého porušenie sa má preukázať týmto dôkazom (napr. zmluvné, majetkové právo alebo právo duševného vlastníctva).

Na tomto mieste považujeme za potrebné spomenúť pojem *neústavnosti* dôkazného prostriedku, ktorý v sebe logicky zahŕňa neplatnosť a nezákonnosť, avšak je výsledkom ústavného prieskumu. Podľa Hanuša ingerencia ÚS ČR do rozhodovacej činnosti všeobecných súdov vo vzťahu k dôkazného procesu je sporadická a týka sa iba prípadov, ktoré sú relevantné pre nájdenie ústavnoprávnych vád, resp. neústavnosti a nezákonnosti dôkazu. Ide o také vady, ktoré sú „*dôsledkom nedostatočného či prípadne racionálne logicky neakceptovateľného odôvodnenia, ako aj odôvodnenia, ktoré sa opiera o dokazovanie, ktoré ústavným (zákonným) postulátom odporujúcej vady ich robí nepoužiteľným pre vyvodenie skutkového základu veci. Sú teda zahrnuteľné pod pojem svojvôle (ľubovôle) v najširšom zmysle.“*[155] Rozlišuje tri zásadné okruhy neústavných dôkazov:

- zabudnuté (opomenuté) dôkazy, resp. nevykonané dôkazy,[156]

[154] Napr. ÚS ČR pri otázke proporcionality uviedol. že *„použitelnost záznamu rozhovoru pořízeného soukromou osobou bez vědomí nahrávané osoby jako důkazu v příslušném řízení je závislá na poměřování chráněných práv a zájmů, které se v této soukromé sféře střetávají. Zásah do práva na soukromí osoby, jejíž mluvený projev je zaznamenán, je ospravedlnitelný zájmem na ochraně slabší strany právního vztahu, jíž hrozí závažná újma (včetně např. ztráty zaměstnání). Opatření jediného nebo klíčového důkazu touto cestou je analogické k jednání za podmínek krajní nouze či dovolené svépomoci.“* Nález ÚS ČR ze dne 9. 12. 2014, sp. zn. II. ÚS 1774/14.

[155] HANUŠ, Libor. Ústavněprávní vady důkazního procesu z pohledu judikatury Ústavního soudu. Právní rozhledy. 2006, č. 18, Str. 647 – 653.

[156] Ide o vady súdneho rozhodnutia *„ktoré sa malo vysporiadať s myšlienkovými úvahami súdu a s vykonanými dôkaznými prostriedkami v tom zmysle, že vo vzťahu k nim alebo ich nezanedbateľným častiam (v prípade napr. výsluchu účastníkov konania alebo svedkov) nie sú predložené citeľné argumenty o tom, aké z nich súdy vyvodili závery (v relácii k ich vierohodnosti, pravdivosti a závažnosti) podporujúce či odporujúce tvrdenie, ku ktorých preukázanie boli vykonané.“* Ibid. HANUŠ, Libor. Ústavněprávní vady důkazního procesu z pohledu judikatury Ústavního soudu.

- dôkaz (informácia v ňom obsiahnutá) nepochádza čo do jednotlivých čiastkových komponentov (fáz) procesu vykonávania dôkazov z procesne prípustného spôsobu,[157]
- skutkové zistenia sú v extrémnom nesúlade s vykonanými dôkazmi (nemajú oporu vo vykonanom dokazovaní), čo môže spôsobiť aj nesprávne právne posúdenie.

Domnievame sa, že platnosť a zákonnosť sú veľmi komplexné kategórie kvality. V praxi bude argumentom najčastejšie spochybnenie zákonnosti navrhnutého dôkazného prostriedku. Teoretické uchopenie dokazovania v súkromnom práve a najmä riešenia konfliktov práv spôsobených ich rôznymi záujmami, či už pomocou legislatívnej úpravy (napr. v slovenskom CSP) alebo rozhodovacou praxou súdov o teste proporcionality, nasvedčuje dostatočnej garancii pre správne pochopenie tejto kategórie aj pre elektronické dokazovanie. Na základe vyššie uvedeného je možné uviesť, že kategória platnosti a zákonnosti je vzájomne závislá aj na formálnych vlastnostiach dôkazu (dôkaznej spoľahlivosti). Ide o závislosť na tom, ako sa dôkazný prostriedok získal a uchovával (napr. na technickom spôsobe vyťaženia a uchovávania elektronického nosiča) alebo na objektívnej možnosti kontroly vzniku, zmeny a zániku elektronického nosiča a tiež na nestrannom vykonaní tohto dôkazu. Tieto skutočnosti môžu zohrať podstatnú rolu pri úvahách súdu o účelnosti, potrebnosti a primeranosti. V kontinentálnom systéme civilného práva procesného, všetky kategórie kvalít elektronického dôkazného prostriedku sú vždy vyhodnocované súdom na základe zásady voľného hodnotenia dôkazov na čo nadviažeme v nasledujúcej časti.

2.6. Zásada voľného hodnotenia dôkazov ako analýza rizík

2.6.1. Všeobecne o zásade voľného hodnotenia dôkazov

Český, resp. slovenský súdny proces týkajúci sa otázky dokazovania je vystavaný na zásade voľného hodnotenia dôkazov. Korene tejto zásady siahajú až do rímskeho práva, kde mal sudca pomerne veľkú voľnosť vyhodnocovať všetky dôkazy podľa

[157] Podľa rozhodnutia ÚS ČR *„důkazem může být toliko ten prostředek, jímž lze zjistit a objasnit skutečný stav věci, jenž je předvídán příslušným procesním řádem a jenž je podle tohoto řádu proveden. Tyto požadavky, tj. určitost a předvídatelnost procesních pravidel, jakož i jejich promítnutí do důkazního řízení, nutno podřadit pod kautely vyžadované čl. 36 odst. 1 Listiny základních práv a svobod.“* Viď Nález ÚS ČR ze dne 1. 11. 2001, sp. zn. III. ÚS 190/01.

svojej úvahy.[158] V súčasnosti je táto zásada zachytená v mnohých procesných kódexoch krajín kontinentálneho práva. Zásada je vystavaná na premise, že žiaden dôkazný prostriedok nemá väčšiu alebo menšiu formálnu silu alebo váhu.[159] Dôkazy súd hodnotí podľa svojej úvahy, a to každý dôkaz jednotlivo a všetky dôkazy v ich vzájomnej súvislosti. Súd by mal prihliadať na každú skutočnosť, ktorá vyšla počas konania najavo.[160] Podľa Polčáka *„jediným limitem skutečně omezujícím kontinentálního soudce v jeho skutkové úvaze je totiž kromě empirie už pouze logika.“*[161] Opakom tejto zásady je zásada *zákonnej dôkaznej (sprievodnej) teórie*, podľa ktorej existujú prísne predpísané pravidlá dokazovania (t.j. spôsob získania, uchovávania a vykonania dôkazov). Ide o rôzne povinné normy ako aplikovať skutkové tvrdenia a ako hodnotiť dôkaznú spoľahlivosť. Tuzemské procesné poriadky a právna prax sú v otázkach aplikácie tejto zásady jednotné, odlišujú sa len prístupom k iným procesným zásadám. Napríklad sporové občianske konanie je ovládané zásadou prejednávaciou a dispozičnou (súd vykoná tie dôkazy, ktoré strany sami navrhnú, iniciatívu majú účastníci konania), no dokazovanie v trestnom práve je okrem iných zásad ovládané vyhľadávacou (vyšetrovacou) zásadou (OČTK majú povinnosť zisťovať informácie v prospech, ale aj neprospech vyšetrovaného).[162] Potrebné vedomosti súdu sú však jednotne vybudované na základe odpovedí na otázky *questio facti* a *questio iuris*. Súdne rozhodnutie o odpovediach na obe otázky spolu s riadnym odôvodnením musí byť preskúmateľné v ďalšom inštančnom postupe.[163]

V súvislosti so všeobecným vysvetlením zásady voľného hodnotenia dôkazov je ešte potrebné sa zamyslieť nad pojmami *materiálnej* a *formálnej pravdy*, ktoré

[158] Až v neskoršom období došlo k predpísaniu pravidiel pre druh a silu jednotlivých dôkazných prostriedkov. Viď BRTKO, Róbert. Dôkazy a dokazovanie v rímskom občianskom procese. Akadémia PZ v Bratislave. [online]. [cit.1.9.2020]. Dostupné z: https://www.akademiapz.sk/sites/default/files/OVVP/004%20BRTKO_cl_Dokazy_APZ.pdf

[159] Ide o opačný princíp oproti anglo-americkému dôkaznému právu, kde niektoré dôkazy požívajú nižšiu dôkaznú silu alebo váhu (napr. atypické a doposiaľ nepoznané dôkazné prostriedky, akým môže byť stresový faktor vypočítaný digitálnymi *smart* hodinkami na základe utajeného algoritmu).

[160] § 191 CSP, § 132 OSŘ.

[161] Ibid. POLČÁK, Radim; PÚRY, František; HARAŠTA, Jakub a kol. Str. 32.

[162] Správny poriadok upravuje dokazovanie v správnom práve procesnom a finančné právo zas definuje nezávisle svoje zásady dokazovania v daňovom poriadku atď. Viď DŘ a SŘ.

[163] WINTEROVÁ, Alena a kol. Civilní právo procesní. 6. aktualiz. vyd. Praha. Linde. 2008. Str.239 an.

predstavujú východiská pre český, ale aj slovenský civilný proces. Materiálna pravda je objektívna pravda, resp. také zistenie, ktoré zodpovedá materiálnej a reálnej skutočnosti. Takýto proces sa často označuje ako materiálny. Protipólom tohto konceptu je takzvaná formálna pravda. Formálna pravda je skutkové zistenie, ku ktorému sa dospeje na základe regulovaného alebo zákonom daného postupu, resp. procesných pravidiel, ktoré nemajú za účel vykonanie dokazovania, pretože výsledkom takého dokazovania by mohol nastať rozpor s objektívnou realitou.[164] Súhlasíme s názorom Šámala, ktorý uvádza, že charakteristika pravdivosti ako atribút materiálnej pravdy je už celkom nadbytočná a používanie pojmu materiálnej pravdy je na mieste *„jen ve vztahu ke svému protikladu, tedy k pojmu „formální pravdy“, což pak má úzký vztah k rozlišování teorie volného hodnocení důkazů oproti zákonné teorii průvodní, nebo-li teorii formálních důkazů.“*[165] Zdá sa, že v sporových (kontradiktórnych) konaniach pojmy materiálnej a formálnej pravdy strácajú zmysel. Za zmienku stojí možno vhodnejší pojem *procesnej pravdy*, a to pre občianske súdne konanie, ako aj pre trestné konanie.[166] Domnievame sa, že tolerancia dvoch právd predstavuje oxymoron a deformuje civilné konanie.[167]

Otázkou je, ako súd prichádza na procesnú pravdu, resp. k odpovediam na *questio facti*? A je vôbec zásada voľného hodnotenia dôkazov naozaj voľná? V procese dokazovania elektronickými dôkaznými prostriedkami je úvaha súdu pri aplikácii zásady voľného hodnotenia dôkazov ovplyvnená aj technológiou, resp. vedeckým a technickým spracovaním dôkazov (formou). Podľa Damašku je *questio facti* nesprávny termín, resp. nevystihuje pomenovanie toho, o čo sa tu snaží súd pri skúmaní sprostredkovanej skutočnosti. *„Ide vlastne o právnu otázku, ale natoľko úzko spätú s faktickými okolnosťami konkrétnych prípadov, že je pre právnika civilného práva málo akademicky zaujímavá.“*[168] Damaška pri porovnaní anglo-amerického dôkazného

[164] Formálna pravda je obzvlášť ťažko definovateľná, miestami predstavuje oxymoron a je ako žena policajného vyšetrovateľa Columba, doposiaľ ju nikto nevidel.

[165] ŠÁMAL, Pavel. Provádění dokazování v hlavním líčení a úprava absolutní a relativní neúčinnosti důkazů ve věcném záměru trestního řádu. Trestněprávní revue. 2008, č. 12, Str. 349-357.

[166] BRTNÍK, Stanislav. Materiální a formální pravda v současném soudním procesu. Bulletin advokacie. 2010, č. 10, Str. 42-45.

[167] Ibid. SVOBODA, Karel, Dokazovaní, Str. 19.

[168] DAMAŠKA, Mirjan. A Continental Lawyer in an American Law School: Trials and Tribulations of Adjustment. University of Pennsylvania Law Review, vol. 116, no. 8, 1968, Str. 1363–1378.

systému s kontinentálnou zásadou voľného hodnotenia dôkazov predpovedal, že *„k radikálnemu vedeckému spracovaniu dôkazov však pravdepodobne nedôjde v blízkej budúcnosti. Z krátkodobého hľadiska je pravdepodobnejšie, že dôjde k ďalšiemu rastu pravidiel, ktoré si vyžadujú, aby sa určité faktické zistenia urobili na základe vedeckých a technických poznatkov.“* [169] Nemožno s týmto tvrdením nesúhlasiť, faktické zistenia urobené na základe vedeckých a technických poznatkov sa stávajú kľúčovými v procese elektronického dokazovania. Avšak nie absencia osobitných právnych noriem o elektronickom dokazovaní, ale absencia transparentného vysvetlenia a porozumenia o vedeckých a technických poznatkoch predstavuje kľúčový limit súčasného súdneho dokazovania pomocou elektronického dôkazného prostriedku. Ak súd predloží odpoveď na otázku *questio facti,* nevyhnutne to ovplyvní aj jeho odpoveď na *questio iuris.*

Ak rozhodnutie stojí a padá na kľúčovom dôkaze prepisu konverzácie z mobilného zariadenia a súd vyhodnotí dôkaz ako nespoľahlivý, môže ísť o dve hypotetické situácie:

1. Súd vyhodnotil dôkaz ako nespoľahlivý. Iné nepriame dôkazy potvrdili jeho falšovanie. Konverzácia z mobilného zariadenia totiž bola pozmenená (falšovaná). Súd nevidel rozpor medzi svojím rozhodnutím a objektívnymi technickými poznatkami. V ďalšom konaní vyšlo najavo, že súd sa nezaoberal celou podstatou elektronického dôkazného prostriedku, a to vrátane použitej technológie. Súd síce nedostatočne pochopil podstatu elektronického dôkazného prostriedku, napriek tomu jeho rozhodnutie bolo správne. [170]

2. Súd vyhodnotí dôkaz ako nespoľahlivý. Súd sa uspokojil so znaleckým posudkom, ktorý konštatoval neurčitosť pôvodu konverzácie.[171] Avšak technológia (napr. unikátny anonymný identifikátor oboch komunikujúcich) nebola dostatočne preverená a daná do súvisu s ostatnými získanými dôkazmi, ktoré by potvrdili

[169] DAMAŠKA, Mirjan. Free Proof and Its Detractors. The American Journal of Comparative Law, Vol. 43, No. 3 (Summer, 1995) Str. 354.

[170] Ide dozaista o marenie spravodlivosti (predloženie dôkazu pred súdom, o ktorom predkladateľ vie, že je sfalšovaný alebo pozmenený), ktoré je v niektorých jurisdikciách postihované ako forma rušenia činnosti orgánov verejnej moci priamo v trestnom hmotnom práve. Viď § 344 TZ.

[171] Znalcovi vo všeobecnosti *„neprislúcha hodnotiť dôkazy ani z hľadiska ich vierohodnosti ani v tom smere, či skutočnosť, o ktorej podáva správu, je preukázaná.“* Viď Rozhodnutí NS ČSSR ze dne 8. 7. 1980, sp. zn. Tzv 17/80. [R 33/1981 tr.].

autenticitu a vierohodnosť. Keďže súd nevidel rozpor medzi svojím rozhodnutím a objektívnymi technickými poznatkami, súd nedostatočne pochopil podstatu elektronického dôkazného prostriedku a aj ho nesprávne vyhodnotil.[172]

V oboch problematických dôkazných situáciách chýba súdu technická znalosť. Súd stojí pred otázkou ako porozumieť technológií, na ktorú mu zásada voľného hodnotenia dôkazov nedáva priamu odpoveď. Inak povedané, stavbu súdneho rozhodnutia ponecháva na jeho zručnosti, profesionalite a expertíze.

V problematickej dôkaznej situácii č. 1 ide o riziko, že súd tým, že sa spoľahne len na nepriame dôkazné prostriedky, opomenie vlastnosti elektronického dôkazného prostriedku, ktoré by mohli byť v rozpore s nepriamymi dôkazmi. Všeobecne v civilnom konaní platí, že na základe nepriamych dôkazov je dostačujúce preukázať skutkový stav s veľkou mierou pravdepodobnosti. Nepriame dôkazy nemusia tvoriť úplne uzavretú sústavu, ktorá nepripúšťa iný skutkový záver.[173] Domnievame sa, že aj keď má súd za to, že došlo k falšovaniu a doplneniu elektronickej komunikácie na základe nepriameho dôkazu (napr. existuje iná indícia o falšovaní, svedecká výpoveď), aby dospel k veľkej miere pravdepodobnosti, mal by si túto skutočnosť verifikovať aj na elektronickom dôkaznom prostriedku priamo a položiť si otázku, ako mohlo dôjsť k jeho manipulácii a či je technický stav prostriedku schopný túto skutočnosť potvrdiť, resp. vyvrátiť. Elektronický dôkazný prostriedok je často sám o sebe spôsobilý osvetliť manipuláciu s dátami (napr. metadáta, geolokácia, čas) alebo forenznou analýzou objasniť ich pôvod.

V problematickej dôkaznej situácii č. 2 ide o riziko, že súd tým, že sa spoľahol len na znalecký posudok, vyhodnotil dôkazný prostriedok ako nespoľahlivý. Inak

[172] Tento limit môže byť korigovaný mimoriadným opravným prostriedkom v prípade, ak by došlo k extrémnemu nesúladu medzi skutkovými zisteniami a úvahami pri hodnotení dôkazov na strane jednej a právnymi závermi na strane druhej: „*Ústavní soud často opakuje, že mu nepřísluší přehodnocovat důkazy, provedené obecnými soudy. Může (a musí) tak ale učinit, pokud dospěje k závěru, že došlo k extrémnímu nesouladu mezi skutkovými zjištěními a úvahami při hodnocení důkazů na straně jedné a právními závěry na straně druhé.“* Viď Nález ÚS ČR ze dne 13. 11. 2018, sp. zn. I. ÚS 1491/17-2.

[173] Podľa NS ČR *„pro závěr o prokázání určité skutečnosti v civilním řízení na základě nepřímých důkazů je dostačující, aby předmětný skutkový závěr bylo možné s velkou mírou pravděpodobnosti připustit. Nepřímé důkazy nemusí tvořit zcela uzavřenou soustavu, která nepřipouští jiný skutkový závěr než ten, k němuž soud dospěl, nýbrž dostačuje, jestliže nepřímé důkazy s velkou mírou pravděpodobnosti k tomuto závěru na rozdíl od jiných možných závěrů vedou.“* Viď Usnesení NS ČR ze dne 4. 6. 2008, sp. zn. 28 Cdo 1938/2008.

povedané, rozhodnutie tak urobil expert - znalec a nie súd. Ak by sa súd oprel o svoje základné technické vedomosti a kriticky sa pýtal na úplnosť posudku, t.j. na to, či je možné vyťažiť ďalšie informácie z elektronického dôkazu (napr. identifikátor komunikujúcich), mohol by dospieť k záveru, že dôkazný prostriedok je spoľahlivý.[174]

Civilné poriadky sa snažia v technických otázkach identifikovať hranicu medzi odbornými znalosťami súdu, odbornými znalosťami spôsobilej osoby svedka (expert) a vedeckými poznatkami (znalec).[175] Odborné znalosti sú také znalosti, ktoré *„presahujú širší rámec všeobecnej skúsenosti (sprostredkovane súdu napríklad aj štúdiom) a ku ktorým je potrebná určitá odborná znalosť a skúsenosť.“*[176] Otázkou ostáva, či je súd vždy povinný privolať k dokazovaniu odborníka, a to aj vtedy, ak sám má potrebné odborné znalosti?[177] Podľa českého OSŘ a jeho gramatického výkladu, zákon ukladá súdu volať na pomoc odborníka aj vtedy, ak sám má potrebné odborné znalosti.[178] Podľa slovenského CSP, v prípade odborného vyjadrenia a znaleckého posudku, súd tak činí iba na návrh procesnej strany.[179] Podľa švajčiarskeho ZPO, ak má akýkoľvek svedok odborné znalosti, súd mu môže (ale nemusí) položiť otázky týkajúce sa posúdenia skutkového stavu prípadu.[180] Obdobne si súd môže vyžiadať

[174] Hodnotenie dôkazov a skutkové zistenie nemajúce v podstatnej časti oporu vo vykonanom dokazovaní nemožno dovolacím dôvodom podľa § 241 ods. 3 OSŘ úspešne napadnúť. Viď Rozsudek NS ČR ze dne 10. 6. 2008, sp. zn. 28 Cdo 1813/2008.

[175] § 206 a § 207 CSP, § 175 a § 183 ZPO.

[176] HROMADA, Miroslav. § 127 [Znalecký posudek a odborné vyjádření]. In: SVOBODA, Karel, SMOLÍK, Petr, LEVÝ, Jiří, ŠÍNOVÁ, Renáta. Občanský soudní řád. 2. vydání. Praha: Nakladatelství C. H. Beck, 2017, Str. 545.

[177] Odborné vyjadrenia majú z dôvodu hospodárnosti prednosť pred znaleckými posudkami. Vo všeobecnosti, odborné vyjadrenia nemajú formálne menšiu silu ako znalecké posudky. Ak sú v písomnej podobe, ide o listinný dôkaz. Podľa NS ČR *„odborné vyjádření není znaleckým, ale listinným důkazem, svou povahou se však znaleckému posudku blíží, pročež proti odbornému vyjádření mohou účastníci vznést v podstatě všechny námitky, které by jim příslušely proti znaleckému posudku.“* Viď Rozsudek NS ČR ze dne 4. 9. 2018, sp. zn. 22 Cdo 2711/2018.

[178] Podľa § 127 ods. 1 OSŘ *„Závisí-li rozhodnutí na posouzení skutečností, k nimž je třeba odborných znalostí, vyžádá soud u orgánu veřejné moci odborné vyjádření. Jestliže pro složitost posuzované otázky takový postup není postačující nebo je-li pochybnost o správnosti podaného odborného vyjádření, ustanoví soud znalce. Soud znalce vyslechne; znalci může také uložit, aby posudek vypracoval písemně. Je-li ustanoveno několik znalců, mohou podat společný posudek. Místo výslechu znalce může se soud v odůvodněných případech spokojit s písemným posudkem znalce.“*

[179] § 206 CSP *„Ak je potrebné posudzovať skutočnosti, na ktoré treba odborné znalosti, súd na návrh vyžiada odborné vyjadrenie od odborne spôsobilej osoby.“, §207 CSP „Ak rozhodnutie závisí od posúdenia skutočností, na ktoré treba vedecké poznatky, a pre zložitosť posudzovaných otázok nepostačuje postup podľa § 206, súd na návrh nariadi znalecké dokazovanie a ustanoví znalca.“*

[180] § 175 ZPO *„Ak má svedok osobitnú odbornosť, môže mu súd položiť aj otázky týkajúce sa posúdenia skutkového stavu prípadu.“*

stanovisko od jedného alebo viacerých znalcov. To vykoná na základe návrhu alebo z úradnej moci.[181] Môže sa zdať, že český civilný súd má zviazané ruky v aplikácií svojich odborných vedomostí. Inak povedané, ak závisí jeho rozhodnutie od posúdenia skutočností, na ktoré treba odbornú znalosť, súd sa spolieha na experta. To platí aj pre slovenský alebo švajčiarsky civilný súd, ale zákonodarca im ponecháva istú flexibilitu v otázkach privolania experta. Napriek tomu, je odborné vyjadrenie alebo znalecký posudok len dôkazom ako každý iný. Súd by síce nemal preskúmavať odborné závery, keďže v zmysle zákona mu k tomu chýba odborná znalosť, avšak to neznamená jeho absolútnu viazanosť znaleckým posudkom. Totiž závery posudku môže konfrontovať s ďalšími vykonanými dôkazmi a aj s vlastnými vedeckými a technickými poznatkami, ktoré sú mu známe, a to vo forme svojich otázok k posudku alebo znalcovi.[182]

Sudca po logickej úvahe rozhodne, ktoré dôkazy, prenesene povedané, stavebné materiály pri stavbe svojho rozhodnutia použije, a ktoré dôvodne odmietne. Jeho stavba bude umiestnená na území platného práva po tom ako subsumuje skutkové zistenia pod právne normy. Stavba bude zároveň v krajine, ktorá je determinovaná architektúrou predošlej rozhodovacej činnosti iných súdov (judikatúry). [183] V stavebníctve riziká spojené s technológiou výstavby sú zmiernené právnymi predpismi, normami, ale aj vedomosťami stavebníka o nových stavebných technológiách a o vlastnostiach krajiny. Proces stavby súdnych rozhodnutí pomocou elektronických dôkazných prostriedkov je na tom podobne. Základná vedomosť o procesnom práve dokazovania je nepostačujúca. V tejto metafore sa snažíme zdôrazniť, že ide o pochopenia rizík spojených s elektronickým dôkazným prostriedkom. Sú to technické vedomosti nad rámec poznania platného práva v zmysle klasickej poučky *iura novit curia*. Dovoľujeme si vysloviť, že dnes je každý praktizujúci právnik viac než len obyčajný užívateľ nových technológií. Je jeho imanentnou povinnosťou vzdelávať sa a pochopiť základné technologické riziká, ktoré

[181] § 183 ods. 1 ZPO *„Na žiadosť účastníka konania alebo z úradnej moci môže súd získať stanovisko od jedného alebo viacerých znalcov. Súd musí najskôr vypočuť účastníkov konania.“*

[182] Obdobne rozhodol NS ČR, keď sa vyslovil, že *„skutková zjištění podávající se ze znaleckého posudku, který soud využije z řízení o zbavení způsobilosti fyzické osoby k právním úkonům, nemusí bez dalšího tvořit relevantní skutkový základ pro rozhodnutí o neplatnosti právního úkonu ve smyslu § 38 odst. 2 ObčZ 1964.“* Viď Rozsudek NS ČR ze dne 24. 4. 2013, sp. zn. 30 Cdo 718/2013.

[183] Na tomto mieste je vhodné zdôrazniť význam konštantnej rozhodovacej praxe súdov. Je zrejmé, že jeden mrakodrap v meste ešte Manhattan z neho neurobí, ale každé mesto začína prvou stavbou.

majú vplyv na aplikáciu a vymožiteľnosť práva.[184] Netvrdíme, že expert, odborník alebo znalec je v dokazovaní nadbytočný. Ale aby bol jeho výstup v súlade s platným právom, musí mať k dispozícii všetky informácie súvisiace s elektronickým dôkazným prostriedkom potrebné k jeho činnosti. S tým súvisí aj jeho prístup k ostatným dôkazom a skutočnostiam prípadu dôležitým pre jeho záver. Avšak najdôležitejšie sú inštrukcie a otázky, ktoré má zodpovedať, a ktoré samé o sebe kladú isté technické nároky na pýtajúceho sa (súd alebo strany sporu).

2.6.2. Teória rizika

Slovo *riziko* je používané v mnohých významoch.[185] Súčasná všeobecná teória rizika pracuje s rizikom na základe štatistických a pravdepodobnostných modelov.[186] Finančná teória rizika popisuje modelový rámec, ktorý prispieva k zmierneniu rizika v podobe vyrovnania sa s budúcou neistotou strát alebo ziskov. Snaží sa popísať proces rozhodovania o spôsoboch usporiadania budúcich vzťahov a udalostí tak, aby bolo možné s rizikom prijateľným spôsobom zaobchádzať (kvantifikovať ho), manažovať ho (riadiť ho) alebo popísať ho v kontrolovateľnej forme (kontrolovať ho). Existuje nespočetné množstvo definícií rizík. Najpriliehavejšia definícia pre našu prácu je Lawrencova, ktorá označuje riziko ako *„komplexné meranie pravdepodobnosti a rozsahu nepriaznivého účinku.“* [187] Inak povedané, ide o chápanie zloženého potenciálu viacerých prepletených negatívnych dôsledkov konania alebo udalostí do budúcnosti.[188]

---

[184] Obdobne v kontexte použitia komparatívneho zahraničného práva, Kühn apeluje na to, aby argumentácia tuzemských právnikov získala *„novú medzinárodnú a komparatívnu dimenziu.“* Viď KÜHN, Zdeněk. Iura novit curia: aplikace starého principu v nových podmínkách. Právní rozhledy. 2004, č. 8, Str. 295.

[185] Termín riziko sa dáva do súvislosti s organizáciou poisťovacích spolkov námorníkov v talianskych mestských štátoch na prelome 14. storočia. *„Talianske rischio, španielske riesgo, francúzske risque, nemecké Risiko možno vysledovať až k ranno-talianskemu riscu (čo znamená „útes“) a ku gréckej ριζα (rhíza), čo znamená koreň.“* Viď Etymology of the term risk. [online]. [cit.1.9.2020]. Dostupné z: https://www.risknet.de/en/knowledge/etymology/

[186] BORCH, Karl. The Theory of Risk. Journal of the Royal Statistical Society. Series B. vol. 29, no. 3, 1967, Str. 432–467.

[187] LOWRANCE, W.William. The Nature of Risk. In: Schwing R.C., Albers W.A. (eds) Societal Risk Assessment. General Motors Research Laboratories. 1980. Springer, Boston, MA. Str. 5-17.

[188] Je však potrebné poznamenať, že niekedy môže riziko predstavovať aj priaznivý účinok. V ekonomickom ponímaní to bude možnosť, resp. potencionálna negatívna alebo pozitívna miera odklonu dosiahnutých finančných výsledkov od plánovaných finančných výsledkov a následne identifikácia právnych, ekonomických, hospodárskych a manažérskych dôvodov.

Vo všeobecnosti je riziko možné vnímať ako pravdepodobnosť a rozsah priaznivého alebo nepriaznivého účinku v nadväznosti na predchádzajúce rozhodnutie. Preto pri rozhodovaní hovoríme aj o miere rizika, ktorá sa zvažuje na základe dvoch alebo viacerých alternatív. Rozhodovanie o riziku naráža na obmedzenia, ktorými sú:[189]

- Empirická analýza faktov pred rozhodnutím
    - Ide o otázku vstupov, t.j. či je rozhodujúci schopný zhromaždiť maximum faktov a dôsledne ich vyhodnotiť pre svoje najlepšie možné rozhodnutie. Empirická analýza je vždy limitovaná časom a prostriedkami.[190]

- Merateľnosť hodnoty, resp. dopadu rozhodnutia
    - Ide o najkomplexnejšiu otázku súvisiacu s tým, ako dobre sú fakty zanalyzované rozhodujúcim subjektom a ako sú jednotlivé rozhodnutia konzistentné medzi sebou a zároveň voči celku. Rozhodovanie o finančnom riziku je istotne kvantifikovateľnejšie ako rozhodovanie a právach a povinnostiach strán súdneho sporu.[191] Dopad rozhodnutia však môže byť vyjadrený aj kvalitatívnou formou. Merateľnosť dopadu rozhodnutia do budúcnosti sa dá vykonať na základe jeho pravdepodobnostných účinkov a historickej analýzy podobných rozhodnutí v obdobných veciach.

- Riadenie rizika
    - V manažmente financií ide o kľúčovú zložku. Riadenie je možné vykonávať len vtedy, ak má manažér rizika postačujúcu spätnú väzbu a prehľad o pravdepodobnosti a

[189] Ibid. LOWRANCE, W.William. The Nature of Risk.

[190] Tu je potrebné zdôrazniť úlohu informačných technológií, najmä asistencie v podobe automatizovaného rozhodnutia (viď 4. kapitolu Počítač ako sudca).

[191] V práve tu možno odkázať na „jurimetriku“, disciplínu, ktorá sa zameriava na otázky matematicko-logickej indexácie a použitia štatistických metód v právnej praxi. Ibid. POLČÁK, Radim. Pět tichých minut za Viktorem Knappem.

rozsahu priaznivého alebo nepriaznivého účinku z riadených častí (aktualizovanie informácií o riadených záležitostiach). Pri rozhodovaní o riziku súvisí riadenie rizika s referenciou k štandardom, normám a predošlým rozhodnutiam tak, aby existovali nastavené kontroly v systéme, o ktorom je rozhodované. Ide o to, aby bolo zabránené nechcenému alebo nepredvídateľnému účinku pomocou sústavných úprav týchto kontrol.

2.6.3. Hodnotenie elektronického dôkazu ako analýza rizík

Pre potreby tejto práce sa pokúsime uvažovať o tom, že rozhodovanie o elektronických dôkazných prostriedkoch môže byť videné aj ako rozhodovanie o riziku.[192] Inak povedané, sudca rozhoduje o riziku, ktoré predstavuje použitie dôkazu v elektronickej podobe. Dôkaz totiž môže predstavovať priaznivý alebo nepriaznivý účinok pre hľadanie práva. To bude záležať od toho, ako bude dobre vysvetlený.[193] Dôvody, ktoré vedú k aplikácii teórie rizika pri dokazovaní, sú potenciálna kvantifikácia a hľadanie ľahšej automatizácie rozhodnutí o dôkazoch.[194]

Prirovnanie dôkazu k merateľnému riziku má však aj svojich odporcov (najmä v anglo-americkom systéme práva). Podľa Nessona *„cieľom procesu zisťovania faktov nie je generovať matematicky „pravdepodobné“ verdikty, ale skôr generovať prijateľné verdikty; iba prijateľný verdikt premietne základné právne pravidlo do*

[192] Používanie analýzy rizika v súdnom systéme anglo-amerického práva nie je novinkou, najmä v prípade pochopenia, aké riziko predstavuje sám páchateľ trestného činu pre spoločnosť. Úloha analýzy rizika v anglo-americkom právnom systéme je čoraz dôležitejšia najmä vo všetkých fázach systému trestného súdnictva, vrátane policajnej kontroly, väzby, udeľovania trestov, nápravných opatrení a podmienečného prepustenia. Viď GARRETT, B. L., Monahan, J. Judging Risk. California Law Review. 2020. Roč, 108. č.2. Str. 439–493. [online]. [cit.1.9.2020]. Dostupné z: https://lawcat.berkeley.edu/record/1161691

[193] Princíp nachádzania práva bol opätovne zdôraznený ÚS ČR tak, že *„prvořadým úkolem obecných soudů a smyslem občanského soudního řízení je nalézání hmotného práva a spravedlivé řešení sporů mezi účastníky [srov. nález ÚS ČR sp. zn. IV. ÚS 22/03 ze dne 6. 4. 2004 (N 51/33 SbNU 31), v němž Ústavní soud považoval za nejvyšší hodnotu rozhodování sporů individuální spravedlnost].“* Viď Nález ÚS ČR ze dne 22. 9. 2015, sp. zn. I. ÚS 1944/15.

[194] Automatizácia hodnotenia rizík však znamená aj kvalitnú transparentnosť, neutrálnosť a porozumenie verejnosti dôležitým algoritmom. Bolo preukázané, že používanie historických údajov na učenie systémov AI na hodnotenie justičného rizika nesie so sebou ľudské chyby z minulosti. Viď HAO, Karen. AI is sending people to jail—and getting it wrong. MIT Technology Review. Január 2019. [online]. [cit.1.9.2020]. Dostupné z: https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

spoločnosti a potvrdí normu správania tohto pravidla.“ [195] S týmto tvrdením vo všeobecnosti súhlasíme, avšak v prípade elektronických dôkazných prostriedkov, sme toho názoru, že súd pracuje s predmetom, ktorý musí byť interpretovaný odbornými technologickými vedomosťami. Súd, resp. strany sporu, sa často spoliehajú na experta alebo znalca, ktorému pripisujú dôležitú úlohu, čo vytvára priestor pre predsudok o odbornej rade a následnú chybu v rozhodnutí. Ide aj o psychologický aspekt súdneho rozhodnutia. Zahraničná literatúra ho popisuje ako teóriu výraznosti (*Salience Theory*).[196] Je to jednoduchá myšlienka, že ak je medzi možnosťami jedná krikľavá možnosť, tá pritiahne pozornosť, nastaví rámec rozhodovania a ovplyvní výslednú voľbu. Inak povedané, ak sa dá do pozornosti súdu výrazný dôkaz, napr. znalecký posudok o elektronickom dôkaznom prostriedku, existuje riziko, že to môže ovplyvniť prevažnú časť rozhodnutia a menej nápadné dôkazy sa opomenú alebo budú ponechané bokom.

Sudca nerozhoduje vo vzduchoprázdne. Novovznikajúci smer *behaviorálnej justície* hovorí, že presvedčenie sudcu o spore je formované jeho vzdelaním, politickým názorom, skúsenosťami, ale aj názorom na pozíciu účastníkov sporu, a to aj nad rámec obsahu spisu, t.j. predložených dôkazov. [197] Tento smer sa opiera o výsledky psychológie a najmä o práce Kahnemana a Tverského, ktoré identifikujú celý rad predsudkov (*biases*) založených na intuitívnych (rýchlych) rozhodnutiach.[198] Príkladom je skúmanie averzie alebo chuti procesných strán k riziku. Ide o kontrast medzi preferenciou rizika strán s opačnými motívmi, napr. žalobcu oproti žalovanému v majetkovom spore. Štatistický výskum potvrdil, že preferencie rozhodujúcich

[195] NESSON, Charles. The evidence or the event? on judicial proof and the acceptability of verdicts, Logic, Probab. Presumptions Leg. Reason., vol. 98, no. 7. 2013. Str. 251–286.

[196] BORDALO, P. GENNAIOLI, N. and SHLEIFER, A. Salience theory of judicial decisions, Journal of Legal Studies, Vol. 44, No. S1, Str. S7–S33, 2015, [online]. [cit.1.9.2020]. Dostupné z: https://scholar.harvard.edu/shleifer/publications/salience-theory-judicial-decisions

[197] EPSTEIN, L., LANDES, W., POSNER, R. A Realistic Theory of Judicial Behavior. In The Behavior of Federal Judges. 2013. Cambridge, Massachusetts; London, England: Harvard University Press. Str. 25-64.

[198] TVERSKY, Amos. KAHNEMAN, Daniel. Judgment under Uncertainty: Heuristics and Biases. Science, vol. 185, no. 4157, 1974, Str. 1124–1131.

o riziku závisia od toho, ako sú ich výhody formulované rámcom zisku alebo straty (nie len monetárnej), a to aj keď taký rámec je v danom prípade irelevantný.[199]

Súd je povinný budovať silnú hradbu medzi jeho myšlienkovým postupom o hodnotení dôkazov a externým vplyvom tak, aby si zachoval objektívnosť a nezaujatosť pri svojom rozhodovaní. Ide takmer o nadľudskú požiadavku. Tak ako žalobcovia a žalovaní preferujú určité riziko súvisiace so stratou alebo prehrou sporu, tak aj súd sa môže ocitnúť v nebezpečnom priestore preferencie rizika súvisiaceho s rozhodovaním práve o elektronických dôkazoch. Totiž, ak súd bude rozhodovať o určitom počte dôkazov, z ktorých je jeden alebo viac elektronických, môže takýto dôkaz v podobe listinného prepisu alebo znaleckého posudku vzbudiť dojem, že je pravdivejší ako ostatné dôkazy. Inak povedané, miera rizika nepriaznivého účinku pri použití tohto dôkazu pre rozhodnutie súdu sa zdá nižšia. Plne súhlasíme s tvrdením Deseta, ktorý sa vyjadril k miere objektivity elektronických dôkazov v konkrétnom trestnom konaní úkladnej vraždy novinára a jeho snúbenice, ktorá otriaslo celou slovenskou spoločnosťou: *„Vecné, respektíve listinné dôkazy, akým je aj komunikácia získaná z Threemy, ktoré sa znalecky preskúmajú, vykazujú oveľa vyššiu mieru objektivity a hodnovernosti ako výpovede obžalovaných, ktoré sú, naopak, do značnej miery subjektívne, pretože obžalovaní môžu svojimi výpoveďami sledovať predovšetkým vlastné záujmy s vidinou dosiahnutia čo najpriaznivejšieho verdiktu.“*[200] Áno, prepis komunikácie z mobilného zariadenia, digitálna kópia dokumentu alebo záznam logov slúžia ďaleko lepšie ako pamäť človeka, ktorá je interpretovaná ľudskou rečou vo svedeckej výpovedi. Ale práve preto, že technologickým dôkazom pripisujeme automaticky väčšiu váhu, musíme poznať aj ich riziká. Aby nešlo len o

[199] Toto je možné demonštrovať na Rachlinského psychologickom výskume, ktorý podrobil skupinu študentov práv experimentu. Polovica hrala úlohu žalobcu a polovica úlohu žalovaného. Žalobcovia si mohli zvoliť medzi istou ponukou mimosúdneho narovnania v hodnote 200.000,-$ alebo 50% šancou na výhru 400.000,-$ v súdnom konaní (a zodpovedajúcou 50% šancou na prehru). Žalovaní si mali zvoliť medzi zaplatením mimosúdneho narovnania vo výške 200.000,-$ alebo 50% pravdepodobnosti straty 400.000,-$ pred súdom (so zodpovedajúcou 50% pravdepodobnosťou, že platiť nebudú musieť nič). Z výsledkov ankety vyplynulo, že skupina žalobcov je vo všeobecnosti averznejšia k riziku a uprednostňujú mimosúdnu dohodu (až 77% skupiny). Naopak skupina žalovaných je viac naklonená k riziku (vyhľadáva riziko) a uprednostňuje súdne rozhodnutie. Viď RACHLINSKI, Jeffrey J. Gains, Losses, and the Psychology of Litigation. 1996. Cornell Law Faculty Publications. Paper 795. [online]. [cit.1.9.2020]. Dostupné z: http://scholarship.law.cornell.edu/facpub/795

[200] DESET, Miloš. V prípade Kuciakovej úkladnej vraždy je Threema zákonný dôkaz. Denník N. 23. januára 2020. [online]. [cit. 1.9.2020]. Dostupné z: https://dennikn.sk/1728346/v-pripade-kuciakovej-ukladnej-vrazdy-je-threema-zakonny-dokaz/

všeobecné konštatovanie súdu o vyššej miere objektivity a hodnovernosti v duchu zásady voľného hodnotenia dôkazov, domnievame sa, že je potrebné, aby sa súd vysporiadal aj s ich vlastnosťami a vyhodnotil si riziko, ktoré predstavuje použitie elektronického dôkazu v jednotlivom prípade.

Ako sme už uviedli vyššie, ak súd rozhoduje o dôkaze, ktorý závisí na pochopení technológie, rozhoduje aj o riziku, ktoré má dopad na odôvodnenie rozhodnutia a samotný spor. Riziká je možné rozdeliť do dvoch skupín a popísať ich použitím nasledujúcich otázok (vhodných pre civilné sporové konanie):

- Vnútorné riziko elektronického dôkazného prostriedku
  - Je kópia dôkazného prostriedku dostupná stranám sporu podľa procesných ustanovení toho ktorého štátu?
  - Mali sa strany k vykonaniu dôkazného prostriedku možnosť vyjadriť? Namietala niektorá zo strán tento prostriedok?
  - Je technológia dôkazného prostriedku vysvetliteľná?
  - Je dôkazný prostriedok čitateľný bez ďalšieho a môže byť vykonaný súdom?
  - Je potrebné pristúpiť k odbornému vyjadreniu, resp. znaleckému posudku? Ide o súkromný znalecký posudok alebo posudok zaobstaraný súdom?
  - Je odborné vyjadrenie alebo znalecký posudok založený na pravdepodobnosti alebo štatistickej metóde?
  - Sú položené otázky znalcovi formulované na základe dostupných vedomostí súdu alebo strán o dôkaznom prostriedku a ostatných skutočnostiach prípadu?
  - Hodnotí odborné vyjadrenie alebo znalecký posudok vykonanie dôkazného prostriedku alebo právne otázky, čo by bolo v rozpore so zákonom?
  - Skúmal súd kvalitu dôkazného prostriedku (potencionálnu ubiquitu a volatilitu, dôkaznú spoľahlivosť a integritu, pravdivosť a vierohodnosť)? Existujú iné skutočnosti alebo dôkazy, ktoré spochybňujú dôkaznú spoľahlivosť a integritu tohto dôkazného prostriedku?

- Je dôkazný prostriedok konvertovaný do súdneho spisu tak, aby bol čitateľný pre všetky procesné strany v budúcnosti?

- Vonkajšie riziko elektronického dôkazného prostriedku
  - Ide o jediný dôkazný prostriedok v spore? Nepramenia z tohto prostriedku ďalšie možné prostriedky, ktoré je potrebné vykonať?
  - Bol dôkazný prostriedok získaný z iného súdneho alebo správneho konania?
  - Existuje vyhlásenie o vierohodnosti dôkazného prostriedku nezávislou osobou?
  - Vyhodnotil súd získaný dôkaz jednotlivo?
  - Vyhodnotil súd všetky získané dôkazy v ich vzájomnej súvislosti?
  - Je získaný dôkaz vyhodnotený súdom súčasťou odôvodnenia rozhodnutia?
  - Prihliadol súd na všetko, čo vyšlo počas konania najavo?
  - Existuje možnosť, že by bol dôkazný prostriedok spochybnený novšou technológiou alebo pokrokom v informačných technológiách?

Vyššie uvedené otázky predstavujú počiatočný rámec, resp. postup pre vyhodnotenie rizika elektronického dôkazného prostriedku súdom. Domnievame sa, že v závislostí od odpovedí na vyššie uvedené otázky predstavuje alebo nepredstavuje konkrétny elektronický dôkazný prostriedok riziko pri hľadaní práva v danom spore. Tento rámec je rovnako dôležitý aj pre kontrolu a riadenie rizík spojených s obdobným dôkazným prostriedkom v iných podobných sporoch do budúcna. V jednotlivých otázkach môže analyzovať najčastejšie príčiny a problémy dokazovania elektronickými dôkaznými prostriedkami naprieč rôznymi spormi.

Na záver možno uviesť už len známy Nessonov výrok, že *„ten, kto je absolútne odhodlaný k zisťovaniu a skúšaniu pravdy a kto by sa vyhýbal akémukoľvek ústupku v hľadaní pravdy, môže zistiť po vypracovaní prijateľného rozhodnutia, že to robí na úkor iných dôležitých hodnôt. Môže zistiť, že extrémy v hľadaní pravdy môžu narušiť schopnosť systému vyvodiť prijateľné rozhodnutia, a tým podkopať jeho schopnosť*

premietnuť normy obsiahnuté v hmotnom práve. Nepohodlná myšlienka, že naše hľadanie pravdy nesmie oslabiť našu snahu o prijateľné rozhodnutia, podkopáva našu súčasnú pohodlnú pozíciu, v ktorej by naša snaha o prijateľné rozhodnutia nemala kompromitovať naše hľadanie pravdy.“[201]

2.6.4. Vplyv znaleckého dokazovania na hodnotenie elektronický dôkazov

Domnievame sa, že technologický interpreter alebo prekladač je podstatnou zložkou každého elektronického dokazovania. Práve táto technologická vrstva odlišuje elektronický dôkazný prostriedok od tradičných dôkazných prostriedkov. Vykonávateľ elektronického dôkazného prostriedku musí poznať technológiu, ktorou dokáže vyťažiť dôkaz. Zdá sa, že ide o trivialitu, ale pri nespočetnom množstve technológií, ktoré môžu sprostredkovať dôkaz, nie je vždy ľahké vyhľadávať tie elektronické dôkazné prostriedky, ktoré sú kompatibilné s technickými možnosťami vykonávateľa. Z tohto dôvodu súdy alebo procesné strany pristupujú pomerne často k použitiu odborného vyjadrenia alebo znaleckého skúmania. V oblasti dokazovania zastáva odborná verejnosť názor, že dochádza k nadužívaniu znaleckých posudkov súdmi.[202] Navyše, odborná činnosť by mala smerovať len k zodpovedaniu technických a faktických otázok, nesmie nahrádzať hľadanie práva súdmi.[203] V civilnej procesnej praxi kontinentálneho práva sa vyskytujú najčastejšie dva typy odbornej, resp. znaleckej činnosti v podobe súkromného posudku (navrhnutého stranou sporu) a posudku vyžiadaného súdom. Niektoré civilné poriadky pripisujú súdnemu znaleckému posudku vyššiu dôkaznú silu ako súkromnému z dôvodu objektívnosti a nezávislosti súdom zvoleného znalca (viď nižšie prípad švajčiarskeho ZPO). Táto skutočnosť má vplyv aj na hodnotenie elektronického dôkazného prostriedku, ktorý v

[201] Ibid. NESSON, Charles. The evidence or the event? on judicial proof and the acceptability of verdicts, Logic, Probab.

[202] VUČKA, Ján. Znalecký posudek - dobrý sluha, ale zlý pán. Jiné Právo. [online]. [cit.1.9.2020]. Dostupné z: https://jinepravo.blogspot.com/2011/09/znalecky-posudek-dobry-sluha-ale-zly.html

[203] Postavenie odborníkov a znalcov je upravené v civilných poriadkoch a podrobnosti, najmä ohľadom znaleckého posudku, sú ponechané na samostatný predpis. Viď § 127 OSŘ, § 206 a § 207 CSP, § 175 a § 183an ZOP, Zákon č. 36/1967 Sb. o znalcích a tlumočnících (nový zákon č. 254/2019 Sb. o znalcích, znaleckých kancelářích a znaleckých ústavech s účinnosťou od 1. januára 2021 a nový zákon č. 255/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o znalcích, znaleckých kancelářích a znaleckých ústavech a zákona o soudních tlumočnících a soudních překladatelích), Zákon č. 382/2004 Z.z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.

súčasnosti vo väčšine prípadov prichádza do konania vo forme znaleckého posudku, listiny, odborného vyjadrenia alebo výsluch znalca.

Ak sa pozrieme na český občiansky súdny poriadok, ten predpisuje odborné vyjadrenie v prípade, ak posudzovaná otázka závisí od posúdenia skutočností, na ktoré je potrebná odborná znalosť. Odborné vyjadrenie si súd spravidla vyžiada od orgánu verejnej moci. Ak pre zložitosť posudzovanej otázky takýto postup nie je postačujúci alebo ak je pochybnosť o správnosti podaného odborného vyjadrenia, musí súd ustanoviť znalca (znalecký posudok vyžiadaný súdom). Súd znalca vypočuje a môže mu uložiť, aby posudok vypracoval písomne (znalecký posudok). Ak je ustanovených niekoľko znalcov, môžu podať spoločný posudok. Namiesto výsluchu znalca sa môže súd v odôvodnených prípadoch uspokojiť s písomným posudkom znalca.[204] V zmysle platného znenia § 127a OSŘ pripúšťa zákon súkromný znalecký posudok.[205] Musí mať všetky zákonom požadované náležitosti na znalecký posudok vyžiadaný súdom a obsahovať doložku znalca o tom, že si je vedomý následkov vedome nepravdivého znaleckého posudku. V tomto prípade postupuje súd rovnako, ako by išlo o znalecký posudok vyžiadaný súdom. So súkromným znalecký posudkom súvisí právo znalca nahliadnuť do spisu alebo sa inak oboznámiť s informáciami potrebnými pre vypracovanie znaleckého posudku. Vecný zámer nového CŘS navrhuje vypustiť koncepciu súkromného znaleckého posudku. Opiera sa o súčasnú kritiku znaleckého konania z dôvodu zaplavenia súdov súkromnými protichodnými znaleckými posudkami, predražovania a predlžovania súdneho konania. Vyzdvihuje otázku nezávislosti znalca. Vysvetľuje, že *„oprávnenie strán predložiť expertízu, s ktorou sa bude nakladať ako so súdnym znaleckým posudkom, neprináša pre civilné riadenie súdne nič pozitívne, naopak pojmovo sú o objektivite takého posudku pochybnosti,*

[204] § 127 OSŘ.

[205] Zákonom č. 218/2011 Sb. bol novelizovaný § 127a OSŘ s účinnosťou od 1. 9. 2011, ktorý súdu umožnil posudzovať znalecký posudok predložený účastníkom rovnako, ako by išlo o ním vyžiadaný znalecký posudok. Podľa NS ČR *„účelem novelizace ustanovení § 127 o. s. ř. a začlenění ustanovení § 127a o. s. ř. bylo urychlit řízení a umožnit účastníkům předložit znalecký posudek, na nějž se hledí - obsahuje-li všechny zákonem požadované náležitosti a doložku znalce o tom, že si je vědom následků vědomě nepravdivého znaleckého posudku - jako na posudek vyžádaný soudem. Tím se změnila důkazní hodnota znaleckého posudku předloženého účastníkem, který při dodržení všech obsahových náležitostí stanovených v § 127a o. s. ř. není důkazem listinným, ale má důkazní sílu znaleckého posudku, a proto se stala dosavadní judikatura v tomto směru nepoužitelnou.“* Viď Rozsudek NS ČR ze dne 22. 1. 2014, sp. zn. 26 Cdo 3928/2013.

pretože strana, ktorá tento posudok (pre ňu priaznivý) predkladá, formulovala úlohu znalca a platila ho.“[206]

Slovenský občiansky poriadok robí taktiež rozdiel medzi odborným vyjadrením a znaleckým dokazovaním. Ak súd posudzuje skutočnosti, na ktoré treba odborné znalosti, na návrh vyžiada odborné vyjadrenie od odborne spôsobilej osoby.[207] Ak odborné vyjadrenie nepostačuje a súd posudzuje skutočnosti, na ktoré potrebuje vedecké poznatky, opäť na návrh nariadi znalecké dokazovanie a ustanoví znalca.[208] Znalecký posudok sa vyhotovuje písomne, ak súd nerozhodne inak.[209] Zákon myslí taktiež na súkromný znalecký posudok. Musí byť predložený spolu so žalobou. Má mať všetky zákonom predpísané náležitosti a obsahuje doložku o tom, že znalec si je vedomý následkov vedome nepravdivého znaleckého posudku. Súd k nemu pristupuje ako keby išlo o znalecký posudok súdom ustanoveného znalca. [210]

Švajčiarsky civilný poriadok nerozlišuje priamo tieto dva druhy znaleckého posudku (súkromný a súdny). Švajčiarsky federálny najvyšší súd uviedol, že súkromný znalecký posudok predložený účastníkom konania nemá procesnú hodnotu súdneho znaleckého posudku a nemá dôkaznú hodnotu v zmysle ZPO. Postavil súkromné znalecké posudky na úroveň tvrdenia tretej strany (svedeckej výpovede). Svoje rozhodnutie oprel o to, že tu chýba potrebná objektívna nezávislosť takéhoto znalca. Podľa názoru súdu *„dôkaznú hodnotu ponúkajú len tie znalecké posudky, ktoré sú objednané štátnymi orgánmi a vydané v procesných konaniach.“*[211]

---

[206] Viď § 227 Vecný zámer CŘS, obdobne Vláda ČR na svojom rokovaní dňa 17. 1. 2018 schválila návrh nových zákonov o znalcoch a o tlmočníkoch, ako aj súvisiaceho vykonávacieho zákona, ktorý mal pozmeniť § 127a OSŘ a naviazať súkromný znalecký posudok na súhlas všetkých účastnikov konania *(„Jestliže znalecký posudek předložený účastníkem řízení má všechny zákonem požadované náležitosti a obsahuje doložku znalce o tom, že si je vědom následků vědomě nepravdivého znaleckého posudku, a pokud s tím všichni účastníci řízení souhlasí, postupuje se při provádění tohoto důkazu stejně, jako by se jednalo o znalecký posudek vyžádaný soudem.“*). Tento návrh bol zrušený. Viď Sněmovní tisk 74. Vl.n.z.o změně zák.v souv.s přij. z. o znalcích a soud.tlum. - EU [online]. [cit.1.9.2020]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=8&t=74&snzp=1

[207] § 206 CSP.

[208] § 207 ods. 1 CSP.

[209] § 208 ods. 1 CSP.

[210] § 209 ods. 2 CSP.

[211] BGer 4A_9/2018, 31. Oktober 2018. [online]. [cit.1.9.2020]. Dostupné z: https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F31-10-2018-4A_9-2018&lang=de&type=show_document&zoom=YES&

Domnievame sa, že ak v prípade elektronických dôkazných prostriedkov nastanú rozpory medzi dvoma alebo viacerými znaleckými posudkami rôznych znalcov (či už súkromných alebo ustanovených súdom), súd by ich mal svojou úvahou vždy odstrániť. Ak sa súd bude držať zásady voľného hodnotenia dôkazov a zváži riziká jednotlivých elektronických dôkazných prostriedkov pomocou konfrontácie znalcov a doplňujúcimi otázkami, môže dospieť k záveru, ktorý vykonaný dôkaz je menej rizikový pre hľadanie práva. A ak to súd uváži za potrebné, vo výnimočných a obzvlášť ťažkých prípadoch, môže ustanoviť na preskúmanie posudku podaného znalcom štátny orgán, vedecký ústav, vysokú školu alebo inštitúciu špecializovanú na znaleckú činnosť.[212] Znalec má najmä povinnosť podať správny a nestranný znalecký posudok. Sme toho názoru, že nemožno akceptovať názor, že znalec s pravdou v konaní pred súdom môže byť len jeden, a to ten ustanovený súdom.[213] Existujú však aj opačné názory. Zdôrazňujú, že zákonná regulácia súkromných dôkazných posudkov je na úkor finančne slabšiemu účastníkovi konania a môže byť v rozpore s princípom procesnej spravodlivosti. [214] Teoretický spor o súdnom alebo súkromnom znalcovi nerieši základný problém, a to ako je súd pripravený vyhodnotiť elektronický dôkazný prostriedok a či má na to vhodné inštrumentárium (napríklad hodnotenie rizík elektronického dôkazného prostriedku – viď predošlú podkapitolu). Navyše zastiera potrebnejšiu diskusiu o kvalitatívnych rozdieloch v jednotlivých znaleckých posudkoch, ich metodike a rozsahu.[215]

2.7. Elektronický súdny spis

2.7.1. Konverzia elektronického dôkazného prostriedku

Podľa amerického právneho filozofa Jamesa Boyda White predstavuje *„napätie medzi faktami a právom (príbehom a teóriou)“* ústrednú charakteristiku právnického

[212] § 127 ods. 3 OSŘ, § 207 ods. 3 CSP.

[213] Obdobne viď GRYGAR, Jiří. Ustanovení § 127a o. s. ř. a jeho další legislativní směřování. Bulletin-advokacie.cz. 24.04.2018. [online]. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/ustanoveni-127a-o.-s.-r.-a-jeho-dalsi-legislativni-smerovani?browser=mobi

[214] ZIMA, Petr. Limity použití § 127a OSŘ. Právní rozhledy. 2015, č. 10, Str. 373-374.

[215] KRABEC, Tomáš. Limity použití § 127a OSŘ z pohledu soudního znalce. Právní rozhledy. 2015, č. 15-16, Str. 554-557.

života.[216] Totiž otázky zisťovania faktov zásadne ovplyvňujú rozhodovacie procesy, ktorým predchádza hodnotenie dôkazov. Na to, aby bol elektronický dôkazný prostriedok riadne vykonaný a stal sa súčasťou súdneho spisu v predmetnom konaní, je nutné počítať s jeho konverziou do zmyslami vnímateľnej podoby. Inak povedané, ukladá sa, resp. zaznamenáva sa do takej podoby, ktorá garantuje jeho porozumenie stranám konania.[217] So samotnou konverziou elektronického dôkazného prostriedku preto úzko súvisí elektronický spis a jeho kvalita (napr. dôkazná spoľahlivosť).

Najčastejšie sa je v súdnej praxi možné stretnúť s konverziou elektronického dôkazného prostriedku vo forme výtlačkov e-mailov, printscreenov počítačových obrazoviek, logov alebo sociálnych profilov. Táto konverzia môže byť vykonaná v rámci vypracovania znaleckého posudku alebo svojpomocne jednou z procesných strán súdneho konania. Tu je však potrebné zdôrazniť, že konverzia elektronických dát do analógovej podoby má svoje limity.[218] Napríklad v prípade audiovizuálnych záznamov je možné navrhnúť dôkaz predložením samotného fyzického nosiča (dátového alebo analógového, napr. hard disk, CD, DVD atď.) a nechať vypracovať písomný posudok o jeho obsahu. Je nutné podotknúť, že konverziou sa môže vynechať množstvo súvisiacich informácií o vykonávanom dôkaze, často označovaných ako metadáta.[219] Z technického hľadiska ide o súbor informácií, ktoré vypovedajú o vzniku, zmene alebo o spôsobe nakladania s predmetným dôkazom a taktiež o iných okolnostiach, a to len v prípade, ak je možné predpokladať ich neporušenosť a pôvodnosť. Avšak vynára sa otázka, či bude konverzia elektronických dôkazných prostriedkov nevyhnutná aj v prípade, ak v konaní bude používaný plnohodnotný elektronický spis?

Benefity elektronického spisu je možné demonštrovať na už existujúcich alternatívnych rozhodovacích inštitúciách a procesoch. Príkladom môže byť dopad

[216] Martin Škop používa tento citát v úvode svojho príspevku o základnej metodológií dokazovania v práve. Viď ŠKOP, Martin. Základní metodologie dokazovaní v právu. In: Dokazovanie v civilnom a trestnom konaní. Pezinok: Justičná akadémia Slovenskej republiky, 2012. ISBN 9788097020743. Str. 13.

[217] Viď § 72 ods. 2 OSŘ, podľa ktorého „žalobce je povinen k návrhu připojit písemné důkazy, jichž se dovolává, a to v listinné nebo v elektronické podobě."

[218] Napr. pri 10 GB textu by bolo potrebné vytlačiť cca. 1 310 720 normostrán A4.

[219] Metadáta sú dáta o dátach. Ide väčsinou o štrukturované a vopred definované dáta obsahujúce informácie o primárnych dátach (napr. čas vytvorenia dokumentu, autor dokumentu, počet tlačení atď.).

aspektov virtualizácie procesu autoritatívnej aplikácie práva v podobe systému riešenia on-line sporov z oblasti práva duševného vlastníctva. Rozhodcovské centrum pre spory o domény CZ (Rozhodčí soud při Hospodářské komoře České republiky a Agrární komoře České republiky) ku dnešnému dňu od svojho štartu v roku 2020 eviduje vyše 600 konaní.[220] Táto neveľká štatistika vzhľadom na počet registrovaných doménových mien v Českej republike[221] preukazuje vhodne zvolenú cestu riešenia doménových sporov.[222] Už samotná publikácia a dostupnosť uvedených nálezov na webstránke rozhodovacej autority predstavuje efektný systém korigovania doménových vzťahov. Čo je dôležitejšie, on-line platforma pre obsluhu a vedenie elektronického spisu doménového sporu priniesla zvýšenie informovanosti a posun chápania doménových vzťahov v kontexte priamej aplikácie pravidiel alternatívneho riešenia sporov.[223]

Ako už bolo uvedené vyššie, elektronický spis predstavuje základný pilier virtualizovaného procesu autoritatívnej aplikácie práva a zároveň možné riešenie pre správne vykonanie elektronického dôkazného prostriedku. Jeho technológia je v súčasnosti uchopiteľná v civilnom procese v súlade s § 40 OSŘ a trestnom konaní v súlade s § 59 ods. 1 TŘ. Podľa Polčáka predstavuje elektronický spis *„elektronickú obdobu dosiek, do ktorých sú postupne vkladané jednotlivé dokumenty.“*[224] Podľa Stupku, je elektronický spis *„centrálním momentem autoritativní aplikace práva, jeho elektronická podoba pak obsahuje všechny dokumenty, které by měly být součástí spisu klasického, proto musí být jeho technická realizace dostatečně univerzální.“*[225]

[220] Rozhodčí centrum pro spory o domény .CZ: Rozhodčí soud při HK ČR a AK ČR. [online]. [cit.1.9.2020]. Dostupné z: http://domeny.soud.cz/adr/decisions/index.php

[221] V roku 2020 eviduje CZ.NIC, z. s. p. o. registrovaných viac ako 1 300 000 doménových mien. Viď CZ.NIC, z. s. p. o. Domain Report 2020 [online]. [cit.1.9.2020]. Dostupné z: https://stats.nic.cz

[222] Je treba poznamenať, že NS ČR rozsudkom sp. zn. 23 Cdo 3895/2011 rozhodol, že nie je možné uzavretie rozhodcovskej zmluvy na základe verejnej rozhodcovskej ponuky obsiahnutej v Pravidlách registrácie doménových mien v ccTLD .cz, vydaných združením CZ.NIC, z.s.p.o. *„Obě strany sporu, resp. budoucího sporu, musí v rozhodčí smlouvě vyjádřit souhlas s konáním rozhodčího řízení. Veřejné prohlášení, které držitel doménového jména činí ve smlouvě uzavírané s registrátorem vůči neurčitému okruhu třetích osob, že bude případné vzniklé spory řešit v rozhodčím řízení, není vyjádřením adresné vůle řešit vzniklé spory v rozhodčím řízení.“* Viď Rozsudek NS ČR ze dne 17.12.2013 , sp. zn. 23 Cdo 3895/2011.

[223] BARTOŠKOVÁ, Tereza. Doménové spory před Rozhodčím soudem při Hospodářské komoře České republiky a Agrární komoře České republiky, Odborný seminář: Doménová jména a právo - novinky z České republiky i zahraničí. CZ.NIC, z. s. p. o. [online]. [cit.1.9.2020] Dostupné z: http://www.nic.cz/seminar/

[224] Ibid. POLČÁK, Radim. Internet a proměny práva. Str. 250.

[225] STUPKA, Václav. eJustice. Revue pro právo a technologie. 2011, č. 2, St. 76-97.

Samozrejme, s týmto tvrdením sa nedá nesúhlasiť, procesný inštitút súdneho spisu vo svojej podstate ostáva nemenný. Avšak za dodržania podmienok technologickej neutrality, elektronický spis má potenciál priniesť mimoriadne zaujímavú platformu na riadne vykonávanie elektronických dôkazov, ktorá môže čiastočne *nabúrať a prestavať* už zažité partikularity procesného práva dôkazných prostriedkov, a to bez ohľadu na typ toho ktorého právneho odboru. Úspech každého konania je totiž závislý na procesnom zvládnutí všetkých etáp, vrátane vykonávania dôkazov. Elektronický spis je najvýznamnejším elementom *eJustice*. Prispieva k efektívnosti, rýchlosti, dostupnosti a interoperabilite celej justície.[226] Preto je možné zhrnúť, že virtualizácia súdneho spisu predstavuje možnú budúcu konštrukciu ochrany základných práv a povinností súdnych strán pri dokazovaní. V neposlednom rade taktiež napomáha zachovaniu elementárnej podstaty inštitútu dokazovania vo svete moderných technológií.

2.7.2. Súdny spis v Českej a Slovenskej republike, komparatívny pohľad

Elektronický spis predstavuje základný pilier virtualizovaného procesu autoritatívnej aplikácie práva. Jeho technológia je v súčasnosti uchopiteľná a spis je potrebné vnímať ako základňu justičnej agendy. Procesné práva a povinností sa realizujú prevažne v civilnom sporovom konaní prostredníctvom procesných úkonov. Tieto procesné úkony vykonávajú subjekty konania, predovšetkým súd a procesné strany.[227] Celý priebeh konania, resp. obsah všetkých procesných úkonov musí byť zachytený alebo zaznamenaný. Na uloženie takýchto záznamov slúži centrálny bod – súdny spis.

V súčasnej dobe pripúšťa český OSŘ priamo viaceré formy zachytenia priebehu konania: zvukový záznam, zvukovo-obrazový záznam a písomný záznam (spísanie protokolu).[228] O výbere vhodnej metódy rozhoduje sudca, nakoľko je determinovaný technickými a personálnymi podmienkami. Právny základ existencie súdneho spisu je možné nájsť v civilných súdnych poriadkoch, kancelárskych poriadkoch jednotlivých súdov alebo v iných vykonávacích predpisoch. V českom OSŘ to je najmä § 40b ods.1, ktorý hovorí, že *„o každém sporu nebo jiné právní věci se vede spis v listinné nebo*

[226] Ibid. STUPKA, Václav. eJustice.

[227] Ibid. WINTEROVÁ, Alena a kol. Civilní právo procesní. Str. 174.

[228] § 40 an. OSŘ.

v elektronické podobě.“ Ustanovenie § 40 ods. 1 OSŘ hovorí, že *„ukony, při nichž soud jedná s účastníky, provádí dokazování nebo vyhlašuje rozhodnutí, se zaznamenávají ve formě zvukového nebo zvukově obrazového záznamu (dále jen „záznam“). Záznam se uchovává na trvalém nosiči dat, který je součástí spisu.“* Ako je zrejmé, súčasný stav v Českej republike počíta s hybridným vedením spisu, t.j. v listinnej a elektronickej forme.

Na Slovensku je tento stav o niečo zložitejší. Žiaľ, opäť sa nejde do dôsledkov a elektronizácia je riešená len v závislosti od vývoja inej právnej úpravy a od možnosti materiálno-technického zabezpečenia súdov. Ustanovenie § 98 ods. 1 CSP hovorí, že „*o procesných úkonoch, pri ktorých súd koná so stranou alebo vykonáva dokazovanie, sa vyhotovuje záznam technickým zariadením určeným na zaznamenávanie zvuku. Takto vyhotovený záznam sa uchová na nosiči dát, ktorý sa po skončení pojednávania pripojí k súdnemu spisu alebo sa v súdnom spise urobí poznámka, kde je záznam uložený.“* Je potrebné kriticky poznamenať, že takéto riešenie (priloženého dátového nosiča) v žiadnom prípade nepredstavuje plnohodnotný elektronický spis. Ide len o nadstavbu súčasného stavu, kedy sa do „papierovej košieľky“ okrem znaleckých posudkoch na CD budú vkladať aj „tie oficiálne zápisnice na CD.“ Podobná prax vládne v trestnom konaní na slovenskom Špecializovanom súde. Súčasťou elektronického spisu by mala byť aj možnosť tvorby dokumentov pomocou šablón.[229] Avšak je to škoda, pretože § 96 CSP pod názvom *„Súdny spis a súdny register“* ambiciózne otvoril možnosť zakotvenia elektronického spisu do textu zákona. Namiesto toho sa nešťastne v druhom odseku konštatuje, že *„všetky písomnosti, ktoré sa vzťahujú na to isté konanie, tvoria súdny spis.“* Inak povedané, počíta sa len so spisom ako písomnosťou. Podrobnosti o vedení súdneho spisu a súdnych registrov ustanovuje všeobecne záväzný právny predpis, ktorý vydá Ministerstvo spravodlivosti SR a to v zmysle §466 CSP, čo umožnilo súdom viesť elektronický súdny spis v niektorých agendách.[230]

[229] FINDEJS, Stanislav. K otázce elektronického spisu. Právní Prostor. Publikované 14.05.2018. [online]. [cit.1.9.2020]. Dostupné z: https://www.pravniprostor.cz/nazory/glosa-stanislava-findejse/k-otazce-elektronickeho-spisu

[230] V zmysle §148 ods.4 vyhlášky č. 543/2005 Z. Ministerstva spravodlivosti Slovenskej republiky o spravovacom a kancelárskom poriadku pre okresne súdy, krajské súdy, Špeciálny súd a vojenské súdy. Avšak vyhláška nedefinuje samotný elektronický súdny spis.

2.7.3. Elektronický spis

Čo je to vlastne elektronický spis? Čím sa líši od bežne dostupného – papierového? Vo vyhláške Ministerstva spravodlivosti ČR o pojednávacom poriadku pre okresné a krajské súdy je v § 26a uvedené, že *„elektronický spis je možné vést pouze v informačním systému speciálně k tomu určenému.“* [231] Práve tento znak je pre elektronický súdny spis charakteristický. Ide o svojbytný a samostatný informačný systém. Z pohľadu technológie ide o zabezpečený manažment dokumentov a mediálnych súborov s vopred definovanou prístupovou politikou a odolnosťou voči akejkoľvek volatilite. Takýto systém nemá slúžiť len sudcom alebo súdnym úradníkom. Jeho úlohou je sprostredkovať kvalitnejšiu službu justície voči klientom – účastníkom súdnych sporov. Plnohodnotný elektronický spis sa stáva opodstatneným v momente, ak každý z účastníkov môže využívať svoje oprávnenia na nakladanie s obsahom spisu (tzv. diaľkový prístup). V súčasnosti sa napr. podania v listinnej podobe zakladajú do listinného spisu a ak sa vedie vo veci spis v elektronickej podobe, súd prevedie podania a iné písomnosti doručené v listinnej podobe do elektronickej podoby.[232] Čiže právna úprava stále pozná duálny režim vedenia spisovej agendy. Je však potrebné pripomenúť, že tá elektronická je v niektorých prípadoch preferovaná. Tento prevládajúci princíp je možné demonštrovať na rozhodnutí NSS ČR, ktoré sa týkalo verejného práva, resp. správy agendy exekútorov.[233]

V sporovom konaní je najciteľnejší posun vo veciach elektronického platobného rozkazu.[234] Ide o agendy, ktoré majú väčšinou plný elektronický životný cyklus, elektronický spis sa vedie od začiatku až do konca. Písomná agenda neexistuje alebo

---

[231] Vyhláška č. 37/1992 Sb., ministerstva spravedlnosti České republiky o jednacím řádu pro okresní a krajské soudy.

[232] Viď § 25 ods. 2 vyhlášky č. 37/1992 Sb.

[233] Podľa súdu *„exekutor nepochybně má na výběr, zda bude vést elektronický spis nebo spis v listinné podobě [§ 46 odst. 2 in fine zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád)], v každém případě však musí kterýkoli ze způsobů vedení spisu splňovat veškeré požadavky kladené na vedení spisu exekučním řádem, resp. kancelářským řádem a ostatními právními předpisy upravujícími vedení spisové služby (zákonem č. 499/2004 Sb., o archivnictví a spisové službě, včetně prováděcích předpisů k němu). Pokud vede soudní exekutor spis pouze v elektronické podobě, musí vždy veškeré písemnosti doručené mu v listinné podobě převést do elektronické podoby. Nenaplňuje-li soudní exekutor podmínky, které pro vedení elektronického spisu předpisy vyžadují (nezměnitelnost dokumentů ve formátu pdf), je povinen dokumenty, které vede ve své evidenci elektronicky, vytisknout a zařadit do spisu v listinné podobě tak, aby spis obsahoval v chronologické posloupnosti veškeré písemnosti s požadovanými náležitostmi a byl úplný.“* Rozhodnutí NSS ČR ze dne 19. 9. 2011, č. j. 15 Kse 4/2011-62.

[234] Viď § 174a OSŘ.

je len v podobe zberných spisov na príslušných súdoch. Navyše, tento systém využíva hybridnú poštu.[235] Systém sa datuje do roku 2011 a v súčasnosti je využívaný na mnohých okresných, krajských a vrchných súdoch.[236] ÚS ČR nedávno zaviedol aplikáciu *NaSpis* určenú advokátom pre nazeranie do elektronického spisu cez internet.[237] Výsledkom takejto informatizácie je, že všetky dokumenty, ktoré vznikajú v rámci tejto agendy na príslušných súdoch, majú výlučne elektronickú podobu, čo má priamy dopad na materiálne zabezpečenie a výdavky súdov. Lukeš v rámci agendy elektronického spisu uvádza, že hlavnými komplikáciami sú *„nedostatky hybridnej pošty (na strane Českе pošty), neexistencia jednotných vzorových šablón úkonov na každom súde, otázky vyznačovania právnej moci na dokumentoch, vymieňanie si originálov medzi súdmi a ojedinelosť existencie elektronického spisu medzi ďalšími súdnymi agendami.“*[238]

Čo sa týka slovenského elektronického súdneho spisu, ten bol zavedený v obmedzenej podobe (súčasťou balíku Elektronických služieb súdnictva). Systém umožňuje:

- podanie žiadosti o sprístupnenie obsahu súdneho spisu;
- sprístupnenie obsahu elektronického súdneho spisu, informácií o konaní a archívu nahrávok pojednávaní;
- vyhľadanie a prezeranie záznamov v spise;
- zápis dokumentu do spisu; a
- informovanie o udalostiach v súdnom konaní a zmenách v spise.

Cieľom modulu elektronický súdny spis je *„zabezpečiť najmä vstup elektronických dokumentov z rôznych zdrojov pre zabezpečenie maximálnej efektivity*

[235] Súdy elektronicky doručia podanie do Českej pošty, ktorá ho vytlačí a osobne doručí. Súdu sa vracia len elektronická správa o prevzatí zásielky. Viď Česká pošta. PostServis. Co je to hybridní pošta? [online]. [cit. 1.9.2020]. Dostupné z: http://www.ceskaposta.cz/sluzby/tisk-a-kompletace-zasilek/postservis#1

[236] LUKEŠ, Ján. Elektronický spis v agendě elektronického platebního rozkazu. Systém CEPR po roce provozu. [online]. [cit. 1.9.2020]. Dostupné z: http://www.isss.cz/archiv/2013/download/prezentace/msp_lukes.pdf

[237] Do spisů Ústavního soudu přistupuje elektronicky přes internet 222 advokátů. Česká justice. Media Network s.r.o. [online]. [cit. 1.9.2020]. Dostupné z: https://www.ceska-justice.cz/2019/03/do-spisu-ustavniho-soudu-pristupuje-elektronicky-pres-internet-222-advokatu/

[238] Ibid. LUKEŠ, Ján.

pri zavádzaní plne elektronickej práce so súdnym spisom a manažment elektronických dokumentov počas ich bežného životného cyklu. Rovnako sa snaží o poskytovanie elektronických dokumentov pre ostatné systémy pri zachovaní vysokého stupňa bezpečnosti.“[239] Pod elektronizáciu slovenského súdnictva je možné zahrnúť okrem elektronického spisu aj rýchle elektronické doručovanie písomností zo súdu, nahrávanie pojednávaní a prepis hovoreného slova.

Bude zaujímavé sledovať, ako sa podarí Slovensku, ale aj Českej republike dohnať „rozbehnutý vlak“, ktorý už odštartoval v iných členských štátoch EÚ. Obe krajiny majú s inštitútom elektronického spisu pomerne vysoké ambície. Okrem možnosti účastníka uplatniť si svoje právo nazerania do súdneho spisu, elektronizácia má priniesť širokú paletu výhod. Cieľom oboch projektov je vytvorenie komplexného informačného systému justície. Ako už bolo uvedené, tento informačný systém by mal priniesť lepšiu správu civilnej agendy tak, aby bolo umožnené vedenie spisu počas celého jeho životného cyklu v plne elektronickej forme, čo umožní kvalitnejší prístup zúčastneným. Projekty počítajú s využitím elektronického podpisu vo všetkých vrstvách.[240] Je možné konštatovať, že sa očakáva zníženie súdnych prieťahov a nárast produktivity práce súdov prostredníctvom vhodne zvolenej informatizácie.[241]

Avšak jeden z najzaujímavejších momentov je práve možnosť využívať súdny spis aj v otázkach elektronického dokazovania. Virtualizácia súdneho spisu predstavuje stabilnú konštrukciu ochrany týchto základných povinností a napomáha pri zachovaní elementárnej podstaty tohto inštitútu zvyšovať dynamiku prístupu k informáciám pre zúčastnených.

2.7.4. Alternatívne riešenia súdnych sporov a ich technologický pokrok

V predošlej sub-kapitole bol popísaný súčasný stav zavádzania elektronického spisu v Českej a Slovenskej republike. Je potrebné uviesť, že s podobnými problémami

[239] Ministerstvo spravodlivosti SR. Elektronický súdny spis. [online]. [cit.1.9.2020]. Dostupné z: http://www.justice.gov.sk/Stranky/Nase-sluzby/Nase-projekty/Elektronicky%20sudny%20spis/Elektronicky-sudny-spis.aspx

[240] Je potrebné poukázať na nariadenie eIDAS. Podľa čl.3 sa *„elektronickým dokumentom“* rozumie akýkoľvek obsah uložený v elektronickej forme, najmä text alebo zvukový, obrazový či audiovizuálny záznam. Dôležitý je čl.46, ktorý hovorí, že právny účinok elektronického dokumentu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z dôvodu, že má elektronickú formu. Toto nariadenie má množstvo ďalších dosahov na oblasť elektronického dokazovania.

[241] Ministerstvo spravodlivosti SR. Správa o základných otázkach justície. [online]. [cit.1.9.2020]. Dostupné z: http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=374610.

zápasia aj ostatné európske štáty. Podľa záverov Rady Európy sa elektronický spis stáva regulárnou súčasťou súdov. Avšak je nejasné, čo všetko spadá pod pojem elektronický spis. Súdy si uvedomujú, že elektronický spis nie je len otázkou moderného prístupu, ale reálne predstavuje nástroj, ktorý stráži práva a povinnosti zainteresovaných strán, či už ide o lehoty alebo výšku súdnych poplatkov.

Ďalším pozitívnym príkladom môže byť dopad aspektov virtualizácie procesu autoritatívnej aplikácie práva v podobe systému riešenia on-line sporov, akými môžu byť práve spory o doménové mená. Tieto konania sú vo väčšine prípadov spojené s dobre nastaveným informačným systémom elektronických spisov. Príkladom je inštitúcia využívajúca elektronický spis s názvom National Arbitration Forum so sídlom v USA. Ide o jedno z piatich autorizovaných centier organizáciou ICANN, určených pre alternatívne riešenie doménových sporov (ADR).[242] Toto centrum okrem doménových sporov rozhoduje aj rôzne rozhodcovské, arbitrážne a mediačné prípady. Ročne spracuje vyše 200.000 prípadov a od roku 1999 rozhodovalo vyše 10.000 prípadov týkajúcich sa výlučne doménových mien.[243] Je to druhé najväčšie centrum po arbitrážnom súde spravovanom Svetovou organizáciou duševného vlastníctva.[244] Centrum v súčasnosti poskytuje na základe *soft-law* vypracovaného združením ICANN a zmluvného rámca s vrcholovými registrátormi doménových mien, jednoduchý a prehľadný informačný on-line systém od podania návrhu, jeho rozhodnutia až po jeho vykonanie. Celá komunikácia prebieha elektronicky, len ojedinele je prípustná písomná korešpondencia. Pozitívnym príkladom je to, že systém kladie dôraz na neformálnosť a užívateľskú spokojnosť, a to za dodržania bezpečnostných opatrení, ktoré chránia systém pred neautorizovaným zneužitím.

Na základe praktických príkladov je možné uviesť, že technologické zmeny v spôsobe vedenia spisu prispeli k lepšej procesnej vymožiteľnosti práv duševného vlastníctva na internete. Aj keď sa môže zdať, že ide o výsostne partikulárnu a technickú oblasť doménových mien, je potrebné zdôrazniť, že elektronický spis

[242] ICANN: List of Approved Dispute Resolution Service Providers. [online]. [cit. 1.9.2020]. Dostupné z: https://www.icann.org/resources/pages/providers-6d-2012-02-25-en

[243] National Arbitration Forum: Domain Names Disputes. [online]. [cit. 1.9.2020]. Dostupné z: http://domains.adrforum.com/decision.aspx

[244] WIPO: Alternative dispute resolution. [online]. [cit. 1.9.2020]. Dostupné z: http://www.wipo.int/amc/en/domains/search/index.html

používaný v tzv. alternatívnom riešení sporov len potvrdil účelnosť a výhodu virtualizácie procesných úkonov. Jeho forma s funkcionalitami, akými sú bezpečná autentifikácia, disponovanie s podaniami a dôkazmi, nakladanie s elektronickými rozhodnutiami a možnosť zúčastniť sa on-line konferencie, je použiteľná aj v každom sporovom súdnom konaní. Navyše, existencia zákonného inštitútu dátových schránok v Českej republike a aj na Slovensku pripravila pôdu na ďalšie plnohodnotné využitie elektronického spisu v súvislosti s procesným doručovaním.[245] Elektronický súdny spis sa vzhľadom na rýchly technologický pokrok stane nevyhnutnosťou a zdá sa, že v informačnej spoločnosti bude jeho existencia predstavovať jednu z podmienok pre naplnenie základného práva účastníka na spravodlivý súdny proces. Avšak s takouto predikciou je ešte potrebné nakladať veľmi opatrne, nakoľko podľa Reilinga *„elektronická agenda na súdoch, akou je elektronické podanie, vedenie prípadu a elektronické spisy, nepredstavuje absolútnu podmienkou pre neohraničené poskytovanie digitálneho prístupu [účastníkom] ako takého.“* Inak povedané, otvorenie súdnej agendy formou „webových obchodov“ ešte neznamená zvýšenie právneho povedomia alebo väčší záujem o lepšie uplatňovanie práva zo strany občanov. Vždy bude totiž existovať istá skupina ľudí, ktorá si nebude takýto prístup môcť dovoliť alebo ktorá si bude vyžadovať ľudskú pomoc s prístupom k predmetnému informačnému systému.[246]

V súčasnosti sa najstarší koncept elektronického spisu využíva v právnom systéme USA. Je súčasťou tzv. celoštátneho informačného systému PACER (*Public Access to Court Electronic Records*).[247] Veľmi kritizovanou skutočnosťou je, že za prístup do spisu si servisné centrum PACER účtuje poplatky. Tento systém spravuje viac ako 500 miliónov dokumentov.[248] Je nutné ďalej pripomenúť, že PACER čelí kritike pre svoju technologickú zaostalosť. Solove uvádza, že *„systém PACER*

[245] MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6. Str. 162 an.

[246] REILING, Dory. Technology for Justice, Leiden University Press, 2009. Str. 204 an. [cit.1.9.2020]. Dostupné z: https://openaccess.leidenuniv.nl/bitstream/handle/1887/21365/file174577.pdf?sequence=1

[247] PACER: Public Access to Court Electronic Records [online]. [cit. 1.9.2020]. Dostupné z: https://www.pacer.gov/psc/hfaq.html

[248] LEE, Timothy. The inside story of Aaron Swartz's campaign to liberate court filings. ARS Technica. [online]. [cit.1.9.2020]. Dostupné z: http://arstechnica.com/tech-policy/2013/02/the-inside-story-of-aaron-swartzs-campaign-to-liberate-court-filings/2/

z technického pohľadu už dostatočne nechráni osobné údaje a zvyšuje riziko exponovania citlivých údajov súkromných osôb.“[249] Z dôvodu jeho spoplatnenia začali vznikať nové alternatívne systémy, ktoré sú schopné v nejakej časti získavať (kopírovať) dokumenty z PACERu a voľne ich publikovať.[250] Súčasné technické nastavenie bezpečnosti takéhoto systému je preto naozaj na zamyslenie. Aj keď vyššie uvedené analyzované systémy elektronických spisov trpia technickými nedostatkami, ich materiálny prínos je zjavne prevyšujúci.

2.7.5. Prínosy elektronického spisu

Je zrejmé že uvedené kvality sú v súčasnosti konfrontované s novými technologickými výzvami a hrozbami. Kybernetické útoky, poškodzovanie informačných systémov, zneužívanie citlivých a osobných údajov získali v poslednom čase odlišný rozmer. Nejde už len o pionierske rozmary uzavretej skupiny tínedžerov - programátorov, ale o riadenú činnosť organizovaných profesionálnych skupín motivovaných ziskom alebo politickou objednávkou. Napriek týmto hrozbám sa spoločnosť nemôže odvracať od využitia technologického pokroku. Ako Wiener kedysi povedal, je potrebné pamätať na to, že *„pokrok dáva nielen nové možnosti pre budúcnosť, ale prináša aj nové obmedzenia.“* [251] Preto každá implementácia informačných technológií do súdneho procesu musí byť vykonaná v takej miere, aby prípadné neželané účinky tejto implementácie nepredstavovali rovnaké alebo väčšie obmedzenie ako to, ktoré mohlo byť spôsobené zastaranými postupmi a metódami pôvodného súdneho procesu. Navyše, je vždy potrebné pomeriavať kvalitu pôvodných obmedzení s tými, ktoré prináša pokrok a technologická inovácia.

Každá implementácia technológie do sféry justičných procesov so sebou prináša určitú dávku komplikácií. Dotknutých subjektov a ich záujmov je tak veľa, že ani ten najlepší úmysel by nedokázal naplniť všetky rozmanité požiadavky a potreby.

---

[249] SCHWARTZ, John. An Effort to Upgrade a Court Archive System to Free and Easy. New York Times. [online]. [cit.1.9.2020]. Dostupné z: http://www.nytimes.com/2009/02/13/us/13records.html?pagewanted=all&_r=0

[250] Príkladom môže byť systém RECAP US Federal Court Documents. Aaron Schwarz do tohto systému stiahol z PACERu 2,7. mil. dokumentov (1%). Systém je dostupný na: https://archive.org/details/usfederalcourts alebo Viď SINGEL, Ryan. FBI Investigated Coder for Liberating Paywalled Court Records. WIRED. [online]. [cit.1.9.2020]. Dostupné z: http://www.wired.com/2009/10/swartz-fbi/

[251] WIENER, Norbert. With a new introduction by Steve J. HEIMS. The human use of human beings: cybernetics and society. London: Free Association, 1989. ISBN 18-534-3075-7.

Na druhej strane, hľadanie strednej cesty, t.j. vyvažovanie práv a záujmov s čo najmenšou budúcou ujmou a držanie sa fungujúceho, je osvedčeným historickým receptom. V časoch prvej americkej technologickej implementácie sa už v polovici deväťdesiatych rokoch na administratívnej pôde amerických súdov analyzovali benefity elektronického spisu. Bockweg vo svojej analýze uviedol nasledujúce výhody elektronického spisu, ktoré sú pozoruhodne stále platné:[252]

- *Okamžitý prístup k dokumentom v súdnom spise;*
- *Prenositeľnosť;*
- *Zníženie práce s fyzickými dokumentami ich údržbou a zbytočným kopírovaním;*
- *Jeho implementáciou dôjde k zníženiu počtu potrebných zamestnancov na správu spisovej služby, zjednodušeniu archívnej služby a umožní preradenie zamestnancov spisovej služby na iné vhodnejšie pozície;*
- *Integrita dokumentov a eliminácia omylov a nepresností;*
- *Zníženie časových strát a nákladov nazerajúcim subjektom;*
- *Lepšia kontrola publikácie judikatúry;*
- *Zníženie asistenčné služby s verejným prístupom k informáciám;*
- *Sprístupnenie zdieľania, anotácie a editovania dokumentov emailom;*
- *Možnosť fulltextového vyhľadávania;*
- *Priestorové úspory týkajúce sa administratívnych budov; a*
- *Automatické generovanie potrebných verejných správ ohľadom súdnych prípadov.*

K týmto kladným prínosom je ešte potrebné dodať jeden špeciálne dôležitý prínos pre priestor strednej Európy. Elektronický spis môže za predpokladu jeho

[252] BOCKWEG, Gary. Electronic case files in the federal courts: A preliminray examiation of goals, issues and road ahead. [online]. [cit.1.9.2020]. Dostupné z: http://www.kentlaw.edu/faculty/rstaudt/classes/oldclasses/internetlaw/casebook/Electronic%20Case%20Files%20in%20the%20Federal%20Courts%20Executive%20Summary%20in%20pdf%20format.pdf

transparentného fungovania priniesť aj zníženie nežiadúcej súdnej korupcie. Totiž jeho štatistické výstupy umožňujú bezprostrednú kontrolu zo strany účastníkov sporu – občanov. Nepochybne by išlo o jeden z vhodne zvolených nástrojov kontroly justície zo strany občanov.

2.8. Exkurz: anglo-americká právna doktrína elektronického dokazovania *e-discovery*

2.8.1. Predsúdne vyhľadávanie (*pre-trial discovery*)

Súdne alebo mimosúdne konanie začína prípravnou fázou. V občianskom súdnom konaní to je činnosť súdu pred zahájením konania.[253] V trestnom konaní je to napríklad prípravné konanie.[254] V rozhodcovskom konaní ide o prípravu prerokovania sporu.[255] Sú to zvyčajne úkony súdu, procesných strán alebo štátnych orgánov, ktoré v záujme zachovania kvality a prípravy na hlavné štádium súdneho konania zbierajú a posudzujú potrebné informácie. Angloamerický súdny proces kladie silný dôraz na túto fázu. Prípravné konanie je tu úzko späté so zaistením a vyťažovaním dôkazných prostriedkov, a to často aj bez ingerencie súdu alebo štátneho orgánu. V americkom práve sa táto fáza označuje ako *pre-trial discovery* (vyhľadávanie, objavovanie, resp. odhaľovanie).

Z historického pohľadu vznikol inštitút *discovery* ako diskrečný opravný prostriedok (*equity*), no neskôr sa transformoval do obyčajového a aj písaného práva. Účelom bolo umožniť strane zistiť od protistrany všetky skutočnosti a fakty týkajúce sa vlastného prípadu. Americký súd je zvyčajne v tejto fáze pasívnym aktérom a priamo neparticipuje na procese vyhľadávania dôkazných prostriedkov. Rozhoduje len o návrhoch strán o špecifikácii vyhľadávania alebo o poskytnutí súdnej ochrany proti neprimerane rozsiahlemu vyhľadávaniu.[256] V súčasnosti môžu strany žiadať o

[253] Napr. zaistenie dôkazu v zmysle § 78 OSŘ.

[254] Prípravné konanie v ČR zahŕňa štádium preverovania všetkých okolností dôvodne nasvedčujúcich tomu, že sa stal trestný čin, a štádium vyšetrovania. To už predstavuje vedenie trestného stíhania proti konkrétnej osobe (obvinenému). Prípravné konanie vykonáva OČTK, t.j. policajný orgán a štátny zástupca. Viď JELÍNEK, Jiří, a kolektiv. Trestní právo procesní. 3. vyd. Praha: Leges, 2013. ISBN 978-80-87576-44-1. Str. 17.

[255] § 22 Řádu Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky, [online]. [cit.1.9.2020]. Dostupné z: https://www.soud.cz/rady/rad-rozhodciho-soudu-01-07-2012

[256] Rule 26 FRCP.

objavenie takého dôkazného prostriedku, ktorý vedie k vykonania prípustných dôkazov, najčastejšie od žalovanej strany alebo tretej strany.[257] Ide o pomerne široké procesné právo, ktoré zahŕňa skúmanie rôznorodých dôkazných prostriedkov. Základnou črtou tohto inštitútu je, že informácie nemusia byť priamo so skúmanou vecou spojené, ale môžu viesť k objaveniu ďalších dôkazných prostriedkov, ktoré sú pre danú vec relevantné.[258]

Z pohľadu kontinentálneho súkromného práva je zaujímavé, že povinnosť odkrývať informácie je vymožiteľná a sankcionovateľná štátom (súdom). Inak povedané, proces prípravy dokazovania je ponechaný výlučne súkromným stranám sporu, avšak je vynútiteľný štátnou mocou. Je potrebné pripomenúť, že veľká časť civilných súdnych prípadov v USA končí vzájomnou dohodou strán po objasnení a predložení dôkazov v prípravnom konaní.[259] Tento inštitút sa môže uplatniť aj v trestnom konaní, kde obžalovaný má právo žiadať vydanie relevantných informácií od prokurátora (štátneho zástupcu). Inštitút je regulovaný federálnymi, ale aj štátnymi zákonmi s veľmi detailným popisom procesu pozostávajúceho z iniciačného stretnutia strán, spôsobu odhaľovania a sprístupňovania informácií, procesu depozície, vypočúvania, žiadosti o sprístupnenie a žiadosti o vydanie informácie.[260]

[257] V prípade strany, ktorá nie je účastníkom súdneho konania, sa inštitút discovery uplatňuje pomocou súdnej obsielky nazývanej *subpoena*. Anglo-americký právny systém rozlišuje dva základne druhy: *subpoena ad testificandum* (predvolanie alebo predvedenie osoby k výsluchu) a *subpoena duces tecum* (výzva na vydanie alebo predloženie veci). Názov pochádza z latinského *sub poena*, čo znamená pod hrozbou sankcie. Viď CUMMINS, Robert R. Basics of legal document preparation. Delmar Publishers Inc. 1997. ISBN: 0-8273-6799-6. Str. 209.

[258] Táto otázka je kontroverzná v prípade vyhľadávania dát uložených na verejnom cloude, ktorý používa viacero užívateľov. Viď ARAIZA, Alberto, G. Electronic Discovery in the Cloud, Duke Law and Technology Review, č. 8. 2011. Str. 323–330. [online]. [cit.1.9.2020]. Dostupné z: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1222&context=dltr

[259] KYCKELHAHN T., COHE T.C. Bureau of Justice Statistics Special Report. Civil Rights Complaints in U.S. District Courts, 1990-2000. Str. 5. [online]. [cit.1.9.2020]. Dostupné z: https://www.bjs.gov/content/pub/pdf/crcusdc06.pdf

[260] *„[...] domnievame sa, že zneprístupnenie dôkazov svedčiacich v prospech obžalovaného na základe jeho žiadosti je v rozpore s riadnym procesom, pri ktorom je dôkaz podstatný pre vinu alebo trest, a to bez ohľadu na dobrú vieru alebo zlú vieru stíhania."* Bod 87. Najvyšší súd USA: Prípad Brady v. Maryland, 373 U.S. 83 (1963) [online]. [cit.1.9.2020]. Dostupné z: https://scholar.google.com/scholar_case?case=9550433126269674519

Pre-trial discovery má podobné vlastnosti s procesným inštitútom *vyšetrovacieho dôkazu*, ktorý je zriedkavo používaný v kontinentálnom systéme práva[261] alebo s predbežným opatrením v podobe zabezpečenia dôkazného prostriedku (napr. vo veciach práv duševného vlastníctva).[262] Tieto inštitúty sú ale v kontinentálnom systéme vykonávané prostredníctvom súdu. V americkom práve je *pre-trial discovery* však ďaleko širší, neznamená len povinnosť vydať vec (dôkaz) v zmysle známej edičnej povinnosti,[263] ale cieli na zaobstaranie rôznych svedeckých výpovedí (*depositions by oral examination*), žiadostí vo forme písomných dopytov (*depositions by written questions*), žiadostí smerujúcich k vyvráteniu alebo priznaniu určitej skutočnosti (*requests for admissions*), žiadostí smerujúcich k vydaniu dôkazov (*production*). Proces je ohraničený zásadou prísnej koncentrácie dôkazov (všetky rozumne zistiteľné dôkazy musia byť známe pred postúpením veci na súd), nakoľko v americkom procesnom práve sú rozhodnutia o *questio facti* v právomoci poroty a nie súdu. Preto v sebe proces *pre-trial discovery* zahŕňa časť procesu, v ktorom sa získané dôkazy hodnotia a analyzujú v nadväznosti na podanú žalobu do doby, kedy sporné časti žaloby nezamieria pred súd.

2.8.2. Elektronické vyhľadávanie (*electronic discovery*)

Inštitút *pre-trial discovery* je kľúčovým štádiom súdneho sporu v anglo-americkom práve, ktorý vo väčšine prípadov vedie k ukončeniu samotného konania pred súdom.[264] Sústredenie sporu do procesnej fázy prípravného konania odbremeňuje štát od finančných nákladov na zbieranie dôkazov a prenáša ich na strany sporu. Žiaľ, môže byť aj zárodkom nespravodlivosti alebo nerovného postavenia strán. Kritici amerického *pre-trial discovery* hovoria o „rybárskych výpravách“ (*fishing expeditions*).[265] Ich účelom môže byť zneužitie pravidiel získavania dôkazov formou

[261] Napr. ak dôkazný návrh je ešte neúplný a neurčitý, ide o návrh na vyšetrovací dôkaz. Jeho vykonanie má strane ešte len umožniť, aby mohla konkretizovať svoje skutkové tvrdenia a k ich preukázaniu potom následne podať ďalšie, presnejšie a jasnejšie dôkazné návrhy. Viď MACUR, Josef. Vyšetřovací důkaz v civilním soudním řízení. Právní rozhledy. 2000, č. 2, Str. 46 - 51.

[262] § 78 OSŘ alebo § 345 an CSP.

[263] V zmysle § 129 ods. 2 OSŘ „předseda senátu může uložit tomu, kdo má listinu potřebnou k důkazu, aby ji předložil, nebo ji opatří sám od jiného soudu, orgánu nebo právnické osoby.“

[264] Väčšina súdnych konaní v Amerike končí vo fáze *pre-trial discovery*.

[265] Advokáti používajú *fishing expeditions* na odhalenie defamujúcich informácií o žalovanom alebo jeho zamestnancoch. Rovnako takto získavajú obchodné tajomstvo, know-how alebo iné právom chránené informácie. Viď BEISNER, John H. Discovering a better way: the need for effective civil litigation reform. Duke Law Journal, vol. 60, no. 3, 2010, Str. 547–596.

obrovského počtu dopytov voči povinnej strane a upravovanie žaloby na základe získaných informácií. [266] Finančná stránka súdneho konania sa odráža najmä v otázkach nákladného vyhľadávania a získavania elektronických dát a záznamov (*electronic stored information*). [267] Pre toto štádium sa vžil názov *electronic discovery* alebo *e-discovery.* Ako už bolo uvedené, inštitút *e-discovery* je používaný v civilnom, ale aj trestnom konaní anglo-amerického systému práva.[268] Každá procesná strana má právo vyšetrovať skutkové okolnosti prípadu prostredníctvom použitia procesného inštitútu objavovania dôkazov. V najširšom zmysle slova ide o každý akt objavovania elektronickej informácie, ktorá doposiaľ nebola objavujúcej strane známa.[269]

2.8.3. Vplyv *e-discovery* na civilný proces

Systém dokazovania v USA je príznačný veľmi detailnou legislatívnou úpravou na federálnej, ale aj štátnej úrovni a bohatou judikatúrou súdov, ktorá má svoj prameň v sérii známych precedensoch okresného súdu New York vo veci *Zubulake v. UBS Warburg.*[270] Tu sa zrodilo pravidlo, ktoré definuje rozsah povinnosti strany, ktorá čelí alebo môže čeliť sporu, na uchovávanie všetkých potencionálnych dôkazov. Totiž, ak strana odôvodnene predvída súdny spor, musí ukončiť svoju rutinnú archiváciu alebo ničenie dokumentov a zaviesť takzvaný *litigation hold* (zábezpeku dôkazov pre spor) pre všetky dotknuté dokumenty a súvisiace elektronické dáta. Tento inštitút zabezpečuje časom neobmedzené uchovanie relevantných dát, avšak so zrejmým dopadom na finančné náklady povinného. Najproblematickejšie sú situácie, kedy

[266] MCMAHON, P. Rediscovering the Equitable Origins of Discovery: The 'Blending' of Law and Equity Prior to Fusion. in J. Goldberg, H. Smith, & P. Turner (Eds.), Equity and Law: Fusion and Fission. Cambridge: Cambridge University Press. 2019. Str. 280.

[267] V angličtine je to pojem "*ESI*" alebo "*Electronic Stored Information*", ktorý zahŕňa všetky elektronicky uložené informácie vrátane spisov, kresieb, grafov, fotografií, zvukových záznamov, obrázkov a iných údajov alebo kompilácií údajov - uložených na akomkoľvek médiu, z ktorého je možné získať informácie buď priamo alebo v prípade potreby po preklade odpovedajúcou stranou do primerane použiteľnej formy. Rule 34 (1) FRCP.

[268] Rule 34 (a) (1) (A) FRCP.

[269] Názov "*discovery*" je príznačný pre americký právny systém. Právny systém Anglicka a Walles používa názov "*disclosure*", brazilský súdny proces pracuje s názvom "*producao de provas*" a japonský poriadok s termínom "*Shoko-hozen*". Viď Bento. V.M. Globalization of Discovery: The Law and Practice under 28 U.S.C. § 1782. Kluwer Law International B.V., 21 Nov 2019. E-book. Chapter 1 Foundational Concepts of International Discovery. [online]. [cit.1.9.2020]. Dostupné z: https://books.google.ch/books?id=YmfIDwAAQBAJ&printsec=frontcover&dq=inauthor:%22Lucas+V.M.+Bento%22&hl=en&sa=X&ved=0ahUKEwiw19CL6OznAhXhGDQIHYpxB1sQ6AEIKDAA

[270] LI, Victor. Zubulake 10 Years After: Landmark case created an industry–and still stirs debate. ABA Journal, vol. 100, no. 9, 2014, Str. 48.

povinný disponuje množstvom neštruktúrovaných a nezatriedených dát. Vzhľadom na to, že nepozná dobre objem a obsah svojich dát, spôsobí to jeho neschopnosť splniť túto zákonom predpísanú požiadavku a vystavuje sa riziku penalizácie alebo trestného stíhania.

Žiaden právny systém nie je v otázkach zbierania a produkcie dôkazov tak komplexný a zároveň tak prísne formálny ako americký súbor noriem dôkazného práva. Napriek tomu, že už existujú nepatrné prieniky tohto spôsobu dokazovania do kontinentálneho systému, ide hlavne o vysokú formálnosť dokazovania v americkom práve, ktorá je príznačná tým, že strany predkladajú len dôkazné prostriedky definované zákonom alebo judikatúrou a vedú dôkazné konanie podľa presne špecifikované postupu. [271] V tomto vidíme značnú nevýhodu oproti kontinentálnej zásade voľného hodnotenia dôkazov. Na jednej strane je americký systém dokazovania predvídateľný, stranám je jasné, aké dôkazy musia byť predložené, no na druhej strane, v prípade elektronického dôkazného prostriedku z atypického a nepoznaného zdroja bude taký dôkaz čeliť procesným prekážkam na jeho vykonanie a strádať na svojej dôkaznej sile. Trend používania nových formátov dátových zdrojov a celková dynamika technológie je pre udržanie kroku s legislatívou, ale aj s rozhodovacou praxou ťažko dosiahnuteľná. Je však potrebné súhlasiť s Macourom v tom, že otázka informačného deficitu procesnej strany v kontinentálnom systéme práva ostáva bez povšimnutia a neriešená. *„Jeho instituty, zejména předběžné vyhledávání informací v rámci „discovery“, nelze převzít ani přizpůsobit kontinentálnímu procesu, v němž každé konkrétní civilní soudní řízení od počátku až do konce je řízeno soudem a vyhledávání informací nelze svěřit výlučné aktivitě stran, resp. jejich advokátů, bez řídící ingerence soudu.“*[272] Domnievame sa, že fundamenty a princípy elektronického dokazovania v anglo-americkom práve sú inšpirujúce, a to aj pre kontinentálne právo (najmä z pohľadu hodnotenia dôkazných prostriedkov), ale prísna reštrikcia počtu a

[271] Napr. v otázkach súťažného práva v prístupe k verejným dokumentom a vyhľadávaniu podľa smernice Európskeho parlamentu a Rady 2014/104/EÚ z 26. novembra 2014 o určitých pravidlách upravujúcich žaloby podľa vnútroštátneho práva o náhradu škody utrpenej v dôsledku porušenia ustanovení práva hospodárskej súťaže členských štátov a Európskej únie. Viď KULMS, R. Competition law enforcement under informational asymmetry. China-EU Law Journal 5, 2017. Str. 209–231. [online]. [cit.1.9.2020]. Dostupné z: https://link.springer.com/content/pdf/10.1007/s12689-016-0073-8.pdf

[272] MACUR, Josef. Vyšetřovací důkaz v civilním soudním řízení. Právní rozhledy. 2000, č. 2, Str. 46 – 51.

formulárový postup zabezpečenia dôkazných prostriedkov je pre našu právnu kultúru neudržateľný.

2.9. Zhrnutie kapitoly

Elektronické dokazovanie predstavuje stále málo poznanú oblasť procesného práva a samotná téma v nadväznosti na informačné technológie sľubuje svoje budúce rozšírenie. Na rozdiel od anglo-americkej právnej tradície nemá proces dokazovania pomocou elektronického dôkazného prostriedku v civilnom konaní ucelenú osobitnú zákonnú alebo podzákonnú úpravu, čo však nebráni jeho plnej aplikácii v podmienkach občianskeho súdneho konania kontinentálnej právnej kultúry.

V predloženej kapitole sme sa snažili priblížiť podstatu elektronického dôkazného prostriedku z pohľadu českého, slovenského, ale aj zahraničného práva. Boli identifikované problematické biele miesta, ktoré si zaslúžia hlbšie štúdium a bádanie. Pokúsili sme sa objasniť terminológiu elektronického dokazovania a jeho súčasné limity. Vysvetlili sme, prečo na strane vykonávateľa dôkazného prostriedku prevláda informačný deficit, a akú úlohu tu zohráva informačná teória.

Aby bol elektronický dôkazný prostriedok správne vykonaný, je potrebné, aby súd poznal rôzne kategórie jeho kvalít. Opísali sme otázky potencionálnej ubiquity a volatility. Poukázali sme na dôkaznú spoľahlivosť a integritu. Načrtli sme, do akej miery je možné skúmanie dôkaznej spoľahlivosti elektronických dôkazných prostriedkov v konkrétnych prípadoch nahradiť formálne akceptovanou deklaráciou o dôveryhodnosti zdroja pôvodu. Medzi ďalšie skúmané kategórie sme zaradili pravdivosť a vierohodnosť, ktoré súvisia s diskutovanou mierou dôkazu. Ako posledné boli vysvetlené kategórie platnosti a zákonnosti elektronického dôkazného prostriedku v kontexte ústavného testu proporcionality, ktorý v určitých prípadoch dáva priechod aj inak nezákonným dôkazom.

Ťažiskovou časťou bola predložená zásada voľného hodnotenia dôkazov v kontexte analýzy rizík. Objasnili sme, prečo súd môže voliť určitú preferenciu rizika súvisiaceho s rozhodovaním práve o elektronických dôkazných prostriedkoch. Rovnako, aká je miera rizika priaznivého alebo nepriaznivého účinku pri použití tohto dôkazného prostriedku pre hľadanie práva súdom. Analýza rizika mala podporiť platnosť zásady voľného hodnotenia dôkazov a načrtnúť istý rámec možného

posudzovania elektronického dôkazného prostriedku súdom. V neposlednom rade neostali nepovšimnuté ani všeobecné otázky znaleckého dokazovania a ich vplyv na hodnotenie elektronického dôkazného prostriedku.

Pri hľadaní podstaty elektronického dôkazného prostriedku bolo potrebné uviesť jeho praktický aspekt - elektronický súdny spis, a to z hľadiska viacerých súdnych, ale aj mimosúdnych procesných úprav. V poslednej a doplnkovej časti sme urobili exkurz do anglo-amerického právneho systému a vysvetlili procesný inštitút *electronic discovery*, a aký je jeho vplyv na civilný proces.

V tejto kapitole sme poukázali na to, že elektronický dôkazný prostriedok je vo svetle každodenného praktického použitia zraniteľný, ba dokonca deformovaný a často nepochopený súdmi. Ako bude vysvetlené ďalej v osobitnej časti, či už ide o zaistenie elektronického dôkazného prostriedku v súvislosti s podozrením zo spáchania trestného činu alebo o zaistenie obsahu webovej stránky v civilnom konaní, vždy je potrebné brať na zreteľ, že elektronické dokazovanie vyžaduje špeciálny prístup a hlbšiu vedomosť o technologických aspektoch získavania a uchovávania elektronických informácií. K samotnej podstate elektronického dokazovaniu možno dodať slová literárnej postavy, detektíva Sherlocka Holmesa, a to že *„sú určité pozície na šachovnici, ktoré nezaujímajú šachistov ako hra – nezaujímajú ich, čo sa týka budúceho vývoja – ale sú nanajvýš zaujímavé tým, že obsahujú stopy toho, čo sa muselo odohrať v minulosti.“*[273]

[273]SMULLYAN, Raymond. Šachové záhady Sherlocka Holmese, aneb, Padesát úloh šachové dedukce, které vám nedají spát. 1. vyd. Praha: Mladá fronta, 2005. ISBN 80-204-1233-6. Str. 14.

3. Informačná suverenita štátu a cezhraničné dokazovanie

3.1. Úvodné poznámky

Informačná suverenita je v súčasnosti často skloňovaný pojem v otázkach medzinárodného práva verejného, akými sú napríklad otázky kyberbezpečnosti, cezhraničných kyberútokov, virtuálnych vojenských operácií, ale aj cezhraničného elektronického dokazovania. V nasledujúcej kapitole opíšeme základy suverenity zo štátoprávneho hľadiska, jej formovanie v kyberpriestore a následný vplyv takejto informačnej suverenity na výkon súdnej moci. Pokúsime sa zodpovedať otázku vplyvu informačnej suverenity na dostupnosť elektronických dôkazných prostriedkov v kyberpriestore. Nasledujúca kapitola má za cieľ vysvetliť pojem informačnej suverenity štátu a odôvodniť tézu, že technológia kyberpriestoru oslabuje teritoriálnu výkonnú moc štátu voči virtualizovaným subjektom, čo má dopad na súdnu moc, ako aj na elektronické dokazovanie. Štát toto oslabenie kompenzuje buď snahou o „oplotenie“ kyberpriestoru (napr. cenzúra internetu, regulácia definičných autorít) alebo snahou o pristúpenie k zdieľanej suverenite tak, ako to robí v prípade vonkajšej zvrchovanosti, kde prirodzene vyhľadáva spojencov a partnerov. Štát preto pristupuje ku kooperácií s ostatnými štátmi a vyhľadáva zdroj svojej suverenity v spolupráci s definičnými autoritami, resp. nadnárodnými združeniami, ktoré sa podieľajú na fungovaní kyberpriestoru.

3.2. Suverenita štátu

Suverenita štátu je základným znakom každého štátneho zriadenia. Ide taktiež o hlavný pojem medzinárodného práva verejného, ktorý označuje nezávislosť štátu na akejkoľvek inej moci ako tej vlastnej.[274] Táto nezávislosť sa skladá z dvoch častí. Z vonkajšej zvrchovanosti v medzinárodných záležitostiach a z výlučnej právomoci voči vnútorným veciam. V tradičnej štátovede je pojem suverenity vždy spätý s hranicami

[274] HENDRYCH, D. a kol., Heslo: Suverenita státu, Právnický slovník. 3., podstatně rozš. vyd. v Praze: C.H. Beck. Beckovy odborné slovníky. 2009, ISBN 978-80-7400-059-1. Str. 38.

štátneho fyzického územia (obdobne Jellinek).[275] Totiž fyzické hranice vedia presne opísať priestor štátnej moci, kde sa táto vykonáva.

Ale ako to je so suverenitou štátu vo virtualizovaných spoločenských vzťahoch, resp. v kyberpriestore? Môžu národné súdy, orgány štátnej moci alebo jednotlivci zabezpečovať a získavať elektronické dôkazy v cezhraničných prípadoch? Aby štát mohol vykonávať svoju informačnú zvrchovanosť, musí ňou disponovať. Pre účel tejto práce budeme pojem informačnej suverenity definovať ako pole pôsobnosti štátu v kyperpriestore, ktoré štát kontroluje a ovplyvňuje, a ktoré predstavuje súbor jeho virtualizovaných záujmov, nad ktorými má štát právo vykonať moc v prípade ich napadnutia, resp. narušenia (vonkajší aspekt), a súčasne tu vykonáva výlučnú kompetenciu ochrany informačných práv svojich občanov (vnútorný aspekt).

Podobne ako tomu je pri kompetenčnej teórii, ktorá chápe územie štátu ako vymedzenú časť územia, na ktorej sa realizuje teritoriálna kompetencia štátu, domnievame sa, že štát má povinnosť zabezpečiť odvodenú informačnú svojbytnosť seba, svojich záujmov a občanov v kyberpriestore. Princíp neporušiteľnosti štátnych hraníc definuje klasickú zvrchovanosť štátneho zriadenia. Revolúcie, spojenia, rozdelenia, vojny a dobyvačné výpravy prekresľujú politickú mapu, ktorá jasne stanovuje pravidlá hry vo fyzickom, resp. aktuálnom priestore. História a štátoprávna veda priniesla viacero teórií ako sa pozerať na štátne územie, napr.:[276]

- *teória subjektu*
    - *posudzuje územie ako vlastníctvo, resp. predmet, s ktorým štát môže ľubovoľne nakladať a disponovať,*
- *priestorová teória*
    - *rozoznáva územie ako fyzický priestor, resp. plochu, ktorá sa vyznačuje uplatnením štátnej moci v rámci tohto priestoru a je nezávislá od iných zvrchovaných priestorov, resp. štátov,*
- *kompetenčná teória*

[275] Štát je zložený zo štátneho územia, štátneho národu a štátnej moci. Viď PAVLÍČEK, Václav. a kol., Ústavní právo a státověda, I.díl, Linde Praha, a.s. 1998, Str. 48.

[276] PIROŠ, Peter. Princíp ochrany a neporušiteľnosti štátnych hraníc. e-Polis.cz. [online]. [cit.1.9.2020]. Dostupné z: http://www.e-polis.cz/clanek/princip-ochrany-a-neporusitelnosti-statnych-hranic.html

- *rozoznáva územie štátu ako časť územia, na ktorej sa realizuje len priestorová kompetencia štátu.*

Z historického hľadiska je vznik akéhokoľvek štátu ukončený až vtedy, keď sú všetky jeho podstatné znaky naplnené, a keď orgány tohto štátu skutočne vykonávajú vládu a dostáva sa im poslušnosti od obyvateľov žijúcich na danom území.[277] Medzinárodné uznanie prichádza neskôr v podobe deklaratórneho aktu. Tu sa vynára otázka, čo s obyvateľmi žijúcimi alebo pohybujúcimi sa v globálnom kyberpriestore, ktorí sa virtualizujú bez hraníc štátov pomocou digitálnej siete internet? Ktorého suveréna legitimujú k výkonu skutočne najvyššej a konečnej vlády v tomto priestore?

3.3. Hranice ako technológia kyberpriestoru

Podľa Lemleyho, môžeme uvažovať o kyberpriestore ako o metafore fyzického územia. Súdy by tu mali analogicky aplikovať zákony obdobne ako tomu je pri území. Avšak táto metafora poslúži účelu len vtedy, ak pochopíme limity kyberpriestoru, ktorý dozaista nie je fyzickým svetom v pravom zmysle slova.[278] Jedným z limitov je, že kyberpriestor je ohraničený technickými prostriedkami a nie politickou mapou ostatných suverénnych štátov. Technické prostriedky sú definované infraštruktúrou siete, kódom prenosových protokolov, použitým softvérom a dozaista aj dostupnosťou (internetovou konektivitou). Občania digitálneho veku sa vymaňujú z tradičných jurisdikcií a dobrovoľne sa podrobujú cudzím poskytovateľom emailových služieb, sociálnych sietí alebo registrátorom doménových mien (definičné autority). Virtualizovanie činností občanov akéhokoľvek štátu neospravedlňuje tento štát ku kapitulácii nad jeho povinnosťou mať informačnú suverenitu nad záujmami, ktoré sú chránené právom. Ale rovnako ho to neoprávňuje k uzurpácii kompetencií od zvolených poskytovateľov informačných služieb alebo iných definičných autorít v kyberpriestore, a to bez ohľadu na ich štátnu príslušnosť. Domnievame sa, že na to, aby štát ovládal toto pole pôsobnosti, musí spolupracovať s definičnými autoritami, ktoré spadajú do jeho jurisdikcie, ale aj jurisdikcie ostatných štátov (zdieľaná suverenita). Štát si vypožičiava ich kompetenciu, ktorá je legitimovaná účastníkmi kyberpriestoru

[277] Ibid. PAVLÍČEK. Str. 50.

[278] LEMLEY, M. Place and Cyberspace. California Law Review. no. 2. vol. 91. California Law Review. 2003. Str. 542.

bez ohľadu na ich štátnu príslušnosť.[279] Najvyššia a konečná moc štátu nie je kritériom pre informačnú suverenitu štátu tak, ako tomu je pri teritoriálnej suverenite. Totiž zdieľaná suverenita môže byť odvodená od legitimity definičnej autority, ktorá má svoj základ v dvoch skutočnostiach:

- prvou je technologická spätná väzba medzi definičnou autoritou a jej adresátom (napr. súhlas užívateľa s informačnou službou),
- druhou je samostatná legitimita vládnej moci v štáte, prostredníctvom ktorého bolo umožnené definičnej autorite virtualizovať svoje aktivity do kyberpriestoru, resp. definovať pravidlá používania tohto priestoru svojím adresátom.

Zdieľaná suverenita prináša vzťahy mimo teritórium štátu. Preto pole pôsobnosti štátu v kyberpriestore môže byť širšie ako tomu je pri klasickom štátnom území. Polčák a Svantensson v otázke kolízie suverenít hovoria o možnom riešení spočívajúcom v hľadaní oprávneného záujmu (*legitimate interest*) a podstatnej súvislosti (*substantial connection*) medzi predmetnou vecou a štátom, berúc do úvahy princíp proporcionality.[280] Pôvodný zdroj princípu teritoriality, t.j. fundamentálny princíp suverenity štátu definovaný Harvardskym návrhom dohovoru o súdnej právomoci vo vzťahu k trestnej činnosti z 1935 [281] považujú títo autori za obmedzujúci a neaplikovateľný pre kyberpriestor. V nekontroverzných situáciách bude mať príslušný štát suverenitu nad prevádzkou servera na jeho území. Bude mať oprávnený záujem a identifikuje hmotnú súvislosť medzi posudzovanou vecou a štátom. Navyše, princíp proporcionality medzi štátom chráneným záujmom a inými záujmami bude dodržaný. Avšak v kontroverzných situáciách pripúšťajú, že nie vždy bude mať štát plnú suverenitu nad dátami a servermi na jeho území. Preto je potrebné dôkladne

[279] Znakom totalitných štátov je, že si uzurpujú túto kompetenciu vlastnou normatívnou reguláciou a prísnymi technologickými obmedzeniami siete (napr. čínsky štátny firewall). Avšak ich informačná suverenita je následne „deravá nádoba“ a nekončiaca naháňačka za technologickým pokrokom.

[280] POLČÁK, Radim. SVANTESSON, Dan. Chapter 6. A possible method for solving sovereignty clashes. In: Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. Edward Elgar Publishing, 2017 – (eBook 1/19) Str. 288 alebo SVANTESSON, Dan. A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. AJIL Unbound. 2015. Vol 109. Str. 69-74.

[281] Draft Convention on Jurisdiction with Respect to Crime. 1935. American Journal of International Law, 29(S1), Str. 439-442. [online]. [cit. 1.9.2020]. Dostupné z: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/draft-convention-on-jurisdiction-with-respect-to-crime/30D6EC4FC2D1E0377E93B7623992A189

posúdiť kolíziu záujmov viacerých štátov. Naša práca podporuje tento názor a dopĺňa tento rámec o úvahu o existencii zdieľanej informačnej suverenity medzi štátom na jednej strane a definičnou autoritou na strane druhej. V súčasnosti sme svedkami toho, že čoraz viac neštátnych autorít zasahuje do organizácie štátu a teda i do jeho samotnej suverenity. Príkladom môže byť vzostup významu medzinárodných organizácií, zdieľanej globálnej ekonomiky, ale aj medzinárodného kapitálu. Paradoxne väčšina týchto narušiteľov tradičného konceptu suverenity súvisí s posilňovaním bezpečnosti štátneho zriadenia a v neposlednom rade vyššej ochrany občana.[282] Jedným z dôležitých narušiteľov sa zdá byť technológia umožňujúca virtualizovanie spoločenských vzťahov. Cieľom štátu je nielen vytvárať podmienky pre fungovanie kybernetickej stratégie v úmysle chrániť vlastné bezpečnostné záujmy, ale aj regulovať tie definičné autority, ktoré spadajú pod jeho výlučnú právomoc (*lex fori*).[283] Práve teritoriálnou reguláciou definičných autorít (napr. doménovej autority alebo poskytovateľa informačných služieb v štáte) si definuje vlastné pole pôsobnosti v kyberpriestore (klasické oplotenie).[284] Ale aby informačná suverenita štátu bola efektívna, štát sa nemôže uspokojiť len s jednostrannou reguláciou. Zdá sa, že podstatným znakom informačnej suverenity štátu je aj to, že musí byť schopný presvedčiť cudzie definičné autority alebo ostatné štáty k vzájomnej spolupráci (napr. prostredníctvom medzinárodného práva v otázkach spolupráce vo veciach dokazovania), čím si upevní svoju informačnú suverenitu aj nad rámec jemu vlastných fyzických hraníc voči svojim občanom. Domnievame sa, že tu hovoríme o zdieľanej suverenite, kedy štát za dodržania určitých podmienok spoluvytvára suverenitu spolu s iným subjektom v kyberpriestore. Vďaka tomu je jeden štát schopný dožiadať údaje a dáta z účtu páchateľa kyberútoku nielen od policajného alebo súdom zvoleného orgánu iného štátu, ale aj priamo od poskytovateľa informačnej služby pôsobiacej mimo klasické hranice svojho územia.

[282] UŠIAK, J.: Premeny suverenity európskych štátov v kontexte vybraných teórií medzinárodných vzťahov. In.: Současná Evropa, roč. 14, 2009, č. 2., St. 35-54, ISSN 1804-1280.

[283] Príkladom v ČR je zákon č. 181/2014 Zb. o kybernetickej bezpečnosti.

[284] Navyše legitimita definičnej autority nepochádza výlučne od štátu, v ktorom má sídlo. Jej základ musíme hľadať v technologickej spätnej väzbe založenej na demokratických hodnotách a postojoch užívateľov, ktorí sa rozhodli pre túto definičnú autoritu. Tento super-rýchly a konkludentný dialóg medzi definičnou autoritou a užívateľom je možné nazvať technologickou spätnou väzbou. Aby mohol štát do takejto technologickej spätnej väzby ingerovať (ovplyvniť jej chovanie), musí mať faktickú dôveru definičnej autority tak, ako ona musí získať svoju dôveru od užívateľov jej služieb.

3.4. Právo štátu na sebaobranu a dokazovanie v kyberpriestore

Kyberpriestor je mód bytia, ktorý prešiel virtualizáciou.[285] Podstatné je, že výstupy z virtuálneho prostredia majú priame dopady na aktuálny svet. Príkladom sú internetové útoky, ktoré majú za cieľ ovládnuť alebo poškodiť hmotné predmety alebo iné záujmy chránené právom napadnutého štátu. Tie sa nelíšia od bezprostredného fyzického útoku na daný predmet. Aj keď Charta OSN v článku 2 ods. 4 použitie sily v medzinárodných vzťahoch zakazuje, v kompetencii každého suveréna je možnosť takéto útoky odvracať využitím sily alebo iných donucovacích prostriedkov.[286] V Charte OSN z roku 1945 sú explicitne uvedené dve výnimky zo zákazu použitia ozbrojenej sily v medzinárodných vzťahoch. Ide o použitie sily so súhlasom Bezpečnostnej rady OSN a použitie sily pri sebaobrane štátu či koalície štátov, ktoré je definované v článku 51 kapitoly VII.[287]

Prirodzené právo na individuálnu alebo kolektívnu sebaobranu je základným pilierom suverenity štátu. Toto právo je v súčasnosti interpretované veľmi úzko. Doktrína uvádza, že útok musí trvať a protiútok musí rešpektovať zásady nevyhnutnosti a primeranosti. Avšak existujú aj opačné názory, ktoré hovoria, že sebaobrana je prípustná v prípade, ak bola predvídateľná pred zahájením útoku (hroziaci útok).[288] Otázkou je, do akej miery môžeme toto právo vykladať aj v prípade sebaobrany voči asymetrickým útokom, akými sú kybernetické ataky na virtualizované záujmy štátu alebo jeho občanov? Analogicky sa môžeme pýtať, či je možné považovať

[285] Ibid. LÉVY, Pierre. Str. 27 a 44.

[286] Na základe článku 2 (4) Charty OSN sa štáty majú vystríhať *„vo svojich medzinárodných stykoch hrozby silou alebo použitia sily proti územnej celistvosti alebo politickej nezávislosti ktoréhokoľvek štátu, tak aj akýmkoľvek iným spôsobom nezlučiteľným s cieľmi Organizácie Spojených národov.“* Viď Charta Organizace spojených národů a Statut Mezinárodního soudního dvora, Informační centrum OSN, Praha, 2002, Str. 9.

[287] *„Žiadne ustanovenie tejto charty neobmedzuje, v prípade ozbrojeného útoku na niektorého člena Organizácie Spojených národov prirodzené právo na individuálnu alebo kolektívnu sebaobranu, kým Bezpečnostná rada neurobí opatrenia na udržanie medzinárodného mieru a bezpečnosti. Opatrenia urobené členmi pri výkone tohto práva sebaobrany oznámi štát ihneď Bezpečnostnej rade; nedotýkajú sa nijako právomoci a zodpovednosti Bezpečnostnej rady, pokiaľ ide o to, aby kedykoľvek podľa tejto Charty podnikla takú akciu, akú považuje za potrebné na udržanie a obnovenie medzinárodného mieru a bezpečnosti.“* Ibid. Charta Organizace spojených národů a Statut Mezinárodního soudního Dvora.

[288] SIMMA, B. NATO, the UN and the Use of Force: Legal Aspects, European Journal of International Law, roč. 10, č. 1, 2003, Str. 2–5.

za právo štátu na sebaobranu aj právo zadovážiť si elektronické dôkazy o kyberútoku z kyberpriestoru bez ohľadu na fyzické hranice jeho územia?

Na zodpovedanie tejto otázky je nutné určiť, či je útok v kyberpriestore použitím sily v medzinárodných vzťahoch. Aj keď kyberútoky nemajú jednoznačnú podobu použitia sily podľa medzinárodného práva (napr. ozývajú sa hlasy proti zbytočnej militarizácii kyberpriestoru),[289] je nutné posudzovať tieto útoky podľa ich následkov v príčinnej súvislosti s konaním porušujúcim kód (software kyberpriestoru), technickú infraštruktúru, normy definičnej autority alebo štátu, resp. medzinárodnej organizácie. Tak ako postupom času v rímskom práve dospela právna náuka pri posudzovaní škody z priameho pôsobenia na vec analogickým výkladom k pôsobeniu nepriamemu a dokonca ku škode bez telesného pôsobenia na vec, je nutné dospieť k tomu, že aj virtualizované bezprávne konanie kyberútočníka (*virtual iniura*) môže byť príčinou vzniku škody, resp. škodlivého následku.[290] Podľa Mačáka *„to, či zničenie tisícov centrifúg v iránskom nukleárnom zariadení, a teda závažnú škodu na infraštruktúre, USA a Izrael spôsobili riadenými raketami, alebo počítačovým vírusom, je z medzinárodnoprávneho hľadiska irelevantné.“* [291] Avšak k dôslednému záveru o virtualizovanom bezprávnom konaní útočníka je možné dospieť len za predpokladu posúdenia jeho úmyslu. Totiž existujú útoky bez zjavnej škody (napr. estónsky útok bez hmotnej škody v roku 2007), avšak s úmyslom takúto škodu spôsobiť. S tým rovnako súvisí aj otázka pričitateľnosti tohto konania (*attribution*). Podobne ako u vojakov, agentov alebo iných osôb poverených štátom k použitiu sily proti inému štátu, bude kyberútok pričítaný tomu štátu, ktorý bol na začiatku reťaze kauzálnej súvislosti medzi jeho konaním a škodným následkom v kyberpriestore.

V teórii sa rozlišujú tri základné modely klasifikácie kybernetických útokov: [292]

[289] DORR, O. Use of Force, Prohibition of, Max Planck Encyclopedia of Public International Law [MPEPIL]. [online]. [cit.1.9.2020]. Dostupné z: Dostupné z: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e427?rskey=4C8VMG&result=1&prd=EPIL

[290] BARTOŠEK, Milan. 1981. Encyklopedie římského práva. Praha: Panorama. Pyramida (Panorama). Str. 125.

[291] MAČÁK, K. Kyberútok: ilegalita jednotiek a núl. SME.sk. zo dňa 5. jún 2012. [online]. [cit.1.9.2020]. Dostupné z: http://komentare.sme.sk/c/6405738/kyberutok-ilegalita-jednotiek-a-nul.html

[292] CARR, J. Inside cyber warfare. Sebastopol, Calif.: 2010. O'Reilly Media, Inc. ISBN 05-968-0215-3. Str. 59.

- *prvý model skúma, či by spôsobená škoda mohla byť spôsobená kinetickým útokom ako tomu je v klasickej vojne (instrument-based approach),*
- *druhý model je spojený s následkom (effects-based approach), kde sa skúma iba výsledný efekt útoku na základe kaskády príčinných súvislostí, a*
- *tretí model uvažuje o prísnej zodpovednosti, kde každý útok voči kritickej infraštruktúre je automaticky chápaný ako ozbrojený útok, a to z pohľadu možných následkov (strict liability approach).*

Pre potreby tejto práce sa stotožníme s druhým modelom, ktorý hľadá kaskádu príčinných súvislostí medzi útokom a škodou. Za splnenia vyššie uvedených podmienok (virtualizované bezprávné konanie útočníka, hrozba alebo poškodenie virtualizovaných záujmov, úmysel útočníka a pričitateľnosť, resp. príčinná súvislosť medzi konaním útočníka a následkom) môže štát pristúpiť k výkonu práva na sebaobranu v kyberpriestore, a to aj vtedy, ak nie je zrejmé, na ktoré konkrétne miesto sa fyzicky útoky viažu alebo z ktorého miesta vychádzajú, ak však pozná útočníka. Aby bolo možné vykonať obranu, musí ísť o primeranú sebaobranu. Hľadisko primeranosti je nutné posudzovať v každej veci samostatne.[293] Môžeme uzavrieť, že možnosť štátu vykonať právo na sebaobranu v kyberpriestore je podstatnou náležitosťou jeho informačnej suverenity. Preto sa je možné domnievať, že ak štát disponuje možnosťou vykonať právo na sebaobranu v kyberpriestore, rovnako disponuje právom získavať alebo vyťažovať elektronické dôkazné prostriedky od cudzích definičných autorít v prípade útoku alebo v prípade jeho predchádzaniu. Tento úkon môže mať podobu hrubej sily (napr. hackerského proti-útoku s úmyslom vyťažiť čo najviac dát svedčiacich o protiprávnom konaní) alebo získania dôkazných prostriedkov na základe dohody od tretieho štátu, resp. definičnej autority. Domnievame sa, že hľadisko primeranosti je rovnako aktuálne a je ho nutné aplikovať aj vo veci získavania dôkazov v prípade, ak nepôjde o kyberobranu. Takýto proces sa

[293] Napríklad útok prostredníctvom vírusu Stuxnet v iránskych jadrových centrifúgach dozaista už netrvá. Podľa Mačáka *"ak by však Irán mal o jeho trvaní dôkazy, jeho reakcia v sebaobrane by nesmela presiahnuť intenzitu nevyhnutnú a primeranú na zastavenie a odvrátenie útoku."* Ibid. MAČÁK.

formuje pomocou medzinárodných dohôd alebo regulácii.[294] Napr. štát v prípade vyšetrovania trestného činu môže požiadať iný štát o právnu pomoc, čo má opodstatnenie v medzinárodnej zmluve o právnej pomoci. Ak zmluva o právnej pomoci neexistuje alebo ju nie je možné dodržať, môže využiť princíp reciprocity a vlastný právny poriadok o cezhraničnej spolupráci. Avšak vidíme, že tieto klasické inštitúty medzinárodného práva sú nepostačujúce. Elektronické dôkazy sú často delokalizované (bez vzťahu ku konkrétnemu teritóriu). Podľa Kasselovej *„jednostranné rozšírenie jurisdikcie mimo vlastných územných hraníc nie je zriedkavým javom a snaží sa o ňu väčšina krajín, najmä vo vzťahu k trestným veciam.“*[295] Odborná prax potvrdzuje, že princíp teritoriality dát ustupuje do pozadia a faktická kontrola dát sa stáva centrálnym princípom legislatív, ktoré majú ambíciu pôsobiť mimo teritória alebo jurisdikciu daného štátu. Sú nimi napríklad americký *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*[296] alebo návrh nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.[297]

Otázkou je, do akej miery sú tieto snahy ešte výkonom samostatnej suverenity alebo pristúpením k zdieľanej informačnej suverenite? Z teoretického hľadiska predstavuje súdna moc a rovnako jej časť v podobe výkonu dokazovania podstatnú náležitosť informačnej suverenity štátu. V prípade zdieľanej informačnej suverenity stráca štát výhradné právo a fakticky je limitovaný informačnou suverenitou iného štátu alebo definičnej autority. Domnievame sa, že práve v tejto časti musí štát (alebo spolok štátov) vyvinúť snahu o zmluvný rámec ohľadom výkonu práv dvoch alebo viacerých

[294] Viď napr. návrh nariadenia a smernice Komisie EÚ na vytvorenie právneho rámca, ktorý by policajným a súdnym orgánom uľahčil a urýchlil zabezpečovanie a získavanie prístupu k elektronickým dôkazom v cezhraničných prípadoch zo dňa 17.4.2018. Procedurálna zložka č. 2018/0107(COD) a 2018/0108(COD) [online]. [cit.1.9.2020]. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0107(COD)&l=en a https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108(COD)&l=en

[295] KESSELOVÁ, Katarína. Cezhraničný prístup k elektronickým dôkazom v trestných veciach. Visí vo vzduchu európsky Cloud act? Revue pro právo a technologie. č.19. 2019. Str. 41.

[296] H.R.4943 — 115th Congress (2017-2018). [online]. [cit.1.9.2020]. Dostupné z: https://www.congress.gov/bill/115th-congress/house-bill/4943

[297] Návrh nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

suverenít. Ide o spoluprácu medzi štátom a definičnou autoritou, kde obe strany akceptujú isté „pravidlá hry“ procesu dokazovania. V praxi by to znamenalo komunikáciu alebo dohodu o elektronickom dokazovaní medzi štátom a definičnou autoritou. V súčasnosti však vidíme len dobrovoľné, resp. transparentné podmienky stanovené definičnou autoritou o vydávaní vopred stanovených elektronických údajov cudziemu štátu na základe jeho žiadosti.[298] Domnievame sa, že v budúcnosti budú musieť štáty rovnako otvorene komunikovať svoje preferencie a podmienky pre získavanie dôkazných prostriedkov od cudzích definičných autorít. Cudzie definičné autority budú tieto návrhy prijímať alebo navrhovať zmeny, čím v zásade môže dôjsť ku dohode o zdieľaní informačnej suverenity.

3.5. Medzinárodná spolupráca vo veciach dokazovania v občianskych a obchodných veciach

Dokazovanie v občianskoprávnom konaní sa neobmedzuje iba na hranice jedného štátu. Niekedy môže byť potrebné vykonať dôkazy v inom štáte, ak sa tam takýto dôkazný prostriedok nachádza. V prípade výsluchu svedkov, znalcov alebo vykonania obhliadky, ako už bolo uvedené, štáty spoliehajú na medzinárodnú spoluprácu. Základným pilierom v súkromnom práve tu je medzinárodný dohovor o vykonávaní dôkazov v cudzine v občianskych a obchodných veciach zo dňa 18. marca 1970 uzavretý v Haagu na XI. zasadaní Haagskej konferencie o medzinárodnom práve súkromnom.[299] Dohovor ustanovuje rámcové spôsoby spolupráce medzi 63 zmluvnými štátmi vo veciach cezhraničného dokazovania. Dohovor poskytuje účinné prostriedky v dvoch častiach. Ide o dokazovanie prostredníctvom žiadostí zvolených justičných orgánov jedného štátu voči orgánom iného štátu alebo dokazovanie

[298] Spoločnosť Google LLC, so sídlom v USA, dostáva mnohé žiadosti od štátnych orgánov pochádzajúcich mimo USA. Ako definičná autorita vytvorila vlastný právny rámec vydávania a poskytovania vyžiadaných údajov týmto štátnym orgánom. Sama spoločnosť sa zaväzuje poskytnúť údaje na dobrovoľnej báze. Hovorí, že môže poskytnúť informácie o používateľovi, ak je to v súlade s právom USA, právom žiadajúcej krajiny, čo znamená, že požaduje, aby sa orgán riadil rovnakým riadnym procesom a zákonnými požiadavkami, ktoré by sa uplatňovali, keby bola žiadosť podaná miestnemu poskytovateľovi podobnej služby, rovnako v súlade medzinárodným právom a pravidlami spoločnosti Google. Viď Google Transparency Report. [online]. [cit.1.9.2020]. Dostupné z: https://policies.google.com/terms/information-requests

[299] Vyhláška č. 129/1976 Sb. ministra zahraničních věcí o Úmluvě o provádění důkazů v cizině ve věcech občanských a obchodních v znení sdělení č. 68/2014 Sb. m. s. Ministerstva zahraničních věcí, kterým se vyhlašuje oprava českého překladu Úmluvy o provádění důkazů v cizině ve věcech občanských nebo obchodních, vyhlášené pod č. 129/1976 Sb.

pomocou diplomatických alebo konzulárnych úradníkov.[300] Justičný orgán zmluvného štátu podľa vlastných právnych predpisov žiada od príslušného orgánu iného zmluvného štátu, aby bol vykonaný dôkazný prostriedok alebo iný súdny úkon. Dožiadanie okrem iných náležitostí obsahuje povahu konania, v ktorom sa o vykonanie dôkazu žiada, s uvedením všetkých potrebných skutočností a popis požadovaného dôkazu alebo iných súdnych úkonov, ktoré sa majú vykonať. V zmysle čl. 9 veta prvá tohto dohovoru, *„justičný orgán, ktorý dožiadanie vykonáva, použije, pokiaľ ide o procesný postup, právo svojho štátu.“* Možno sa pýtať, čo v prípade, ak vykonávajúci štát nepozná formu dôkazného prostriedku, ktorá je žiadaná? V zmysle čl. 9 veta druhá dožiadaný justičný orgán vyhovie takémuto prianiu (aby sa postupovalo podľa osobitnej formy), s výnimkou ak by táto forma nebola zlučiteľná s právnym poriadkom dožiadaného štátu, alebo ak by jej použitie nebolo možné buď s ohľadom na súdne zvyklosti dožiadaného štátu alebo pre ťažkosti v praxi. Dohovor ponúka rovnako riešenie pomocou vykonávanie dokazovania prostredníctvom diplomatických zástupcov, konzulárnych úradníkov a komisárov (čl. 15). Je potrebné mať na pamäti, že v zmysle čl. 1 veta druhá, dožiadaním nemožno žiadať o vykonanie dôkazu, ktorý nie je určený na použitie v súdnom konaní, ktoré sa koná alebo bude konať.

Dohovor nešpecifikuje typ dôkazných prostriedkov. Čo sa týka elektronického dokazovania, prax dohovoru ukázala, že s elektronickým dôkazným prostriedkom (dáta) sa nakladá ako s listinným dokumentom. Navyše v apríli 2020, stály úrad pri Svetovej organizácii pre cezhraničnú spoluprácu v občianskych a obchodných veciach publikoval kvalitný manuál, t.j. osvedčené postupy pri používaní videolinku, resp. videokonferencie pre vykonávanie dôkazných prostriedkov a výsluchov svedkov na diaľku.[301] Táto inštrukcia prišla v začiatkoch pandemickej krízy COVID-19, kedy sa vykonávanie dôkazov na diaľku začalo stávať nutnosťou. Videolink označuje technológiu, ktorá umožňuje vzájomné prepojenie dvoch alebo viacerých vzdialených miest *„obojsmerným prenosom videa a zvuku, čo uľahčuje komunikáciu a osobnú interakciu medzi týmito miestami. Pretože sa táto prax postupne zavádzala do procesných právnych predpisov, ako aj do mechanizmov cezhraničnej právnej*

[300] Outline of the Convention. HCCH. [online]. [cit.1.9.2020]. Dostupné z: https://www.hcch.net/en/instruments/conventions/specialised-sections/evidence

[301] Guide to Good Practice on the Use of Video-Link under the Evidence Convention. The Hague Conference on Private International Law – HCCH Permanent Bureau. 2020. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/docs/569cfb46-9bb2-45e0-b240-ec02645ac20d.pdf

spolupráce, boli vyvinuté rôzne právne definície.“[302] Je zrejmé, najmä v prípade klasického výsluchu, že videolink je stará technológia, ktorá bola používaná justičnými orgánmi najmä v prípadoch nutnosti výsluchov na diaľku, za sťažených podmienok (napr. osoba vo výkone trestu) alebo v prípade výsluchov utajených svedkov. Videolink v sebe stelesňuje prostriedok tradičného „real-time“ výsluchu s možnosťami využitia plného elektronického dokazovania elektronickým konferenčným systémom (napr. nahrávanie a zaznamenanie videokonferencie, posielanie a preberanie elektronických súborov, púšťanie prezentácii, oboznamovanie sa s webstránkami v priamom prenose). Prekonaním vzdialenosti medzi súdom, účastníkmi konania, ich zástupcami a akýmikoľvek svedkami má videolink potenciál šetriť čas, náklady a environmentálne dopady cestovania do miest výsluchov alebo vykonania dôkazov. Pozitívom je, že mnoho zmluvných strán dohovoru tento manuál privítalo a nevidelo právne alebo technické prekážky v použití videolinku vo svojom štáte.

Úlohou dohovoru je taktiež prekonávať rozdiely medzi systémami kontinentálneho práva a anglo-amerického práva v oblasti dokazovania. Neschopnosť naplniť tento cieľ sa plne ukázala v otázkach anglo-amerického pohľadu na *discovery*, kde súdy zastrešujúce tento inštitútu často prekračujú hranice štátu.[303] Závery a odporúčania osobitnej komisie z roku 2009 o praktickom fungovaní dohovoru boli, že je *„pravdepodobné, že sa zvýši počet žiadostí o discovery v súvislosti s elektronicky uloženými informáciami, a odporúča, aby sa s týmito požiadavkami zaobchádzalo rovnako ako so žiadosťami o listinné dokumenty.“*[304] Je však zaujímavosťou, že v zmysle čl. 23 dohovoru každý štát *„môže pri podpise, ratifikácii alebo prístupe vyhlásiť, že nebude vykonávať dožiadania, ktorých predmetom je konanie známe v štátoch oblasti Common Law pod označením „pre-trial discovery of documents.“*

[302] Ďalšie pojmy, ktoré sa bežne používajú na opísanie tohto postupu, zahŕňajú „videokonferencie“, „vzdialené vystupovanie“ alebo „prítomnosť vo videu“. Ibid. Guide to Good Practice on the Use of Video-Link under the Evidence Convention. Str. 15.

[303] Viď rozhodnutie Najvyššieho súdu Spojených štátov vo veci Société Nationale Industrielle Aérospatiale proti Okresnému súdu Spojených štátov pre južný okres Iowa, kde Najvyšší súd jednomyseľne rozhodol, že dohovor o vykonaní dôkazov nie je „povinný“ (*is non-mandatory*). Societe Nationale Industrielle Aerospatiale and Societe de Construction d'Avions de Tourisme, Petitioners v. United States District Court for the Southern District of Iowa 107 S.Ct 2542. [online]. [cit.1.9.2020]. Dostupné z: https://www.law.cornell.edu/supremecourt/text/482/522

[304] Conclusions and Recommendations of the 2009 Special Commission on the practical operation of the Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions. HCCH. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/upload/wop/jac_concl_e.pdf

Doposiaľ však existuje nepochopenie týkajúce sa prepojenia anglo-amerického právneho systému v otázkach *discovery* a kontinentálného právneho systému. Išlo o namietanú exkluzivitu dohovoru a možnosť využitia procesu *discovery* mimo tento dohovor.[305]

Východiská medzinárodnej justičnej spolupráci pre Európsku úniu je možné nájsť v čl. 81 ods. 1 písm. a) a c) ZFEÚ. Ten ukladá Európskemu Parlamentu a Rade úlohu prijímať opatrenia zamerané na zabezpečenie vzájomného uznávania a výkonu rozsudkov a zlučiteľnosti vnútroštátnych právnych predpisov s ohľadom na kolízie právnych predpisov a rozhodnutí súdov. Pre zrýchlenie spolupráce medzi súdmi členských štátov Európskej únie prijala Rada 28. mája 2001 Nariadenie (ES) č. 1206/2001 v oblasti dokazovania v občianskych a obchodných veciach. [306] Nariadenie je vykonateľné vo všetkých členských štátoch Európskej únie s výnimkou Dánska. Nariadenie zavádza dva spôsoby vykonávania dôkazov: vykonanie dôkazu dožiadaným súdom a priame vykonanie dôkazu dožadujúcim súdom. Obdobne Európska únia identifikovala nutnosť používania videolinku ako jeden z hlavných nástrojov na získavanie dôkazov na diaľku pri výsluchoch svedkov.[307]

3.6. Zhrnutie kapitoly

V kapitole sme predložili základy suverenity štátu, jej formovanie v kyberpriestore a následný vplyv takejto suverenity na výkon súdnej moci, resp. elektronického dokazovania. Na príklade zdieľanej informačnej suverenity sme demonštrovali, že kyberpriestor oslabuje teritoriálnu výkonnú moc štátu voči virtualizovaným subjektom a núti štát spolupracovať s definičnou autoritou. V kapitole sme sa snažili porovnať právo štátu na sebaobranu so súdnou mocou, resp. právom získavať alebo vyťažovať elektronické dôkazne prostriedky v kyberpriestore. Úvaha mala za cieľ vysvetliť, že štát si oslabenie svojej suverenity kompenzuje buď zdieľanou suverenitou (spolieha sa

[305] Stretnutia osobitnej komisie Haagského dohovoru v rokoch 2003, 2009 a 2014 objasnili povahu a účel tohto postupu a vyzvali štáty, ktoré vydali všeobecné, nekonkrétne vyhlásenia, aby tieto prehodnotili. Pre-trial discovery (Art. 23). HCCH Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/docs/ec1fc148-c2b1-49dc-ba2f-65f45cb2b2d3.pdf

[306] Nariadenie Rady (ES) č. 1206/2001 z 28. mája 2001 o spolupráci medzi súdmi členských štátov pri vykonávaní dôkazov v občianskych a obchodných veciach.

[307] Videokonferencia ako súčasť európskej e-spravodlivosti: základy videokonferencie v cezhraničných konaniach. 2009. [online]. [cit.1.9.2020]. Dostupné z: https://e-justice.europa.eu/fileDownload.do?id=f26030b3-ae25-4d08-825f-05152d7bb772

na inú autoritu) alebo autoritatívnym obmedzením kyberpriestoru (napr. cenzúrou). Stranou však neostali ani klasické možnosti medzinárodného práva. Preto sme kapitolu uzavreli exkurzom do medzinárodnej úpravy cezhraničného dokazovania. Domnievame sa, že budúcnosť cezhraničného dokazovania patrí veľmi potrebnému spôsobu vykonania dôkazného prostriedku na diaľku - videolinkom, resp. videokonferenciou. Ide o veľmi vhodný príklad virzualizácie procesného inštitútu dokazovania, ktorý rieši ako vykonať vzdialený dôkazný prostriedok pomocou technológie. Či už pôjde o vzdialený výsluch alebo celé súdne pojednávanie, zdá sa, že tento typ hybridného dôkazu ponúka rôznorodé možnosti ako narábať s elektronickým dôkazným prostriedkom alebo ako pristupovať k elektronickému súdnemu spisu.[308]

Je možné zhrnúť, že tak ako štát, ktorý nedokáže postihnúť alebo predchádzať virtuálnym útokom a chrániť práva občanov v kyberpriestore, aj štát, ktorý nie je schopný spolupracovať alebo zaobstarať si elektronické dôkazné prostriedky z kyberpriestoru, stráca informačnú suverenitu a prestáva plniť jednu z podstatných funkcií spoločenského zriadenia. Preto je v jeho záujme vyhľadávať zmysluplnú koordináciu a spoluprácu s definičnými autoritami.

[308] COVID-19 and the global approach to further court proceedings, hearings. Norton Rose Fulbright. [online]. [cit.1.9.2020]. Dostupné z: https://www.nortonrosefulbright.com/de-de/wissen/publications/bbfeb594/covid-19-and-the-global-approach-to-further-court-proceedings-hearings

4. Počítač ako sudca*

4.1. Úvodne poznámky

Len pred pol storočím Norbert Wiener vydal svoju zásadnú prácu s názvom Kybernetika alebo veda o riadení a komunikácií v živých organizmoch a strojoch.[309] Wiener tak popísal základy novej vedy, ktorá sa stihla penetrovať do mnohých vedných odborov, a to vrátane práva.[310] Totiž bez informácie nie sú mysliteľné organizované systémy, či už živé organizmy v prírode alebo riadiace systémy vytvorené človekom, a to vrátane právneho systému.[311] Nasledujúca kapitola sa bude zaoberať vplyvom kybernetiky a informačných technológií na rozhodovaciu činnosť sudcu. Ako názov predurčuje, predmetom bude posúdenie možných podmienok pre vytvorenia stroja na právo, čo bolo s obľubou v päťdesiatych rokoch minulého storočia označované ako jurimetrika.[312] Tak ako iné vedné odbory aj právo čelí novým výzvam automatizácie a využitia vedeckých poznatkov umelej inteligencie. Už nie je možné zatvárať oči pred vplyvom informačných technológií a je nutné si položiť otázku, či môže počítač nahradiť ľudskú činnosť, akou je súdenie sporov, resp. rozhodovanie o dôkazoch?

* Táto kapitola vychádza z publikovaného článku ABELOVSKÝ, Tomáš. Počítač ako sudca. Revue pro právo a technológie, Masarykova univerzita, 2016, roč. 7, č. 14, ISSN 1804-5383. Str. 25-44.

309 WIENER, N. Cybernetics: or Control and Communication in the Animal and the Machine. 2.edition. Quid Pro Books, 2013.

310 Ibid. POLČÁK, R. Internet a proměny práva. Str. 18 an.

311 Hlavná myšlienka kybernetiky sa odvíja od postavenia a úlohy informácie. Klasická predstava sveta, ktorého základnými zložkami sú hmota a energia, musela ustúpiť predstave, že svet pozostáva ešte z ďalšej formy, ktorou je informácia. Je dôležité poznamenať, že Wiener nestal sám za zrodom kybernetiky ako takej. Jeho dielo má zásluhu na popísaní a ukotvení základných princípov tohto vedného odboru. Avšak francúzsky výraz *cybernétique* bol po prvýkrát použitý už v roku 1834 fyzikom André-Mariom Ampérom v rozsiahlej práci Eseje o filozofii vied. Každému známemu vednému odboru určil vo svojom systéme špecifické miesto. Kybernetiku podradil pod politiku. Označenie kybernetika prevzal z gréckeho jazyka, kde pojem kybernés značí kormidelník, nakoľko v starovekom Grécku predstavovala kybernetika vedu o riadení lodí. Čo je zaujímavé, pripojil k nej latinské veršované motto *et secura cives ut pace fruantur* (a zabezpečuje občanom, aby užívali mier). Viď PEKELIS, V. Malá encyklopédia kybernetiky. Bratislava: Mladé Letá, 1981, Str. 165. alebo AMPÉRE, A. Essai sur la philosophie des sciences ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines. Bachelier, Libraire-éditeur. Paris, 1834. Str. 141. In: [online]. [cit.1.9.2020]. Dostupné z: http://gallica.bnf.fr/ark:/12148/bpt6k110453h

312 BOBEK, M. MOLEK, P. ŠIMÍČEK, V. a kol. Komunistické právo v Československu: kapitoly z dějin bezpráví. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009, Str. 170.

4.2. Sudca človek

4.2.1. Rozhodovacie procesy

Možné nahradenie sudcu počítačom vyvoláva právne, technické, ale aj filozofické otázky. Ide o paradoxnú situáciu. Na jednej strane človek nie je schopný vyčerpávajúcim spôsobom popísať celé platné právo, avšak vie sa priblížiť k splneniu tejto úlohy práve pomocou výpočtovej technológie. Počítač je schopný manipulovať s každým právnym predpisom, súdnym rozhodnutím alebo iným právnym textom s nekončiacim radom funkcionalít. Inak povedané, počítač vie bezpochyby obsiahnuť celé písané právo.[313] No na druhej strane počítač má problém samostatne rozpoznať základné hodnoty chránené právom a nemôže dosiahnuť mentálny stav človeka sudcu, ktorý premýšľa o povahe prípadu a hodnotí vykonané dôkazy. Je na mieste otázka, či si z digitálnej pamäte vedia vyvodiť také postupy, ktoré sú podobné sudcovskej práci vedúcej k vydaniu rozhodnutia? Inak povedané, vie počítač hľadať právo?

Či už použijeme štatistické, pravdepodobnostné alebo iné metódy umelej inteligencie, odpoveď na túto otázku sa musí niesť v duchu, že pri rozhodovaní nejde ani tak o textovú pamäť, ako o schopnosť aplikovať platné právo a navyše vedieť aplikovať hodnoty, princípy alebo zásady vlastné každému právnemu systému. Ide o hľadanie živých interakcií medzi informáciami o práve a faktoch prípadu (*questio facti*), a to aj na základe predchádzajúcich skúseností sudcu, ktoré nemôžu byť nahradené vlastnosťami počítačového programu.[314] Aby sme túto činnosť vedeli správne pochopiť, musíme nazrieť do teoretických základov právotvorby a sudcovského rozhodovania.

Boguszak rozlišuje dve štádia prípravy rozhodnutí: (1) zistenie (zhromaždenie a spracovanie) vstupných informácií a (2) hodnotenie (axiologické štádium). Podľa

[313] Je na mieste sa spýtať, koľko platných právnych predpisov v Českej, resp. Slovenskej republike je vôbec možné identifikovať? Portál zakonyprolidi.cz uvádza v súčasnosti vyše 8900 platných právnych predpisov. Počet účinných ustanovení právnych predpisov v ČR sa v roku 1990 pohyboval na úrovni okolo 500 tisíc a v roku 2010 bol na úrovni 1,5 milióna. Viď BOHÁČ, R. Legislativní proces: (teorie a praxe). Praha: Tiskárna Ministerstva vnitra, 2011. Str. 234.

[314] Podobný názor zastáva Ronald Allen, ktorý uvádza, že *„každý, kto rozhoduje (o prípade), má vlastné osobitné charakteristické presvedčenie, nakoľko žiadny dvaja ľudia nežijú rovnaký život.“* Viď ALLEN, R. Artificial intelligence and the evidentiary process: The challenges of formalism and computation. Artificial Inteligence and Law 9: 99-114, 2001. Kluwer Academic Publisher. Printed in Netherlands. Str. 103.

tohto delenia je možné uviesť, že zber nenormatívnych (faktografických) a normatívnych informácií je možné plne zautomatizovať.[315] Ako bude ďalej uvedené, automatizáciu je možné demonštrovať na elektronickom dokazovaní počítačom. Ale meritórna problematika vzťahujúca sa k axiologickému štádiu je kameňom úrazu automatizovaného rozhodovania. Odpoveďou môže byť teória systémov. Prináša zaujímavé možnosti kategorizácie procesov rozhodovania. Rozlišuje uzavretý (bez možnosti externej komunikácie) a otvorený proces. Práve pri uzavretom procese je možné na rozdiel od otvoreného procesu konštatovať, že všetky premisy potrebné pre rozhodnutie sú v ňom pevne dané. Uzavreté procesy sú preto programovateľné. Podľa Boguszaka je programovateľnosť daná konečným počtom možných kombinácií a väzieb. Dodáva, že *„povaha axiologického štádia prípravy rozhodnutia záleží na miere uzatvorenosti a na miere, v akej je proces programovaný.“* [316] Toto konštatovanie je pritom vlastné aj možnostiam počítačového rozhodovania. Čím je proces otvorenejší a jeho závislosť je vyššia na neznámych premenných, tým sa zvyšuje moment právneho uváženia o hodnotách, ktoré je spoločnosť rozhodnutá chrániť. V súčasnom stave technológií je menšia pravdepodobnosť, že počítač popíše všetky premenné a priblíži sa k uzavretému procesu. K tomu sa však nevie priblížiť ani človek, ale kompenzuje tento deficit tým, že vie identifikovať relevantné hodnoty založené na morálke dobra a zla.

Na tomto mieste je však ešte potrebné spomenúť aktuálnu právnu diskusiu o formalizácii rozhodovacích procesov. Araszkiewicz pracuje s kategóriou interpretačných výrokov a dospel k názoru, že v prípade formálneho modelovania a programovania pozitívneho práva (jazyka) je nutné sa sústrediť na miesto zákonného textu práve na interpretačné výroky, ktoré vytvoria (reprezentujú) vedomostný základ (*knowledge base*). [317] Na druhej strane Sartor poukazuje na využitie robustnej teoretickej konštrukcie teleologického odôvodnenia a proporcionality v legislatíve

[315] Ibid. BOGUSZAK, Str. 244.

[316] Ibid. BOGUSZAK, Str. 246.

[317] ARASZKIEWICZ, M. Towards Systematic Research on Statutory Interpretation in AI and Law. Frontiers in Artificial Intelligence and Applications. Ebook. Volume 259: Legal Knowledge and Information Systems. Str. 29. [online]. [cit.1.9.2020]. Dostupné z: http://ebooks.iospress.nl/publication/35595.

a rozhodovacích procesoch, a to práve pre systémy umelej inteligencie.[318] Praktické výstupy priniesol aj výskum Šavelku a Asheleyho o možnosti využitia technológie pri interpretácii a chápaní právnej terminológie. Pozoruhodné sú tu otázky predikcie interpretačnej užitočnosti právnej vety za použitia počítačových algoritmov.[319]

Rozhodovanie sudcu je primárne vystavané na dokazovaní. Pri každom dokazovaní po získaní požadovanej informácie pristupuje logická operácia. Tá podraďuje skutkovú (dejovú) podstatu pod zodpovedajúcu právnu normu. Môžeme hovoriť, že súčasťou aplikácie práva je práve táto operácia. Je dôležité, ako priliehavo bude zvolená právna norma. Táto musí zodpovedať tomu, čo sa udialo a čo bolo preukázané, teda existujúcej skutkovej podstate. Výsledkom by mala byť vždy korektná aplikácia práva a následne rozhodnutie. Ako sme už uviedli, poznanie v podobe zistenia materiálnej pravdy, ktoré dosahuje sudca v rámci súdneho konania, nie je a ani nemôže byť absolútnym poznaním.[320] Má pravdepodobnostný charakter určitej kvalitatívnej úrovne, ktorá je totožná s praktickou istotou. Ide o psychologicko-praktickú hranicu poznania sudcu. Podľa Holländera samotné približovanie k nie celkom presným hraniciam pravdy nič nemení na noetickej analýze procesu dokazovania. [321] Je možné uzavrieť, že psychologicko-praktická hranica poznania sudcu je zásadný znak vlastný sudcovskému rozhodovaniu.

4.2.2. Individuálnosť a náhodilosť rozhodovania

Ďalší zo znakov sudcovského rozhodovania je jeho individuálnosť. Podľa Dworkina sú v anglo-americkom právnom systéme profesionálni sudcovia vyškolení k trom základným zručnostiam. Vedia analyzovať zákony a odôvodnenia rozsudkov tak, aby z nich vedeli extrahovať tzv. právnu doktrínu. Taktiež sú vyškolení k analýze komplexných faktických situácií tak, aby vedeli presne sumarizovať zásadné

[318] SARTOR, G. Doing justice to rights and values: teleological reasoning and proportionality. Artificial Intelligence and Law. June 2010, Volume 18, Issue 2, Str. 175–215. [online]. [cit. 1.9.2020]. Dostupné z: http://link.springer.com/article/10.1007/s10506-010-9095-7

[319] ŠAVELKA, J., ASHELEY, K., Extracting Case Law Sentences for Argumentation about the Meaning of Statutory Terms. In Proceedings of the 3rd Workshop on Argument Mining. ACL, 2016, Str. 50-59. [online]. [cit. 1.9.2020]. Dostupné z: http://www.aclweb.org/anthology/W/W16/W16-28.pdf#page=62

[320] MACUR, Josef. Dokazovaní a procesní odpovědnost v občanském soudním řízení. Spisy Právnické fakulty University J.E.Purkyně v Brně ; svazek 56, Brno. 1984, Str. 69.

[321] Ibid. HOLLÄNDER, Pavel. Filosofie práva. Str. 201.

skutočnosti prípadu. A v neposlednom rade sú pripravení na to, aby mysleli takticky, čo má za následok navrhovanie takých rozhodnutí a právnych odôvodnení, ktoré prinesú partikulárne sociálne zmeny na základe predchádzajúceho uváženia.[322] Proces fungovania celej justície je komplikovaný systém, ktorý počíta s týmito zručnosťami sudcov. Navonok sa zdajú byť tieto jednotlivé zručnosti podobné automatizovaným úkonom (najmä v prípade tzv. *easy cases*). Ak sa však niekomu podarí vydestilovať to najlepšie z lorda Deninnga, Olivera Holmesa, R.B.Ginsburg alebo Antonia Scaliu a iných, je nutné, aby tento prototyp sudcu podstúpil ešte pred svojím prvým rozhodnutím test ľudskosti (najmä v prípade tzv. *hard cases*).

Individuálnosť dopĺňa prítomná náhodilosť v možnosti výberu vstupných premenných pre rozhodnutie, čo dotvára ľudský charakter rozhodovania. Rozhodovanie si vyžaduje okrem iného aj empirickú skúsenosť človeka, a to nie len z pohľadu sprievodných emócií, ale aj z pohľadu náhody. Tá sa môže taktiež prejaviť v podobe chyby alebo omylu. Chybovosť v správaní človeka na rozdiel od počítača predstavuje iracionálny aspekt každej ľudskej činnosti. Iheringovsky a trochu metafyzicky je možné dodať, že právo nie je pojem, ale živá sila. A prečo je dôležité toto korenie chýb v prípade súdneho rozhodovania? Okrem toho, že chyby sú v správaní človeka často dôvodom hľadania práva, resp. boja proti bezpráviu, umožňujú vidieť smer Iheringovej živej sily, smer približovania sa k morálnym ideálom (zásadám, hodnotám, princípom, základnému koreňu, morálke, Bohu atď.). Človek platí za ich poznanie vysokú cenu, avšak snaha spočívajúca v ich sústavnom prekonávaní prináša nové možnosti hľadania práva. Táto snaha stojí za nekončiacim výronom jurisprudencie. Iracionalita existencie chybového správania človeka prináša zaujímavý efekt spätnej väzby. Každá empirická skúsenosť spoločnosti s predošlými chybami modifikuje jej budúcu schopnosť sa ďalej správne rozhodovať. Tak ako ich prevážením, tak ich anulovaním, môže dôjsť k tomu, že spoločnosť stratí odstup od toho, čo je dôležité a neuvedomí si to, čo je zlé a dobré. A čo môže byť horšie ako to, keď sa trvajúci stav bezprávia interpretuje bezchybným strojom na rozsudky ako dokonalý poriadok?

[322] DWORKIN, R. Taking rights seriously. Cambridge: Harvard University Press, 1977, ISBN 0-674-86711-4. Str. 2.

4.3. Sudca počítač

Pre analýzu problému sudca počítač je potrebné objasniť spôsob jeho konfigurácie, t.j. či dokáže premýšľať. Ponúka sa tu jeden z mnohých sociálno-psychologických testov, ako nazerať na jeho myslenie. Diskvalifikačným kritériom pre počítač je otázka poznateľnosti morálnych hodnôt, resp. ich nakódovanie do systému počítača.

4.3.1. Mysliaci počítač

Zakladateľ odboru umelej inteligencie McCarthy je známy svojou provokatívnou otázkou: *„čo sudcovia vedia také, čo by sme nemohli povedať počítačom?"*[323] Ďalší z praotcov tohto odboru Minsky sa vyjadril, že ľudský mozog je vlastne len počítač z mäsa, čím prirovnal myslenie počítačovému spracovaniu dát v duchu Weinerovej kybernetiky.[324] V súvislosti s touto úvahou si je možné položiť základnú otázku, môže počítač myslieť? Je však vôbec možné uvažovať o tomto slovnom spojení? Podľa Maysa ide o kategórie, ktoré sú charakteristické výlučne pre človeka. Podľa jeho názoru *„zbytočne vzbudzujú naivné a idealistické predstavy o tom, že je stroj schopný uvažovať alebo rozhodovať."* [325] Predstava, že sudca človek by okrem najnevyhnutejších otázok a textu rozhodnutia nepovedal ani slovo, je odradzujúca. Kto by chcel takého sudcu? Tak ako sudca vie komunikovať pred svojím rozhodnutím a aj po ňom, súčasťou rozhodovacieho algoritmu počítača by mala byť aj časť so schopnosťou pýtať sa správne otázky v nadväznosti na faktické zistenia (*questio facti*) a podať výpoveď o svojom rozhodnutí (*questio iuris*). Inak povedané, mal by vedieť premýšľať a hovoriť o svojom rozhodnutí. Pripusťme, že existuje informačná technológia neurónových sietí, ktorá umožní simulovať ľudské myslenie. Má schopnosť sa učiť a rapídne rozširovať svoje poznatky a prepojenia neurónových konfigurácií. Je napojená na celosvetovú sieť a dokáže spracovať každú digitálnu informáciu. Ako zistíme, či táto technológia dosiahla ľudské schopnosti?

---

[323] GRABINER, J. Partisans and critics of a new science: the case of artificial intelligence and some historical parallels. History and philosophy of modern mathematics, Minnesota Stud. Philos. Sci., XI, Univ. Minnesota Press, Minneapolis, MN, 1988, Str. 329.

[324] WILLIAMS, P. The brain is just a computer made of meat. Science, Technology and Society. STAS Topic 3, [online]. [cit. 1.9.2020]. Dostupné z: http://www.technoid.net/uni/ai.doc

[325] MAYS, W. Can Machines Think?. Philosophy. 1952, vol. 27, issue 101, Str. 149. [online]. [cit.1.9.2020]. Dostupné z: http://www.journals.cambridge.org/abstract_S003181910002266X

4.3.2. Turingov test

V päťdesiatych rokoch sa pokúsil Joseph Weizenbaum nájsť odpoveď pomocou projektu autonómneho systému ELIZA (*chatbot*), ktorý v textovej podobe simuloval rogerianského psychoterapeuta (známeho pod názvom DOCTOR). Zaujímavosťou je, že jeho inteligencia bola obmedzená na algoritmus využívajúci reflexie stanovísk pýtajúceho sa pacienta (osoby, ktorá komunikovala prostredníctvom terminálu).[326] Išlo o pomerne úspešný pokus imitačnej hry – Turingového testu.[327] Tento test predstavuje návod, ako nájsť odpoveď na otázku, či je to mysliaci stroj alebo človek.[328]Analogicky je možné tento typ návodu aplikovať aj na skúmanie počítačového sudcu. V odbornej literatúre sa je možné stretnúť s množstvom oponentúr voči Turingovej metóde, ale za zmienku stojí práve stanovisko Moora, ktorý hovorí, že *„myslenie je spracovanie informácií pomocou metód, ktoré zahŕňajú rozpoznávanie, predstavivosť, vyhodnocovanie a rozhodovanie.“*[329] Zdá sa, že okrem predstavivosti sú súčasné počítače schopné uvedených činností. Otázkou ostáva, či sa dokážu v hĺbke myslenia vyrovnať človeku?

[326] HUTCHENS, J. How to Pass the Turing Test by Cheating. University of Western Australia. 1997. Str. 6. [online]. [cit.1.9.2020]. Dostupné z: http://www.csee.umbc.edu/courses/471/papers/hutchens.pdf

[327] Tento test popísal tridsaťosemročný Alan Turing vo svojej slávnej eseji. Esej obsahuje súhrn názorov a argumentov ohľadom umelej inteligencie strojov. TURING, A. Computing machinery and intelligence. Mind, 1950. 59, Str. 433. [online]. [cit.1.9.2020]. Dostupné z: http://www.loebner.net/Prizef/TuringArticle.html

[328] Turing navrhol metódu overenia mysliaceho subjektu a pokúsil sa vopred vyvrátiť deväť námietok. Esej sa na začiatku nestretla s pochopením a často bola radená do sci-fi literatúry. Podľa odborníkov na umelú inteligenciu nie je ani z dnešného pohľadu celkom jasné, prečo sa esej stala klasickým a večne citovaným dielom. Filip Tvrdý konštatuje, že *„Turingová predpoveď ohľadne budúcich úspechov počítačov v imitačnej hre sa ukázala mylnou, niektoré pasáže sú celkom nezrozumiteľné, v texte sa objavujú len málo zábavne pokusy o humor a autor si neláme hlavu s formálnymi požiadavkami vedeckej práce.“* Viď TVRDÝ, F. Turingův test. TOGGA, spol. s r.o., Praha, 2014. Str. 25.

[329] MOOR, J. An analysis of the turing test. Philosophical Studies. 1976, vol. 30, issue 4, Str.250.

Aby bolo možné posúdiť prípadnú rovnocennosť, je možné použiť práve Turingov test, ktorý predstavuje verifikovateľné kritérium pre posúdenie tejto otázky.[330] Išlo o skúmanie procesu súvisiaceho s rozhodnutím počítača. Je možné uviesť nasledujúci príklad Turingovho testu v súvislosti s počítačovým sudcom:

Počítač a človek súčasne zbierajú faktické informácie o prípade. Pýtajú sa na okolnosti prípadu a zisťujú nadväzujúce skutočností. Vykonávajú navrhnuté dokazovanie. Subsumujú dokázané skutky pod nájdenú právnu normu. Vydávajú rozhodnutia. Kontrolór má za úlohu zistiť, či vec rozhodol človek alebo počítač. Kontrolórovi sú predložené dve písomné odôvodnené rozhodnutia dvoch subjektov. V prípade, ak by kontrolór neodhalil, ktorý zo subjektov je počítač a tým nespochybnil jeho rozhodnutie, bude potrebné dospieť k záveru, že počítač - sudca prešiel Turingovým testom.

Je zrejmé, že najkomplikovanejšia časť bude subsumovanie skutkov (dát) pod správnu právnu normu, kde sa dostáva k slovu diskusia o kódovaní morálky. Ide taktiež o otázku normatívneho a faktického pôsobenia technológie na ľudské chovanie. [331] Mnohí autori (Lessig, Polčák, Hildebrandt, Brownsword) majú k faktickému pôsobeniu technológie na ľudské chovanie rôzne názory. Technológia definuje nové prostredie a ovplyvňuje chovanie zúčastnených subjektov (napr. formuje ich chápanie príkazov a zákazov, podieľa sa na definícii normatívnych systémov v kyberpriestore, umožňuje vznik novým definičným autoritám). Navyše, virtualizácia právnych vzťahov má vplyv na chápanie morálnych, resp. hodnotových otázok v práve.[332] Za zmienku tu stojí staršia anglo-americká diskusia o prirovnaní toho, že naprogramovaný počítač – sudca pripomína myslenie „úzkeho zákonného

[330] S jednoduchým Turingovým testom sa je možné stretnúť aj pri zadávaní tzv. CAPTCHA kódu na rôznych webstránkach. Jeho účelom je overenie, či na druhej strane je skutočne človek. Turingov test pozostáva z toho, že skúšajúci sa pýta dvoch respondentov otázky bez toho, aby ich videl. Jeden z respondentov je počítač. Komunikácia prebieha výlučne písomne. Ak skúšajúci nevidí rozdiel, resp. nevie zhodnotiť, ktorý z respondentov je človek, potom počítač prešiel Turingov test. Po prvýkrát počítač zvládol tento test úspešne až v roku 2014. Ruský systém Eugene simuloval 13-ročného chlapca. Komunikáciu hodnotili tri osoby a jednu z nich Eugene presvedčil, že je živý človek (teda 33% úspešnosť). Viď First Turing Test success marks milestone in computing history. In: Phys.org. [online]. [cit.1.9.2020]. Dostupné z: http://phys.org/news/2014-06-turing-success-milestone-history.html

[331] Ibid. POLČÁK, R. Str. 101 an.

[332] ABELOVSKÝ, T. Virtualizácia ako metóda riešenia spoločenských problémov. Právny obzor. Ročník 98. 2015. Str. 164.

pozitivistu.“ Toto prirovnanie sa však zdá byť chybné a prekonané. Detmold uvádza, že zástancovia *„pozitivizmu [Kelsen, H. L. A. Hart atď.] vidia sudcov ako počítače, ktoré sa riadia presne stanoveným programom.“* Poukazuje najmä na prípady jednoduchých káuz, kde sudca aplikuje právo na pár faktov, a to bez „morálneho záväzku.“ Demonštruje to na prípade existencie zákona, ktorý prikazuje popravu modrookých detí. Naprogramovaný sudca – Leviathan – by nerozlišoval osobitosti prípadu, a tak by vlastne zopakoval nacistické besnenie.[333]Aby bolo možné objektívne odpovedať na osobitosti prípadu, sudcovia musia požívať voľnosť a musia mať možnosť porušiť „program.“[334] Odpoveď na názor Detmolda prináša Susskind, ktorý sa pýta prečo dostatočne nepreukázal, či súdne rozhodnutia v sebe zahŕňajú aj morálny súd a či je vôbec v súčasnosti takáto počítačová analógia užitočná a žiadúca? Práve druhá teleologická námietka je podstatná. Najmä v prípade, ak nebolo vyvrátené, či počítač je schopný klasifikovať osobitosti súdneho prípadu (na ktoré poukázal Detmold). Je nutné uviesť, že trend technologického pokroku takéto vyvrátenie spochybňuje. To však neznamená, že v budúcnosti takýto dôkaz nebude možné predložiť.[335]

[333] DETMOLD, M. J. The Unity of law and Morality: A Refutation of Legal Posivism. London: Routledge & Kegan Paul, 1984. Str. 263 an.

[334] Hans Kelsen vo svojej Všeobecnej teórií noriem sa vysporadúva s otázkou, či sú právny princíp alebo právna zásada súčasťou právneho poriadku. Kelsen analyzuje prácu Jozefa Essera (Zásada a norma v sudcovskom vzdelávaní) a na rozdiel Essera prísne odlišuje princípy od právnych noriem a konštatuje, že *„tvorba právnych noriem je ovplyvnená aj inými faktormi, akými sú právne zásady (princípy) morálky, politiky alebo mravov, ako napr. záujmy určitých skupín, bez toho aby sa týmto záujmom prisudzoval právny charakter. […] Zásady morálky, politiky alebo mravov, ktoré ovplyvňujú právotvorného jednotlivca v jeho funkcii, sú – vedľa ostatných faktorov – motívy zákonodarcu, sudcu alebo správneho orgánu, a tieto sú – podľa pozitívneho práva – právne nezáväzné. Tieto princípy nemajú preto charakter právnych noriem. Ak nie je pojem právnej normy od pojmu právnej zásady zreteľné odlíšený, stierajú sa hranice medzi pozitívnym právom na jednej strane a morálkou, politikou a mravmi na strane druhej, čo si môžu želať len takí predstavitelia právnej vedy, ktorí nepovažujú za svoju úlohu až tak príliš poznávať pozitívne právo a objektívne ho popisovať, ale skôr (ďaleko viac) ospravedlňovať (legitimovať) jeho platnosť morálne¬politicky, alebo ho spochybňovať a takto pod vlajkou objektívneho právneho poznávania vykonávať vysoko subjektívne oceňovanie práva.“* Viď KELSEN, H. Všeobecná teorie norem. Preklad Milan Kubín. Masarykova univerzita, Brno. 2000. Str. 130. Viď taktiež Alexyho odmietnutie úzkeho zákonného pozitivizmu, keď uvádza, že *„tradičná viazanosť sudcu zákonom, táto nosná súčasť zásady deľby moci a tým i právneho štátu, je však v Základnom zákone modifikovaná formuláciou, podľa ktorej je aplikácia práva viazaná zákonom a právom."* In ALEXY, R.: Pojem a platnosť práva, Bratislava: Kaligram, 2009, ISBN 978-80- 8101-062-0. Str. 30.

[335] Je potrebné pripomenúť, že táto výmena názorov sa odohrala v roku 1984.

4.3.3. Počítač a hodnoty

Ani ten najlepší algoritmus umelej inteligencie nie je schopný rozlíšiť v čase rozhodnutia, ktoré preferencie určitých hodnôt sú na úkor iných hodnôt správne alebo nesprávne. Totiž ak by tento algoritmus využíval štatistickú alebo pravdepodobnostnú metódu na základe historickej skúsenosti (napr. priebežne hodnotená judikatúra), nezabránilo by to konfrontácii so situáciou bieleho miesta, kde by sa mala uplatniť zásada neprípustnosti *denegatio iustitiae.* Aby nedošlo k odopretiu spravodlivosti, musel by využiť jednu z metód umelej inteligencie, ktorou by bol schopný kreovať nové riešenie. Príkladom môže byť systém IBM Watson, ktorý pracuje s neštruktúrovanými informáciami, strojovým učením a pomocou kognitívnych algoritmov poskytuje odpovede na jednotlivé otázky.[336]

Je nutné upozorniť na aspekt kódovania hodnôt do počítača o tom, čo je dobré a čo je zlé. Definovanie týchto hodnôt by mohlo spôsobiť ich nepochopenie, resp. relativizovanie. Podľa Schelera *„človek sa odvoláva na hodnoty intuitívne, nakoľko majú charakter ideálneho bytia, čo určuje pomyselnú hodnotovú podobu sveta.“*[337] Inak povedané, nevolí si ich plánovite. Ako sa v histórii osvedčilo, relativizovanie niektorých hodnôt je krajne nebezpečné a je otázne, ako by počítač využíval intuíciu pomocou matematických výpočtov. Nie sú práve sloboda uváženia a nezávislosť tie najcennejšie výsady sudcu? Susskind uvádza, že *„počítače doposiaľ neboli naprogramované, aby preukázali morálne, náboženské, sociálne, sexuálne alebo politické preferencie, ktoré by boli podobné tým ľudským […] alebo aby ukázali kreativitu, zručnosť, individualitu, inováciu, inšpiráciu, intuíciu, sedliacky rozum, záujem o vonkajší svet, ako máme my ľudia a čo očakávame nie len jeden od druhého ako občania, ale aj od sudcov v ich verejnoprávnom pôsobení.“*[338] Susskind vyslovuje nádej možného pokroku v tejto oblasti a upozorňuje že výskum prostredníctvom štúdia umelej inteligencie sa len práve odštartoval. Čo je podstatné, Susskind uvádza, že výskum si nekladie za cieľ absolútne zautomatizovať celú justíciu, ale odvoláva sa na výrok klasika umelej inteligencie McCartyho, ktorý zastáva názor, že počítač *„bude*

[336] IBM Watson. Ibm.com. [online]. [cit.1.9.2020]. Dostupné z: https://www.ibm.com/watson

[337] OLŠOVSKÝ, Jiří. Slovník filozofických pojmů současnosti. 3., rozš. a aktualiz. vyd., v nakl. Grada 1. Praha: Grada, 2011, Str. 86.

[338] SUSSKIND, Richard. Transforming the law: essays on technology, justice, and the legal marketplace. 1. publ. New York: Oxford University Press, 2001. Str. 286 an.

vykonávať rudimentárnu formu právneho uváženia a bude predstavovať prostriedok, ako sa naučiť viac o vlastnom právnom odôvodnení prostredníctvom počítačových modelov.“ [339] Domnievame sa, že schopnosť počítačových systémov podporiť rozhodovanie súdov sa ukazuje ako opodstatnený spôsob zefektívnenia justičného systému.

4.4. Východiská v podobe podporného rozhodovania počítačom

Na problém sudca počítač je možné nazerať z pohľadu praktického využitia exitujúcej technológie. Tu je možné uviesť nenahraditeľnú úlohu počítača pri podpore rozhodovania. Táto úloha by mala byť viac podporovaná a skúmaná. Počítač je dobrým nástrojom ako predchádzať niektorým ľudským omylom. Ako príklad je možné uviesť proces elektronického dokazovania, resp. vykonávania dôkazných prostriedkov v elektronickej podobe.

4.4.1. Účel podporného rozhodovania počítačom

Ideálny vzor osoby sudcu sa snaží predchádzať ľudskej omylnosti. Avšak jedným dychom je potrebné dodať, že formálna bezchybnosť vyraďuje počítač z kategórie ľudskosti a stavia ho do roviny formy kódu, t.j. inštrukcií a príkazov. No na druhej strane Murphyho zákon hovorí, že chybovať je ľudské, ale robiť skutočne hanebné chyby, to už vyžaduje počítač. Chyby v rozhodnutiach súdov, resp. justičné omyly sú príznačné právnym systémom rôznych krajín a najčastejšie pripomínajú laickej verejnosti zraniteľnosť procesu individuálnej aplikácie práva, ktorá stojí a padá na profesnej kvalifikácií, morálnej a rozumovej vyspelosti osobnosti sudcu, resp. súdneho systému, v tom ktorom prípade.[340] Ide o paradoxnú situáciu. Bolo vyslovené, že počítač netrpí iracionálnou omylnosťou, a preto sa diskvalifikoval od možnosti plnohodnotného ľudského rozhodovania. Na druhej strane jeho neomylná presnosť má užitočný potenciál. Zdá sa, že informačné technológie môžu predstavovať brzdu

[339] Ibid. SUSSKIND, Richard. Transforming the law: essays on technology, justice, and the legal marketplace. Str. 286 an.

[340] Za justičný omyl sa v najširšom chápaní považuje dovŕšený (právoplatný) akt aplikácie práva, často v oblasti trestného práva, ktorý je s odstupom času považovaný za nespravodlivý, nakoľko bol vykonaný v hrubom rozpore s platným právom (*contra legem*) a často je znakom zlyhania justičného systému, ktorý mal garantovať spravodlivý súdny proces. V užšom chápaní justičný omyl predstavuje objektívnu kategóriou vzťahujúcu sa k výkonu súdnej moci ako takej, spočívajúcou najmä v chybnom posúdení skutkového stavu (*questio facti*) alebo právnych otázok (*questio iuris*). Viď BOHM, R. M. Miscarriages of Criminal Justice: An Introduction. Journal of Contemporary Criminal Justice. 2005, vol. 21, issue 3, Str. 196.

justičných omylov a dopĺňať ľudské schopnosti o analýzy v oblastiach, akými sú forenzné technológie alebo analýzy rizík. Medzi nesystémové príčiny justičných omylov sú najčastejšie radené nesprávne posudky vypracované odbornými znalcami. Niekedy sa stáva, že sudcovia delegujú zodpovednosť za odborné otázky na znalcov, ktorí neraz hľadajú odpovede aj na právne otázky.[341] A práve týmto otázkam je nutné venovať pozornosť aj z pohľadu počítačových systémov umelej inteligencie. Ide o predchádzanie chýb a v podstate o porozumenie rizík vykonaných dôkazov. Totiž v niektorých prípadoch počítač dokáže lepšie, presnejšie a hlavne efektívnejšie vyhodnotiť otázky faktov.

4.4.2. Príklady podporného rozhodovania počítačom

Medzi možné podporné rozhodovanie počítačom patrí proces elektronického dokazovania, a to za podpory autonómnych systémov umelej inteligencie. Ide o obmedzený okruh pôsobnosti prostredníctvom informačných technológií, kde počítač pôsobí podporne a poskytuje sudcovi človeku zásadnú bázu vedomostí a odpovede na niektoré faktické otázky. Príkladom môže byť plne automatizovaná identifikácia fotografií s protiprávnym obsahom (napr. trestné činy súvisiace s výrobou, rozširovaním a prechovávaním detskej pornografie) vykonávaná algoritmom umelej inteligencie, ktorá sa v súčasnosti využíva na úrovni znaleckého dokazovania. Podporné rozhodovanie počítača v oblasti elektronického dokazovania je možné demonštrovať na týchto prípadoch:

- Počítač vykoná (spracuje) elektronický dôkazný prostriedok (dátový nosič alebo cloudove úložisko po získaní prístupu) a vydá písomný záznam o skutkových zisteniach. Tento písomný záznam nahradí vykonávanie dôkazu prostredníctvom znaleckého dokazovania v súdnom procese. Navyše, počítač vykoná prevenčnú funkciu zistenia a odstránenia hroziacej ujmy.
- Počítač zistí, že skúmaný dátový nosič obsahuje stopy po prepojení (alebo kopírovaní) dát na iné samostatné zariadenie, ktoré by bez ďalšieho predstavovalo ďalší predmet zaistenia. V takomto prípade by mohol počítač samostatne vydať a

[341] Byť opatrný pri znaleckom dokazovaní zdôrazňoval Otakar Motejl, ktorý bez servítky vyslovil, že *„soudní znalci ničí lidské životy! Případy, kdy soudní znalci pochybili, mívají často za následek zpackaný lidský život, jejich odpovědnost je ale téměř nulová“* Viď UHLÍŘ, A. Soudní znalci ničí lidské životy: aneb o neschopnosti Ministerstva spravedlnosti ČR vyřešit letitý problém. Britské listy. [online]. [cit.1.9.2020]. Dostupné z: http://blisty.cz/art/57881.html

doručiť návrh na zaistenie dôkazu podľa dostupného technického identifikátora, odôvodnené týmto technickým zistením. Predišlo by sa tak zbytočnej strate času alebo ľudskému zlyhaniu.

- Ak pôjde o dostupné dáta v cloudovom úložisku, počítač vykoná automatické zablokovanie alebo zaistenie sporných dát autonómnym spôsobom. Počítač by vykonal elektronický úkon voči prevádzkovateľovi cloudového úložiska a vyzval by ho na sprístupnenie dát. Ten by bol v určitom časovom rámci povinný na sprístupnenie dát podľa elektronického rozhodnutia. Počítač predbežne vyhodnotí zaistené dáta, o čom vydá správu, ktorá môže ďalej slúžiť súdu pre stanovenie rizík zaistených elektronických dôkazných prostriedkov, ktoré môžu mať dopad na rozhodnutie a pokúsi sa vygenerovať správu o ich stave (viď podkapitolu: 2.6. o zásade voľného hodnotenia dôkazov ako analýze rizík).

Je zrejmé, že výhoda automatizovaného procesu spočíva v bezprostrednej elektronickej komunikácií medzi prevádzkovateľom a autonómnym počítačovým sudcom, a to až do doby využitia opravného prostriedku. Podľa vyššie uvedených príkladov nepôjde o plnohodnotné súdne rozhodovanie. Avšak vykonávanie elektronických dôkazných prostriedkov alebo rozhodovanie o zaisťovacích inštitútoch umelou inteligenciou môže nahradiť administratívnu prácu sudcu o faktických okolnostiach prípadu alebo pôsobiť podporne na jeho ďalšie rozhodnutia. Určitý náznak je už možné vidieť vo veciach rozhodovania mimosúdnych spotrebiteľských sporov rôznorodých kúpno-predajných platforiem (*Amazon, eBay, TaoBao* atď) alebo v otázkach automatického hodnotenia dôkazov o poistných udalostiach, kde dochádza k automatickému vyhodnocovaniu predložených dôkazných prostriedkov v elektronickej forme. Účelom tejto naprogramovanej podpory je v prvom rade snaha zabrániť vzniku omylu a potlačenie aspektu iracionality v ľudskom rozhodovaní. Počítač tu môže plniť pragmatickú funkciu interpretéra skutkov, pripomienkovača okolností, ale aj poštára – vymáhateľa povinností. V neposlednom rade je potrebné dodať, že technológia preventívnej identifikácie sa už dávnejšie uplatňuje v oblasti

cloudových, vyhľadávacích a poštových služieb.[342] Táto technológia zasahujúca do súkromnej sféry užívateľov vyvoláva mnohé právne otázky. Tie sú riešené na úrovni definičnej autority (napr. súhlas užívateľa s podmienkami využitia emailovej služby alebo anonymizovanie prehliadaného obsahu pomocou *hashing technology*), avšak neostávajú bez odozvy a otvárajú viaceré ústavné otázky.[343] Istotne je možné očakávať obdobné námietky a právne diskusie v prípade získaného elektronického dôkazu výlučne počítačom.

4.5. Zhrnutie kapitoly

V kapitole bolo diskutované, že počítač môže dopĺňať a podporovať rozhodovaciu činnosť sudcu, najmä v otázke zaistenia elektronických dôkazných prostriedkov, avšak nemôže prevziať jeho samostatnú právomoc a kompetenciu. Ako je vidieť, počítač sudca otvára starodávny problém mechanickej aplikácie práva. Napriek tomu, počítač môže predstavovať vítanú oporu právneho rozhodovania. Tak ako zákonodarca môže naprogramovať spôsob regulácie spoločnosti právnou normou, tak môže vedec naprogramovať počítač, aby neskôr aplikoval túto právnu normu. Ide však o programy, ktoré musia ostať pod kontrolou človeka. Je možné dodať, že v súčasnosti žiaden počítač nemá odvahu neuposlúchnuť svojho programátora.[344] Preto len človek je schopný identifikovať prípadný rozpor medzi programom a spravodlivosťou. Pre budúcnosť je možné vyjadriť Radbruchovské ponaučenie tak, že ak tento rozpor dosiahne tak neznesiteľnú mieru, že počítač by aplikoval zavrhnutiahodné právo, musí

[342] HECHMAN, M. How Google handles child pornography in Gmail, search. PC World. Aug 5, 2014. [online]. [cit.1.9.2020]. Dostupné z: http://www.pcworld.com/article/2461400/how-google-handles-child-pornography-in-gmail-search.html alebo CURTIS, S. Explained: how tech companies plan to stop paedophiles sharing child pornography. The Telegraph. 11 Dec 2014. [online]. [cit.1.9.2020]. Dostupné z: http://www.telegraph.co.uk/technology/news/11288028/Explained-how-tech-companies-plan-to-stop-paedophiles-sharing-child-pornography.html

[343] Prípad blokácie 1.5 milióna neškodných webov v USA za účelom automatickej blokácie detskej pornografie - Center for Democracy and Technology v. Pappert. Viď DIAZ, F. Using Technology to Prevent the Distribution of Child Pornography. Berkeley Technology Law Journal. November 10, 2015. [online]. [cit.1.9.2020]. Dostupné z:http://btlj.org/2015/11/using-technology-to-prevent-the-distribution-of-child-pornography/

[344] Takéto konštatovanie pripomína druhy zákon robotiky Isaaca Asimova, podľa ktorého *„robot musí poslúchnuť príkazov človeka, okrem prípadov, keď sú tieto príkazy v rozpore s prvým zákonom.“* ASIMOV, I. Nahé slunce. Praha: Ivo Železný, 1994. Str. 9.

vždy takýto program jednoznačne ustúpiť a byť vypnutý.[345] V záujme zachovania spravodlivosti totiž posledné slovo bude mať vždy sám človek. Nech je robotov povzdych v Čapkovej hre v poslednom dejstve mementom každého pokušiteľa uvažujúceho o počítačovom sudcovi: *„Slyšte, ó slyšte, lidé jsou naši otcové! Ten hlas, který volá, že chcete žít; ten hlas, který naříká; ten hlas, který myslí; ten hlas, který mluví o věčnosti, to je jejich hlas! Jsme jejich synové!“*[346]

[345] Radbruchová formula ako reakcia na nacistické besnenie hovorí, že *„konflikt medzi spravodlivosťou a právnou istotou je možné riešiť len tak, že pozitívne právo, zaisťované predpismi a mocou, má prednosť aj vtedy, ak je obsahovo nespravodlivé a neúčelné, okrem prípadu, ak rozpor medzi pozitívnym zákonom a spravodlivosťou dosiahne tak neznesiteľnej miery, že zákon musí ako „nenáležité právo“ spravodlivosti ustúpiť.“* RADBRUCH, G. O napětí mezi účely práva. Vyd. 1. Překlad Libor Hanuš. Praha: Wolters Kluwer Česká republika, 2012, Str. 41.

[346] ČAPEK, K., R.U.R.: Rossum's Universal Robots: kolektivní drama o vstupní komedii a třech dějstvích [online]. Praha: Štorch-Marien, 1920 (Spisy bratří Čapků; sv. 10). Dostupné z: http://web2.mlp.cz/koweb/00/03/34/75/81/rur.pdf

Osobitná časť: Vybrané druhy elektronických dôkazných prostriedkov

Elektronické dôkazné prostriedky sa v mnohých častiach líšia od ostatných druhov dôkazných prostriedkov. Pri ich hodnotení súdmi a inými príslušnými orgánmi vznikajú osobitné problémy. Tieto výzvy poukazujú na potrebu rozšíriť vedomosti o elektronických dôkazných prostriedkoch a zlepšiť zaobchádzanie s nimi.[347] Tuzemské normy procesného práva pracujú s demonštratívnym výpočtom dôkazných prostriedkov, ktorý dostali do vienka vo svojej dobe. Napriek tomu si tu nájde každý typ elektronického dôkazného prostriedku svoje miesto. Síce nie je možné hovoriť o reflektovaní špecifických technických postupov elektronického dokazovania v týchto procesných ustanoveniach tak, ako to nachádzame v anglo-americkom právnom systéme v podobe *e-discovery*, ale to nebráni vykonaniu elektronického dôkazného prostriedku podľa súčasne platných právnych predpisov. Existencia informačných technológií nevytvára nový paralelný svet, ale dochádza len k modifikovaniu formálnych parametrov štandardných spoločenských vzťahov. Podľa Polčáka je práve kľúčové v prípade právnej regulácie objaviť tie formálne aspekty, ktoré sa novými technickými výdobytkami zmenili, pričom všetko materiálne podstatné, t.j. „*fundamentálne, zostáva v práve nemenné*.“[348] Možno sa zdá byť elektronický dôkaz neuchopiteľný z pohľadu tradičného procesného dokazovania, avšak jeho hmotné výstupy sú s veľkou samozrejmosťou akceptované. Nie je prekvapením, že výtlačky emailov, výtlačky profilov sociálnych sietí či audiovizuálne nahrávky slúžia doposiaľ ako dôkaz na súdoch. Preto sa v osobitnej časti zameriame na jednotlivé druhy elektronických dôkazných prostriedkov a ich praktické aspekty. Ide o otázky zaistenia, forenznej analýzy, vykonania a hodnotenia dôkazu. Nakoľko je prepracované trestné právo procesné inšpiráciou pre to, ako precízne nakladať s *questio facti*, pokúsime sa analyzovať dokazovanie profilom sociálnej siete, webstránkou alebo IP adresou práve v trestnom konaní. Rovnako sa pozrieme na zaistenie elektronického dôkazného

[347] Viď napríklad Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings: Explanatory Memorandum. 1335th meeting of the European Committee on Legal Co-operation (CDCJ), 30 January 2019. Council of Europe. [online]. [cit.1.9.2020]. Dostupné z: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e

[348] POLČÁK, Radim. Dokazovaní elektronickými dokumentami. In: Dokazovanie v civilnom a trestnom konaní. Pezinok: Justičná akadémia Slovenskej republiky, 2012. ISBN 978-809-7020-743. Str. 61.

prostriedku v zmysle aktuálnej rekodifikácie trestného poriadku. Posledné dve kapitoly sú špecifické svojím predmetom. Netradične sa zameriame na druh informácie v elektronickej podobe, ktorý taktiež môže dobre slúžiť ako elektronický dôkazný prostriedok v konkrétnych situáciách. Predložíme analýzu toho, čo znamená kyberútok pre súkromnú spoločnosť, čo je to vnútorná informácia pre regulovanú entitu a ako s ňou naložiť. Do poslednej kapitoly sme zvolili starodávny inštitút papierovej zmenky, ktorý z nepochopiteľných príčin stále odoláva elektronickému kontrahovaniu a súčasnej technológií *blockchainu.* Táto skutočnosť vyvoláva nekončiacu radu nedorozumení a súdnych sporov.[349] Osobitnú časť uzavrieme teoretickým návrhom elektronickej zmenky.

[349] Viď napríklad VALČEK, Adam. Aj kľúčová znalkyňa hovorí o antedatovaní zmeniek. Sme.sk. Petit Press, a.s. 10.2.2020. [online]. [cit.1.9.2020]. Dostupné z: https://domov.sme.sk/c/22322855/aj-klucova-znalkyna-hovori-o-antedatovani-zmeniek.html

5. Dokazovanie profilom sociálnej siete, webstránkou a IP adresou v trestnom konaní*

5.1. Úvodné poznámky

Dokazovanie skutočností v trestnom konaní pomocou informácií vyťažených z osobného profilu sociálnej siete a webovej prezentácie predstavuje v súčasnosti problém procesného postupu OČTK. Webová prezentácia, ktorá je neodmysliteľne spojená s priekopníckymi začiatkami širokého využitia internetu, a od nej neskôr odvodený osobný profil v sociálnej sieti, je nositeľom užitočných informácií, ktoré môžu slúžiť ako vhodný dôkazný materiál v trestnom konaní o rôznorodých skutkoch. Je možné konštatovať, že tuzemská súdna prax sa už pokúša vysporiadať s fenoménom sociálnych sietí a súvisiacich digitálnych stôp. Desiatky súdnych rozhodnutí obsahujú tvrdenia strán alebo sa inak odvolávajú na tento elektronický dôkaz, často nahradený listinným výpisom komunikácie, fotografie alebo stav štatútu z portálu sociálnej siete.[350] Za účelom získania skutkových poznatkov tak boli podrobené skúmaniu komunikácie, obsahy fotografií alebo sociálne väzby užívateľov sociálnych portálov alebo webových prezentácií. Je na mieste sa pýtať, akú povahu má dôkaz získaný z týchto prostriedkov a aké je jeho správne vykonanie podľa platného procesného trestného práva?

V nasledujúcej kapitole bude osvetlená technická povaha osobného profilu vyskytujúceho sa na najčastejšie dostupných sociálnych sieťach. Paralelne bude vysvetlený proces fungovania webovej stránky so špecifickým obsahom – osobnou prezentáciou. Pre potreby využitia týchto dôkazných prostriedkov je nutné priblížiť

* Táto podkapitola vychádza z publikovanej kapitoly monografie ABELOVSKÝ, Tomáš. Dokazovanie osobným profilom a webovou prezentáciou. In: POLČÁK, Radim. PÚRY, František HARAŠTA, Jakub a kolektiv. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015, Spisy Právnické fakulty MU č. 542 (řada teoretická, Edice Scientia). ISBN 978-80-210-8073-7. Str. 221-233.

350 Viac ako 100 rozhodnutí NS ČR okrajovo odkazuje na dôkaz alebo inú skutočnosť pochádzajúcu zo sociálnej siete Facebook (Viď http://nsoud.cz/Judikatura/judikatura_ns.nsf/$$WebSearch1?SearchView&Query=%5BARozhodnutiRT%5D%3Dfacebook&Start=1&Count=15&SearchOrder=4&SearchMax=0&lng=). Taktiež existuje viac ako 20 rozhodnutí ÚS ČR, ktoré v texte uvádzajú skutočnosti pochádzajúce zo sociálnej siete Facebook (Viď http://nalus.usoud.cz/). Nižšie súdy s týmto typom zdroja dôkazu pracujú častejšie. Napr. prostredníctvom portálu www.otvorenesudy.sk je možné na Slovensku nájsť viac ako 1600 výsledkov (rozhodnutí nižších súdov, ktoré sú povinne zverejňované) po zadaní kľúčového slova „Facebook“ (Viď https://otvorenesudy.sk/decrees?l=sk&q=facebook&utf8=✓).

procesné otázky ich zaistenia a uchovávania v zmysle platnej zákonnej úpravy trestného poriadku ČR. Navyše, forenzná analýza tohto typu dôkazného prostriedku predstavuje kľúčovú časť celého dôkazného procesu, ktorý je zavŕšený vykonaním a hodnotením takto získaných dôkazov.

5.2. Vysvetlenie pojmov

5.2.1. Sociálna sieť

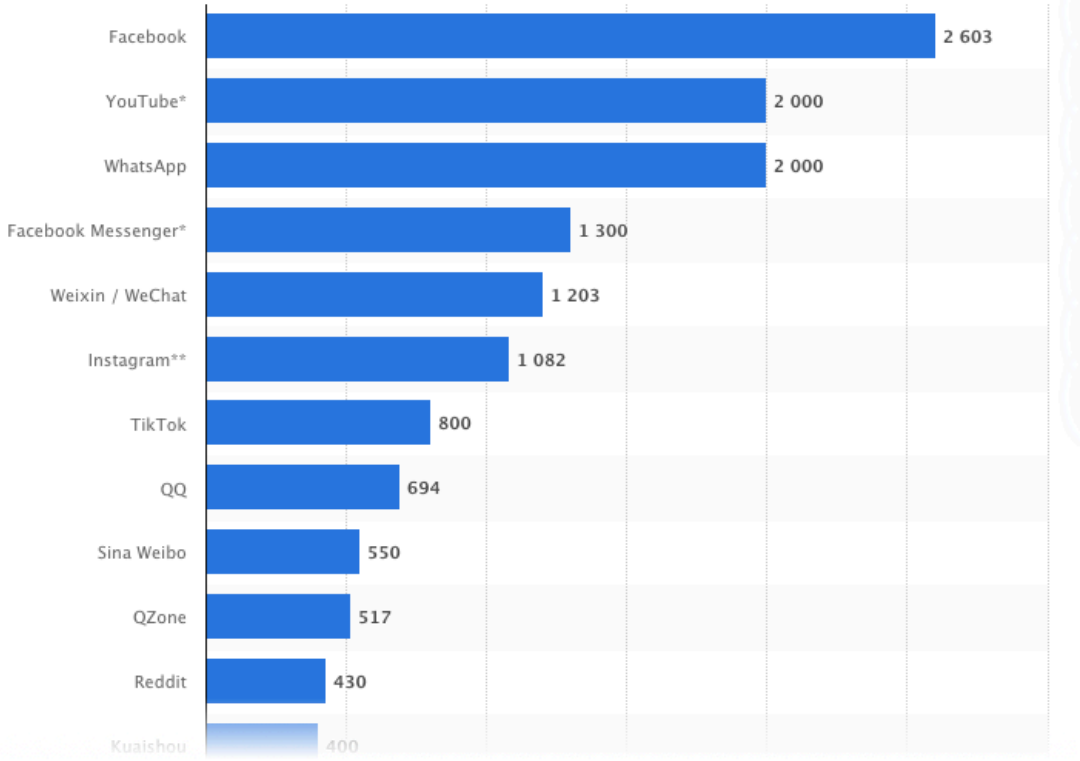
Za sociálnu sieť sa považuje každá webová stránka prístupná verejnosti pomocou webového prehliadača (na PC, tablete alebo mobilnom zariadení) alebo inej aplikácie, ktorej primárnym cieľom je nadväzovanie, udržiavanie a rozširovanie sociálnych väzieb medzi užívateľmi. Ďalším cieľom je zdieľanie obsahu (text, fotky, obrázky, hudba, videá, správy atď.). Sociálne siete sa zväčša delia na súkromne (napr. Facebook) alebo profesné (napr. LinkedIn). Avšak toto delenie sa v posledných rokoch vytráca. Poskytovatelia služieb sociálnych sietí (ďalej len ako „poskytovatelia“) pochopili, že model nadväzovania profesných kontaktov (ponuka platených služieb) a model postavený na platenej reklame pri voľne dostupných zábavných službách môžu často splývať, resp. čerpať výhody jeden od druhého. Napriek tejto skutočnosti je charakter sociálnej sieti a jej zameranie (orientácia na koncového užívateľa) stále významné pre prvotné rozhodnutie o voľbe dôkazného prostriedku.[351] V tuzemskej vyšetrovacej praxi sa je možné najčastejšie stretnúť s vyťažovaním informácií zo sociálnych sietí, akými sú Facebook, Instagram a Lide.cz. Či už ide o páchateľa trestného činu, svedka alebo obeť, tieto siete môžu ponúknuť veľké množstvo digitálnych stôp.

Ďalším významným aspektom pre selekciu dôkazného prostriedku je štát pôvodu sociálnej siete, resp. jurisdikcia, pod ktorú spadá poskytovateľ (alebo jeho server).

[351] Je možné uvažovať o tom, že profesná sieť LinkedIn (známa svojou stavbou osobného profilu v podobe formy životopisu) bude mať u bežného užívateľa väčšiu dôveru pravdivosti zverejnených a dostupných informácií ako sieť Facebook. Samotná podstata tejto siete je založená na vytváraní profesných kontaktov a sprostredkovaní zamestnania. Avšak je potrebné dodať, že aj (pôvodne študentská) sieť Facebook približuje pracovný trh jej užívateľom. Navyše, nedávno zaviedla kontroverzné pravidlá používania „reálnych mien“. Viď Facebook.com, Help Center: What names are allowed on Facebook?. [online]. [cit.1.9.2020]. Dostupné z: https://www.facebook.com/help/112146705538576 alebo PHILLIP, Phillip. Online ‘authenticity’ and how Facebook’s ‘real name’ policy hurts Native Americans. In: The Washington Post [online]. [cit. 1.9.2020]. Dostupné z: https://www.washingtonpost.com/news/morning-mix/wp/2015/02/10/online-authenticity-and-how-facebooks-real-name-policy-hurts-native-americans/

Taktiež to je jeho ochota alebo skúsenosť spolupracovať pri vydávaní potrebných údajov.

Súčasná odborná trestná literatúra radí sociálne siete medzi prostriedky, ktoré sú podobné sieťam elektronických komunikácií (napr. v prípade zákazu styku s určitými osobami v zmysle § 88d TŘ).[352] Navyše, sociálna sieť má charakter služby informačnej spoločnosti v zmysle zákona č. 480/2004 Sb. o niektorých službách informačnej spoločnosti.[353] Medzi najväčšie zahraničné sociálne siete v súčasnosti patria (v mil.):[354]



[352] *„Mezi obdobné prostředky (jako síť elektronických komunikací) lze řadit všechny obdobné typy propojení počítačů (mobilních telefonů, smartphonů nebo tabletů) do sítě založené na přístupu na dálku, např. tedy i prostřednictvím nejrůznějších komunikačních systémů (ICQ, Miranda apod.). Patří sem nepochybně i Facebook, Twitter a systémy podobné.“* Viď ŠÁMAL, P. a kol.: Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013, Str. 1252.

[353] Viď § 2 ods. 1 písm. a) *„Službou informační společnosti je jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat.“* Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů.

[354] CLEMENT, J. Global social networks ranked by number of users 2020. In: STATISTA.com. Most popular social networks worldwide as of July 2020, ranked by number of active users (in millions). [online]. [cit.1.9.2020]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Význam sociálnych sieti je neprehliadnuteľný. Podľa prieskumov, dve tretiny domácich používateľov internetu v ČR navštevujú sociálne siete a z toho štyri pätiny aspoň raz denne. Štvrtina užívateľov aspoň raz denne niečo okomentuje na sociálnych sieťach a nahrá na internet aspoň raz týždenne vlastnoručne vytvorený obsah.[355] Medzi tri najväčšie české sociálne siete v súčasnosti patria Lide.cz (všeobecná sociálna sieť), Spoluzaci.cz (určený pre bývalých spolužiakov) a online zoznamka Libimseti.cz. V posledných rokoch ich popularita klesá hlavne v dôsledku zvyšovania popularity Facebooku, čínskej platformy TikTok a Instagramu.[356]

Užívatelia internetu už dávno uprednostňujú sociálne siete pred pôvodnými elektronickými službami, akými sú obyčajný email, webstránka alebo chat. Sociálne siete tieto služby suplujú a pod jednou strechou v inovatívnom kabáte prinášajú komplexné softvérové riešenia. Príkladom môže byť už zaniknutá sociálna sieť Google+, ktorá bola súčasťou ekosystému aplikácií Google a predstavovala prístup k službám, akými boli webová prezentácia užívateľa, diskusné fórum, email, chat, VoIP, manažment súborov, úložný priestor, hry a kancelárske nástroje atď. Obdobnou cestou sa vybrala sociálna sieť Facebook. Preto si je potrebné túto skutočnosť uvedomiť v prípade získavania informácií z osobného profilu a analyzovať všetky prepojené služby ponúkané poskytovateľom alebo oprávnenou treťou osobou integrovanou do sociálnej siete s prepojením na skúmaný účet.[357]

5.2.2. Osobný profil sociálnej sieti

Zámerom registrácie užívateľa v sociálnej sieti je zdieľať vybrané údaje (často osobnej povahy, napr. meno, adresa, vzdelanie, profesia, stav, národnosť, dátum narodenia, bydlisko, aktivity, záľuby atď.) ďalším užívateľom tejto siete. Množina týchto údajov, či už zadaných počas registrácie alebo neskôr upravených v priebehu existencie účtu, spolu s nahratými grafickými médiami (fotky, obrázky, videá atď.), publikovanými textami a súbormi (blog, mikroblog, knižnica nahratých súborov atď.),

[355] LUPAČ Petr, Alena CHROBÁKOVÁ a Jan SLÁDEK, 2014. Internet v České republice 2014. Praha: Filozofická fakulta Univerzity Karlovy v Praze. [online]. [cit.1.9.2020]. Dostupné z: https://www.academia.edu/12609849/The_Internet_in_the_Czech_Republic_2014

[356] Viď napríklad Sociální sítě nejsou jen Facebook. Podívejte se i na ty české. iDnes.cz. MAFRA, a. s. [online]. [cit.1.9.2020]. Dostupné z: https://www.idnes.cz/technet/internet/socialni-site-nejsou-jen-facebook-podivejte-se-i-na-ty-ceske.A091017_234210_tec_reportaze_vse

[357] Príkladom môže byť množstvo pripravovaných aplikácií pre sociálnu sieť Facebook, ktoré sú technicky, ale aj právne, previazané s pôvodným poskytovateľom sociálnej siete. Viď Facebook Developers. [online]. [cit.1.9.2020]. Dostupné z: https://developers.facebook.com

zoznamom prepojení (kontakt list) a súvisiacimi informáciami o interakciách (wall príspevky alebo odpovede, geolokácie atď.), predstavuje celistvý osobný profil užívateľa sociálnej siete.[358]

Osobný profil užívateľa je ďalej prepojený s prevádzkovými údajmi (napr. záznamy miesta a času prihlásenia, IP adresy, dĺžka spojenia, typ web prehliadača, posledná príchodzia a odchodzia webstránka atď.) a metadátami súborov, ktoré sú zväčša nedostupné pre samotného užívateľa. Navyše, osobný profil užívateľa nemusí byť sprístupnený širokej internetovej verejnosti. Takmer každá sociálna sieť obsahuje možnosť zamedziť verejnosti vidieť takýto profil, resp. jeho výstupy.

Z právneho hľadiska je mimoriadne obtiažné určiť povahu sociálnej siete. Ide čiastočne o verejný, čiastočne o súkromný priestor. Voľba je ponechaná na technických parametroch systému a prípadnej možnosti výberu užívateľa sprístupniť tento priestor tretím osobám. ÚS ČR vo svojom rozhodnutí k povahe sociálnej siete Facebook uviedol nasledujúce:[359]

„Povaha sociální sítě Facebook není dle názoru Ústavního soudu jednoznačně soukromá či veřejná. Vždy záleží na konkrétních uživatelích, jakým způsobem si míru soukromí na svém profilu, případně přímo u jednotlivých příspěvků, nastaví. Teoreticky může uživatel prostřednictvím této sítě komunikovat pouze s jediným dalším uživatelem, a to aniž by tuto komunikaci mohli vidět, či do ní zasahovat, ostatní uživatelé. Taková komunikace by pak jistě mohla být považována za ryze soukromou, byť uskutečněnou prostřednictvím sociální sítě využívané miliardou uživatelů, stejně jako je za soukromou možno považovat emailovou komunikaci dvou osob, uskutečněnou např. prostřednictvím emailové služby Gmail (www.gmail.com), kterou taktéž využívají miliony uživatelů (obdobně v České republice např. emailová služba dostupná na stránkách www.seznam.cz). Uživatel sociální sítě Facebook však má možnost učinit svůj profil také zcela veřejným a tedy přístupným všem uživatelům sociální sítě Facebook, případně i všem uživatelům sítě internet. Tato možnost je hojně využívána např. politickými stranami, zájmovými skupinami, umělci, poskytovateli

[358] Avšak je potrebné mať na pamäti, že žiaden z týchto údajov nemusí byť pravdivý. Napr. pri bezplatnom registrovaní účtu v sieti Facebook je potrebné vyplniť nasledujúci minimálny štandard: meno, priezvisko, email alebo tel. číslo mobilu, heslo, pohlavie a dátum narodenia. Jediná informácia, ktorá podlieha verifikácii, je email alebo mobilné číslo.

[359] Rozhodnutí ÚS ČR ze dne 30.10.2014, sp. zn. III. ÚS 3844/13.

služeb, obchodníky a dalšími, jejichž cílem je prezentovat se prostřednictvím sociální sítě Facebooku co nejširšímu počtu uživatelů internetu. Toto nastavení ale volí i část "běžných" uživatelů.“

V nadväznosti na toto rozhodnutie je nutné spomenúť ešte jeden prípad, ktorý riešil právnu povahu sociálnej siete. NS ČR sa zaoberal tým, či sociálna sieť a prejavy poslanca na nej, sú prejavy v rámci Poslaneckej snemovne, a to z dôvodu jeho vyňatia z právomoci OČTK:[360]

„Nejvyšší soud, pohybujíc se v takto určeném legislativním a výkladovém rámci, konstatuje, že text, uveřejněný na uživatelském profilu internetové sociální sítě facebook jako písemné vyjádření myšlenek obviněného, tehdy poslance Parlamentu ČR, nenaplňuje znaky projevu poslance na půdě sněmovní komory. Nešlo totiž o projev v rámci soutěže politických sil, diskusí při legislativním procesu, jakéhokoli jednání pléna či orgánů sněmovny. Nemohlo ani jít o výkon poslaneckého mandátu ve sněmovně. Veřejně přístupné uživatelské profily internetových sociálních sítí, ostatně stejně jako obecně přístupné internetové stránky, mají v současné době nepochybně již charakter masových komunikačních prostředků, rovnocenných s tiskem, rozhlasem a televizí. Pokud se poslanec Parlamentu rozhodne či je vyzván prezentovat své myšlenky veřejně v prostředcích veřejné komunikace a tyto jsou cíleně zaměřeny právě a jedině vůči veřejnosti, vně sněmovního prostředí, jde o občanské projevy podléhající veřejné kontrole, kritice. V demokratickém společenském zřízení lze zde proto předpokládat občanskou záruku svobodné společnosti proti případným excesům výkonné či soudní moci.“

Pojem verejnosti bol riešený v inom prípade ÚS ČR. K posúdeniu naplneniu znakov „robí verejne prístupným“ podľa TZ, ku ktorému malo dôjsť užitím internetovej sociálnej siete, si súdy musia najprv ujasniť, aké sú jej funkcionality (ktoré mal páchateľ k dispozícii) a aké skutočne využil a čo toto využitie z hľadiska rozsahu jeho trestnej činnosti znamená: [361]

„Pojem veřejné přístupnosti na internetu je přitom nutno hodnotit nejen s ohledem na možnosti uživatelů internetu daný obsah zobrazit, pokud jde o přístupová práva, ale

[360] Usnesení NS ČR ze dne 25. 6. 2014, sp. zn. 3 Tcu 33/2014-26.
[361] Nález ÚS ČR ze dne 20. 8. 2013, sp. zn. I. ÚS 1428/13.

i ve světle jejich možnosti se o něm vůbec v prvé řadě dozvědět (například z příspěvků na chatech a diskusních skupinách, z obsahů stránek indexovaných vyhledávacími službami, nebo právě díky vložení na profil uživatele internetové sociální sítě, jehož obsah je přeposílán jejím dalším uživatelům).“

V inom spore bolo posudzované to, či možno za konanie v rozpore s dobrými mravmi súťaže považovať upozornenie tretej osoby smerujúce prevádzkovateľovi sociálnej siete, v danom prípade Facebooku, na potenciálnu kolíziu profile iného užívateľa s právami z priemyselného vlastníctva, a to v prípade, ak by bolo nepravdivé. NS ČR vo svojom rozhodnutí uviedol, že *„jestliže soutěžitel neopodstatněně oznámí provozovateli komunikačního kanálu na internetu (provozovateli sítě Facebook), že jiný soutěžitel mající profil v síti Facebook porušuje jeho práva z duševního vlastnictví, dopouští se tím nekalosoutěžního jednání.“*[362] Ide tu o zaujímavý prípad, v ktorom zohrali rolu dôkazy o profiloch užívateľov sociálnej siete a povahe takejto siete.

Charakter sociálnej siete bol riešený aj v prípade zverejnenie profilovej fotografie a či bol daný konkludentný súhlas na jej použitie. NS ČR uviedol:[363]

„V případě použití profilové fotografie uživatele sociální sítě Facebook nelze bez dalšího dovodit konkludentní souhlas s jejím dalším zveřejněním ani naplnění předpokladů zákonné zpravodajské licence, ale vždy je třeba zabývat se hlediskem přiměřenosti se zřetelem ke konkrétním okolnostem zveřejnění a chránit nejen svobodu projevu informačních médií a právo veřejnosti na informace, ale též oprávněné zájmy zobrazené osoby.“

Je zrejmé, že užívateľ sociálnej siete si môže nastaviť individuálne okrem iného aj rozsah zdieľania uverejňovaných informácií a ovplyvniť, kto uvidí ním uverejnený obsah. Profilová fotografia z podstaty veci má však obmedzenia. Jedinou možnosťou je jej úplne skrytie, resp. skrytie profilu. Ako súd potvrdil, túto možnosť však nie je možné považovať za alternatívu, resp. možnosť voľby v prostredí sociálnych sietí.[364]

[362] Rozsudek NS ČR ze dne 26. 4. 2016, sp. zn. 23 Cdo 3415/2014.

[363] Rozsudek NS ČR ze dne 15. 10. 2019, sp. zn. 25 Cdo 1778/2019.

[364] Súd uviedol, že použiť takú fotografiu teda možné je, ale aj tu je nevyhnutné vykonať test proporcionality, zvážiť, za akým účelom je fotografie zverejnené, aká je forma a obsah tohto zverejnenia, či je osoba, ku ktorej sa fotografie vzťahuje, osobou verejného záujmu. Až pri splnení týchto podmienok môže byť zverejnenie považované za primerané a teda aj zastrešené spravodajskú licenciou. Viď Rozsudek NS ČR ze dne 15. 10. 2019, sp. zn. 25 Cdo 1778/2019.

Povaha sociálnych sietí je ovplyvnená aj tým, že sa na ne nepriamo vzťahujú povinnosti primárne určené štátom a predstavujú virtualizované ekosystémy, ktorých účelom je *„poskytovanie voľného trhu myšlienok, priestoru pre sebarealizáciu jednotlivcov a sprostredkovanie rozvoja demokratickej spoločnosti,“* ale zároveň aj možnosť prepájať rôzne časti svojho virtualizovaného života.[365]

5.2.3. Webová prezentácia

V nadväznosti na osobný profil sociálnej siete je potrebné uviesť, že pôvodná webová prezentácia (webstránka) prestala byť doménou internetových nadšencov a ustupuje informatívno-vizuálnym prezentáciám komerčných alebo neziskových subjektov. Navyše webstránky plnia množstvo iných úloh, predstavujú informačné zdroje alebo prístupné brány k internetovým web aplikáciám. Webstránka môže obsahovať všetky vyššie uvedené prvky typické pre osobný profil užívateľa sociálnej siete, ale rovnako často obsahuje aj ďalšie technické údaje spojené s jej užívateľom. Vlastnosťou webstránky je existencia doménového mena (pod ktorým je identifikovateľná) a súvisiaci WHOIS zápis.[366]

Pod pojmom webstránka je možné rozumieť jeden alebo viacero súborov (dokumentov) s obsahom presne špecifikovaného kódu (napr. HTML, XHTML), ktoré sa distribuujú prostredníctvom verejnej siete internet (za pomoci HTTP protokolu) z jedného miesta (web servera) a ich výstupy sú zobraziteľné pomocou URL v štandardnom webovom prehliadači (napr. Internet Explorer, Chrome, Safari, Firefox atď.). Súbor všetkých dostupných stránok vytvára celosvetovú webovú sieť (world web site).

Webstránka je pomerne široký pojem. Pre účely trestného konania je nutné považovať za webstránku akýkoľvek zdroj informácie čitateľnej a dostupnej na

[365] HANYCH, Monika, PIVODA, Marek. Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown. Revue pro právo a technologie. 2017, č. 16, Str. 177-220.

[366] WHOIS (z angličtiny, who is? - Kto je?) je označenie pre prístupnú databázu a službu, ktorá slúži na evidenciu údajov o majiteľoch internetových domén a IP adries. Tie často môžu odhaliť komplexné pozadie registrovaných webstránok. Niektoré súkromné spoločnosti (napr. domaintools.com) sa zameriavajú na ukladanie historických údajov z týchto databáz, ukladanie historických screenshotov (webhistory.org), čo umožňuje pomerne ľahké vyhľadávanie alebo reverzný výpis (napr. všetky domény jednej spoločnosti alebo majiteľa). Viď ICANN Lookup: About WHOIS. 2019. Internet Corporation for Assigned Names and Numbers. [online]. [cit. 1.9.2020]. Dostupné z: https://whois.icann.org/en/about-whois

internete alebo intranete prostredníctvom protokolu HTTP/S v štandardnom webovom prehliadači. Navyše, výtlačok (tzv. printscreen) webstránky predstavuje v poslednej dobe jeden z najčastejších dôkazných prostriedkov (v podobe listiny), aj keď často nesprávnym spôsobom interpretovaný. Získané informácie z webstránky môžu byť obsahové (text webstránky) alebo technické (metadáta súborov, v ktorých je stránka naprogramovaná, loggy, databázové súbory atď.). Pre potreby tejto kapitoly bude potrebné skúmať možnosti správneho zaistenia a uchovávania webstránok s údajmi potrebnými pre trestné konanie. V závere je potrebné dodať, že osobný profil sociálnej siete je *de facto* tiež spustiteľná webstránka. Navyše, aj webstránka môže byť v správe tretej osoby – poskytovateľa web hostingu. Preto ak sa v tejto kapitole bude hovoriť o osobnom profile sociálnej siete užívateľa, pokiaľ nie je uvedené inak, má sa na mysli aj webstránka.

5.3. Zaistenie a uchovávanie dôkazného prostriedku

5.3.1. Oprávnená osoba

Oprávnenou osobou v prípade trestného konania pre zaistenie a uchovávanie dôkazného prostriedku osobného profilu sociálnej siete alebo webstránky bude v prvom rade policajný orgán, štátny zástupca alebo súd. Je potrebné uviesť, že aj advokát (obhajca) má právo v zmysle platných právnych predpisov vyhľadávať dôkazy pre svojho mandanta, avšak v rámci trestného konania je toto právo značne limitované.[367] Obmedzenie pochádza aj zo strany poskytovateľov, ktorí nemajú žiadnu právnu povinnosť spolupracovať s tuzemským advokátom (opačný prístup je v prípade anglo-amerického práva, kde advokát za asistencie súdu získava dôkazy aj v trestnom konaní).

Súčasná právna úprava v prípade využitia zaisťovacieho prostriedku v prípravnom konaní alebo konaní pred súdom počíta so všeobecnou edičnou povinnosťou dotknutej osoby zakotvenou v § 78 ods. 1 TŘ:

[367] Súčasná úprava vyhľadávania dôkazov advokátom je obsiahnutá najmä v § 41 ods.1 a 2 a § 89 ods. 2 TŘ. Predmetnú problematiku upravuje aj uznesenie Českej advokátskej komory č. 13/2004 z 12. októbra 2004 a stanovisko NSZ poř. č. 9 / 2004 zo dňa 14. októbra 2004. Taktiež odborná literatúra poukazuje aj na dôležitosť zákona č. 101/2000 Z. z. o ochrane osobných údajov. Viď PECH, Lukáš. Vyhledávání důkazů advokátem v trestním řízení. ePravo.cz [online]. [cit.1.9.2020]. Dostupné z: http://www.epravo.cz/top/clanky/vyhledavani-dukazu-advokatem-v-trestnim-rizeni-55563.html

„Kdo má u sebe věc, která může sloužit pro důkazní účely, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely náležitého zjištění skutečností důležitých pro trestní řízení zajistit, je povinen takovou věc na vyzvání těmto orgánům vydat. Při vyzvání je třeba ho upozornit na to, že nevyhoví-li výzvě, může mu být věc odňata, jakož i na jiné následky nevyhovění (§ 66). Vyzvat k předložení nebo vydání věci je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán."

Navyše v zmysle povinnosti súčinnosti štátnych orgánov, fyzických a právnických osôb, podľa §7b ods.1 TŘ:

„Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat."

Obdobne podľa §7b ods.2 TŘ to platí aj v prípade. ak je to potrebné na zabránenie pokračovania v trestnej činnosti alebo jej opakovaniu. Osobe, ktorá drží alebo má pod svojou kontrolou dáta, ktoré sú uložené v počítačovom systéme alebo na nosiči informácií, možno nariadiť aby znemožnila prístup iných osôb k takýmto dátam. Takýto príkaz je oprávnený vydať predseda senátu a v prípravnom konaní štátny zástupca alebo policajný orgán. Policajný orgán potrebuje na vydanie takého príkazu predchádzajúci súhlas štátneho zástupcu. Bez predchádzajúceho súhlasu môže byť príkaz policajným orgánom vydaný len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť a vec neznesie odklad. V príkaze musia byť konkretizované dáta a dôvod, pre ktorý majú byť dáta uchované alebo k nim má byť znemožnený prístup. Táto povinnosť vyvoláva mnohé nejasnosti o tom, ako detailne majú byť dáta popísané (viď 6. kapitolu: Zaistenie elektronického dôkazného prostriedku v vo svetle trestného poriadku ČR a SR). Rovnako príkaz musí obsahovať dobu, po ktorú majú byť tieto dáta uchované alebo k nim má byť znemožnený prístup, ktorá nesmie byť dlhšia ako 90 dní. Príkaz musí obsahovať aj poučenie o následkoch neuposlúchnutie príkazu.

V praxi sa vyššie uvedené inštitúty využívajú spolu s domovou prehliadkou podľa ustanovení § 82 až § 85b, resp. § 158d ods.1, 3 TŘ v prípade nedobrovoľného zaistenia

elektronických dôkazných prostriedkov. [368] OČTK sa bežne k dôkazom dostávajú prostredníctvom vyťažovania zaistených elektronických nosičov (vecí) za využitia odbornej znaleckej expertízy. Avšak táto koncepcia je v prípade dôkazného prostriedku zo sociálnej siete alebo webovej stránky prekonaná. Kyberpriestor v súčasnosti predstavuje nový fenomén, ktorý umožňuje virtualizovanie dát do takej podoby, že tie sú ťažko fyzicky lokalizovateľné.[369] Čo je však dôležitejšie, zaistenie dát na rozdiel od zaistenia veci (napr. celého hard disku počítača) môže priniesť omnoho šetrnejší a precíznejší zásah do práv vyšetrovaného. Ide o vyjadrenie zásady zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktoré sú vlastné trestnému právu.[370]

Zaujímavou problematikou je skutočnosť, že drvivá väčšina informácií osobných profilov sociálnej siete je uložená v počítačovej databáze. Ide o typický prípad, kedy sa na jednom dátovom nosiči nachádza väčšie množstvo dát, často s vecou nesúvisiacich. Preto je nevyhnutná prvotná selekcia, a to nie len z pohľadu náhrady škody plynúcej v prípade obmedzenia činnosti poskytovateľa (zaistenie celého dátového nosiča), ale aj z pohľadu ochrany práv ostatných účastníkov sociálnej siete.

Navyše, c*onditio sine qua non* pre odňatie veci je aj to, že nejde o listinu, ktorej obsah sa týka okolnosti, o ktorej platí zákaz výsluchu, ibaže došlo k oslobodeniu od povinnosti zachovať vec v tajnosti alebo k oslobodeniu od povinnosti mlčanlivosti (napr. klient pozbaví povinnosti mlčanlivosti svojho advokáta). Podľa výkladového stanoviska NSZ, dátové nosiče nie sú listinou v zmysle § 112 TŘ. [371]

---

[368] *„Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.“* Viď Stanovisko NSZ č. 1/2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf

[369] Napr. cloud systém, ktorý využíva serverové farmy po celom svete a ani sám správca tohto systému nevie, kde sa nachádza ten ktorý sektor disku s požadovanou informáciou, nakoľko tieto môžu byť v neustálom pohybe.

[370] KOLOUCH, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. [online]. [cit.1.9.2020]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/zajistovaci_ukony-rtf.pdf

[371] *„Listinou se záznamy na nosiči informací stanou teprve poté, kdy jsou skutečně z nosiče informací do listinné podoby převedeny.“* a ďalej *„Z uvedeného závěru vyplývá skutečnost, že ve vztahu k nosiči informací nelze aplikovat výjimku z povinnosti vydat věc důležitou pro trestní řízení ve smyslu § 78 odst. 2 tr. ř. a toto ustanovení nebrání jejich zajištění, nastupuje povinnost orgánů činných v trestním řízení takové věci zajistit.“* Preto sa na ne nevzťahovalo pôvodne znenie ustanovenia § 78 ods. 2 TŘ, ktoré však bolo novelizované v roku 2017 zákonom č. 55/2017 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení

Otázkou ostáva, či je možné aplikovať na zaistenie dôkazov zo sociálnych sietí a webových prezentácii aj procesný postup nariadenia odposluchu a záznamu telekomunikačnej prevádzky. Nakoľko systém sociálnej siete môže vykazovať znaky telekomunikačnej prevádzky, môže OČTK žiadať o zachytenie každej budúcej informácie, a to len za splnenia podmienok (v prípade „obsahového" záznamu) podľa § 88 ods. 1, 2 TŘ[372] alebo v prípade zaistenia telekomunikačných údajov (prevádzkové údaje, akými sú IP adresa, čas a dĺžka pripojenia atď.) podľa § 88a TŘ.

Nariadiť odpočúvanie a záznam telekomunikačnej prevádzky v prípade dát prenášaných na sociálnej sieti je oprávnený predseda senátu a v prípravnom konaní na návrh štátneho zástupcu sudca. V prípade zaistenia prevádzkových údajov (údaje o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných a odkazových dát) a ak nemožno sledovaný účel dosiahnuť inak alebo ak bolo by inak jeho dosiahnutie podstatne sťažené, nariadi v konaní pred súdom ich vydanie súdu predseda senátu a v prípravnom konaní nariadi ich vydanie štátnemu zástupcovi alebo policajnému orgánu sudca na návrh štátneho zástupcu. Takýto príkaz musí byť vydaný písomne a musí byť odôvodnený. Problémy môže predstavovať komplikovaná špecifikácia užívateľskej adresy či zariadenia a osoby používateľa (účtu), ktoré musia byť v príkaze presne uvedené.[373] Príkaz musí obsahovať tiež dobu, po ktorú bude odpočúvanie a záznam telekomunikačnej prevádzky vykonávaný, ktorá nesmie byť dlhšia ako štyri mesiace. V neposlednom rade musí príkaz obsahovať konkrétne skutkové okolnosti, ktoré

soudním (trestní řád), ve znění pozdějších předpisů, a další související zákony. V súčastnosti podľa §78 ods.2 „*Povinnost podle odstavce 1 se nevztahuje na listinu nebo na jiný hmotný nosič obsahující obrazový, zvukový nebo datový záznam, jejichž obsah se týká okolnosti, o které platí zákaz výslechu, ledaže došlo k zproštění povinnosti zachovat věc v tajnosti nebo k zproštění povinnosti mlčenlivosti.*" Výkladové stanovisko NSZ č. 9/2001 k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků. [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/stanovisko-9-2001.pdf a stanovisko č. 1/2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf

[372] § 88 ods. 1 TŘ.

[373] Súdna prax taktiež riešila otázku príkazu k domovej prehliadke podľa § 83 ods.1 TŘ, kde bol priestor okrem iného identifikovaný nesprávnou IP adresou. ÚS ČR v konkrétnom prípade vo svojom odôvodnení uviedol, že *„napadený příkaz k domovní prohlídce vyhovoval zákonným požadavkům, neboť z něj bylo zřejmé, kdo jej vydal, o podezření z jakého trestného činu se jednalo, kde se měla prohlídka vykonat, kdo mohl být pachatelem trestné činnosti a rovněž jaké byly důvody vzniku podezření ze spáchání konkrétního trestného činu. Pochybení v podobě nesprávně uvedené IP adresy nebylo takového rázu, aby, přihlédnuto k okolnostem případu, zakládalo pochybnosti o důvodnosti nařízení domovní prohlídky, resp. činilo příkaz k domovní prohlídce nepřezkoumatelným"* Viď Usnesení Ústavního soudu ze dne 14. 12. 2011, sp. zn. IV. ÚS 3225/09

vydanie tohto príkazu, vrátane doby jeho trvania, odôvodňujú. V dôsledku vývoja judikatúry je však v súčasnej dobe vyžadované, aby nad rámec náležitostí uvedených v § 88 ods. 2 TŘ obsahoval príkaz tiež účel odpočúvania záznamu telekomunikačnej prevádzky, ako aj odôvodnenie, prečo nemožno sledovaný účel dosiahnuť inak alebo prečo by bolo inak jeho dosiahnutie podstatne sťažené (porovnaj tiež zásadu zdržanlivosti, vyjadrenú v § 2 ods. 4 druhej vete TŘ). [374]

V prípade ak je potrebné získať obsah, resp. súvisiace prevádzkové údaje osobného profilu alebo webovej prezentácie uloženej na zahraničnom servery (typické komerčné služby Facebook a LinkedIn, ktoré majú svoje sídlo a servre v USA) je potrebné, aby OČTK postupovali cestou právnej pomoci. Buď pôjde o vykonávanie jednotlivých úkonov právnej pomoci na základe medzinárodnej zmluvy alebo o realizáciu právnej pomoci bez zmluvného základu. Príkladom môže byť spolupráca členských štátov EÚ, kde základom sú články 82 a 86 ZFEÚ. Dňa 29. mája 2000 Rada ministrov EÚ schválila Dohovor o vzájomnej pomoci v trestných veciach, ktorého cieľom je podporovať spoluprácu medzi justičnými, policajnými a colnými orgánmi v rámci Únie doplňovaním ustanovení v existujúcich právnych nástrojoch. Taktiež významnú rolu zohráva aj budapeštiansky Dohovor o počítačovej kriminalite zo dňa 23.11.2001. V neposlednom rade ide o Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, vypracovaný Radou v súlade s článkom 34 Zmluvy o EÚ. Justičná spolupráca v trestných veciach v rámci EÚ stojí na dvoch kľúčových princípoch: na uznávaní rozsudkov a súdnych rozhodnutí a taktiež na zbližovaní právnych predpisov členských štátov. Ide najmä o úpravu v prípade príkazu na zaistenie majetku a dôkazov v prípade zaisťovania elektronických dôkazov v pôsobnosti cudzieho prevádzkovateľa sociálnej siete. Vyjadrenie týchto princípov vo sfére dokazovania bolo zavŕšené v smernici Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. [375] Budúci sľubný vývoj predpokladá návrh nariadenie Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických

[374] Výkladové stanovisko č. 1/2018 k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu. [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_719-2017.pdf

[375] Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach

dôkazov v trestných veciach. [376] Úlohou nariadenia je zaviesť alternatívny mechanizmus k existujúcim nástrojom medzinárodnej spolupráce a vzájomnej právnej pomoci v trestných veciach. Nariadenie ponúka riešenie problémov vyplývajúcich z elektronických dôkazných prostriedkov a aspektu nemožnosti lokalizácie.[377]

K otázkam zaistenia elektronického dôkazu sa vyjadril aj ÚS SR, ktorý vo veci výberu nástrojov vo svetle existencie trestného inštitútu „uchovania a vydania počítačových údajov" vyslovil, že:[378]

„Záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov podľa štvrtej hlavy prvej časti Trestného poriadku („Zaistenie osôb a vecí") musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva. Znamená to zvoliť pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa. Samotná právna úprava obsiahnutá v Trestnom poriadku na túto požiadavku reflektuje a určuje na dosiahnutie špecifického cieľa (získanie počítačových údajov dôležitých pre objasnenie trestnej činnosti) prostriedok zaručujúci požadovanú proporcionalitu, ktorým je úkon uchovania a vydania počítačových údajov zakotvený v ustanoveniach § 90 Trestného poriadku. Je nepochybné, že ide o prostriedok, ktorého realizácia predstavuje zásah menšej intenzity v porovnaní so situáciou, keby sa na dosiahnutie cieľa zvolil inštitút vydania, resp. odňatia veci. Napokon to potvrdzuje aj rozdielny režim realizácie uvedených prostriedkov. Vyzvať podľa § 89 ods. 3 Trestného poriadku na vydanie veci je policajt oprávnený bez toho, aby potreboval príkaz či súhlas prokurátora. K odňatiu veci podľa § 91 ods. 1 Trestného poriadku môže policajt pristúpiť na základe vlastného príkazu vydaného po predchádzajúcom súhlase prokurátora, bez predchádzajúceho súhlasu prokurátora môže policajt vydať príkaz len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť a vec neznesie odklad. Naproti tomu na realizáciu úkonu uchovania a vydania

[376] Návrh Nariadenie Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach COM/2018/225 final - 2018/0108 (COD). [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

[377] Európska rada: Rada Európskej komisie. Nariadenie o cezhraničnom prístupe k elektronickým dôkazom: Rada sa dohodla na pozícii. [online]. [cit.1.9.2020]. Dostupné z: https://www.consilium.europa.eu/sk/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[378] Rozhodnutie ÚS SR zo dňa 25.8.2010 vo veci sp. zn. III. ÚS 68/2010-62.

počítačových údajov podľa § 90 Trestného poriadku potrebuje policajt nevyhnutne príkaz prokurátora ako orgánu vykonávajúceho dozor nad dodržiavaním zákonnosti pred začatím trestného stíhania a v prípravnom konaní (§ 230 Trestného poriadku). Policajt v danom konkrétnom prípade pre účely získania počítačových údajov zvolil prostriedok – zaistenie samotného počítačového vybavenia (z obsahu zápisnice nie je zrejmé, či išlo o úkon vydania alebo odňatia veci), ktorý pre tento účel zákonná úprava neumožňuje, jeho postup preto treba považovať za nelegálny.“

V neposlednom rade je potrebné uviesť, že OČTK by mali mať vypracovanú metodiku (*guidelines, best practices*) pre zaisťovanie a uchovávanie elektronických dôkazov. [379] Tieto interné pravidla sú často jediným spätným kontrolným mechanizmom v prípade nesprávneho zaobchádzania s elektronickým dôkazom v trestnom konaní, a to zo strany nadriadeného orgánu, súdu alebo inej dotknutej osoby. Aj keď tieto pravidlá nebudú verejné (napr. interné predpisy zaisťovania elektronických dôkazov Polície ČR), ich obsah je významný pre samotné trestné konanie a správny postup kriminalistických expertov. Metodika by mala rovnako obsahovať presný postup v prípade zaisťovania údajov z osobného profilu sociálnej siete a webstránky s aspektom zahraničnej spolupráce. Na druhú stranu, väčšina veľkých poskytovateľov sociálnych sietí publikuje odporúčania pre štátne orgány, akým spôsobom majú požadovať sprístupnenie údajov v prípade trestného konania (*best practices for law enforcements authorities*). V nasledujúcej podkapitole budú osvetlené práve tieto odporúčania.

5.3.2. Povinná osoba

Z pohľadu práva je poskytovateľ sociálnej siete a poskytovateľ web hostingu, resp. systému pre webstránky (blog, mikro blog atď.) v rovnakom právnom postavení. Často ide o poskytovateľa služby v informačnej spoločnosti. [380] Zaujímavá je tu otázka

[379] Ide o podobné odporúčania, aké publikuje Európska komisia v prípade miestneho šetrenia hospodárskej súťaže (dawn raid) a o spôsobe zaisťovania elektronických dôkazov. Viď European Commission: Explanatory note to an authorisation to conduct an inspection in execution of a Commission decision under Article 20(4) of Council Regulation No 1/2003 [online]. [cit.1.9.2020]. Dostupné z: https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf alebo Štandardy ISO. Viď ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. [online]. [cit.1.9.2020]. Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=44381

[380] § 2 ods.1 písm. d) poskytovatelem služby je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti. Viď Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů.

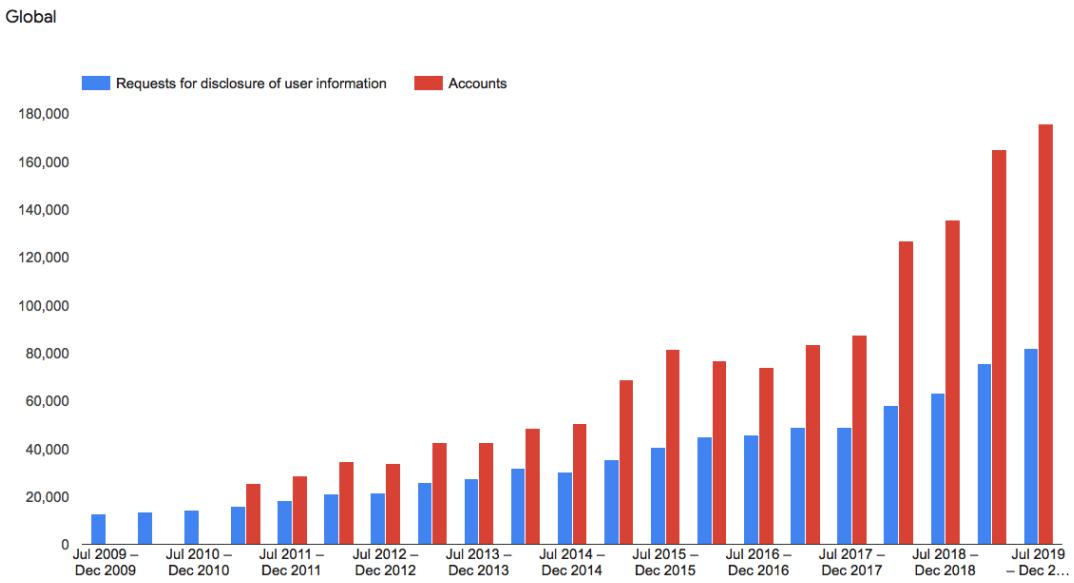
jurisdikcie vo vzťahu k zahraničným prevádzkovateľom. Podľa Mareka je jurisdikcia trestného orgánu delokalizovaných právnych vzťahov v kyberpriestore určená miestom protiprávneho následku: „*Co se týče jednání na Facebooku a deliktní způsobilosti občanů ČR, v rámci veřejnoprávních norem, v tomto případě především přestupků a trestných činů, jurisdikce českých soudů je dána tehdy, pokud následek nastane na území ČR nebo pokud ten, kdo poruší zákon, je českým občanem (blíže § 4–11 TrZ a § 8 PřesZ). S ohledem na skutečnost, že případné trestněprávní jednání v rámci sociální sítě probíhá na internetu, stačí, že takové jednání má následek v ČR (což má právě z povahy delokalizace právních vztahů v kyberprostoru vždy, kdy je tento následek dostupný v rámci připojení k internetu z ČR), a jurisdikce českých orgánů veřejné moci je dána.*“ [381] Ako už bolo uvedené, viacerí poskytovatelia sociálnych sietí publikujú odporúčania pre štátne orgány a rovnako sprístupňujú správy transparentnosti. [382] Ide o prehľadné a anonymné štatistiky o dožiadaní štátov a štátnych orgánov smerujúcich k vydaniu údajov a informácií o jednotlivých užívateľoch. [383] Tieto odovzdávané dáta často slúžia ako dôkazné prostriedky v trestnom konaní alebo ako poznatky bezpečnostných služieb (tzv. informačno-technické prostriedky). Príkladom správy transparentnosti je štatistika spoločnosti Google Inc., ktorá vypovedá o rastúcom trende dopytov štátnych orgánov za posledných päť rokov: [384]

[381] MAREK, T.: Autonomie vůle a soukromí na Facebooku. Právní rozhledy, Nakladatelství C. H. Beck 2015. č. 6/2015, Str. 196.

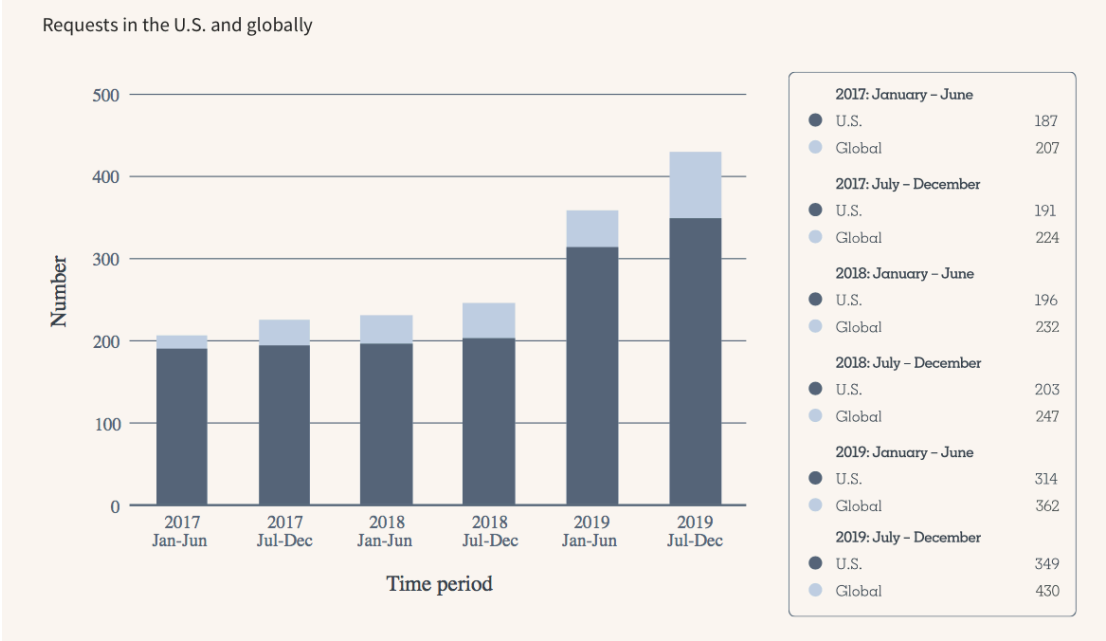
[382] Medzi prvými to bola spoločnosť Google (rok 2010), potom Twitter, Microsoft, Verizon, AT&T, Apple, Dropbox, Facebook, Yahoo and CloudFlare. Každá z týchto spoločnosti v súčasnosti zverejňuje správu transparentnosti o tom, ako sprístupňuje svoje dáta tretím osobám. Viď Transparency report. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2020. [online]. [cit.1.9.2020]. Dostupné z:http://en.wikipedia.org/wiki/Transparency_report

[383] Je potrebné dodať, že viaceré spoločnosti sú nútené pripúšťať nielen žiadosti orgánov štátnej správy, ale aj žiadosti súkromných osôb na odstránenie škodlivého obsahu. Príkladom môže byť medializovaný prípad španiela Maria Gonzalesa proti spoločnosti Google Inc., ktorý dosiahol stiahnutie odkazov na webové stránky o jeho osobe z výsledkov vyhľadávania, Viď Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014, No. C-131/12. Case-law of the Court of Justice [online]. 6.June 2013. [online]. [cit.1.9.2020]. Dostupné z:http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[384] Informácie o transparentnosti. Žiadosti od vládnych orgánov a súdov. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: https://transparencyreport.google.com/user-data/overview?hl=en



Obdobný trend potvrdzujú aj iné spoločnosti. Príkladom môže byť profesná sociálna sieť LinkedIn:[385]

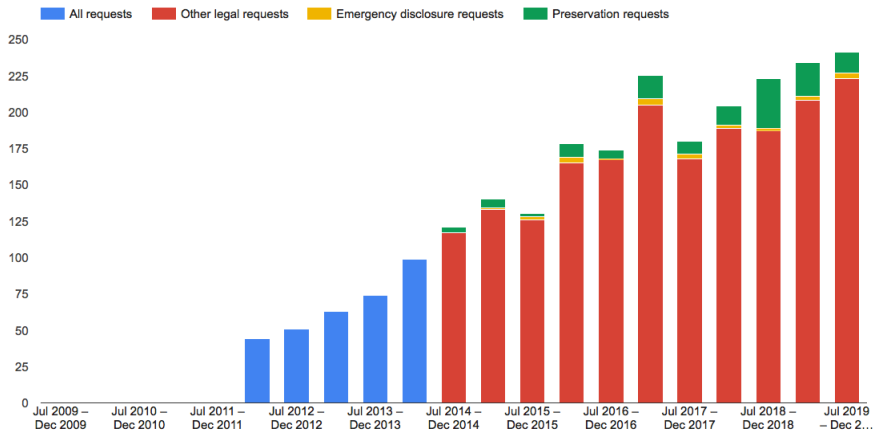


Je zrejmé, že žiadosti o sprístupnenie dát neprichádzajú len z krajiny sídla poskytovateľa sociálnej sieti alebo webovej prezentácie. Práve naopak, ide o strhujúci zápas množstva lokálnych jurisdikcií o výkon práva v kyberpriestore, v ktorom je ťažké určiť rozhodné právo.

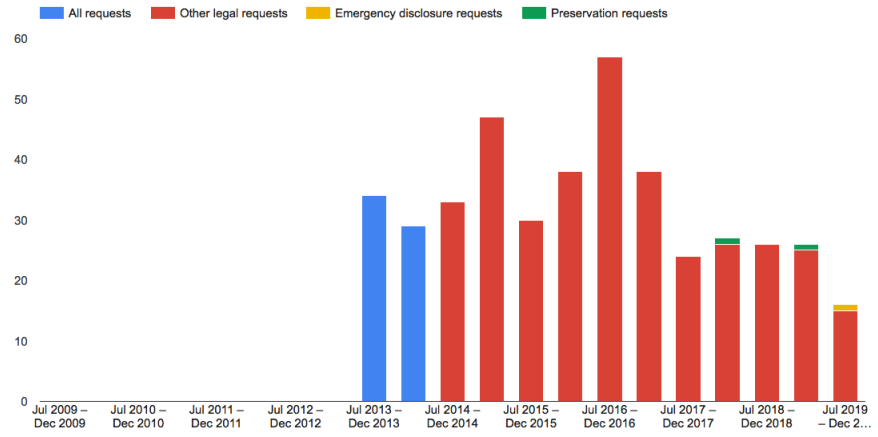
[385] Our Transparency Report. LinkedIn Inc. [online]. [cit.1.9.2020]. Dostupné https://about.linkedin.com/transparency/government-requests-report#government-requests-2019-2017

Za zmienku stojí taktiež prehľad žiadosti z ČR, SR a Švajčiarska na spoločnosť Google Inc.:[386]

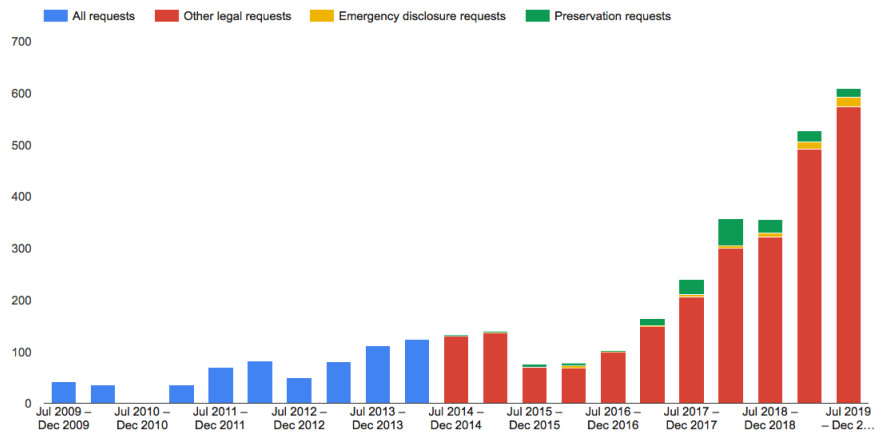
Czechia



Slovakia

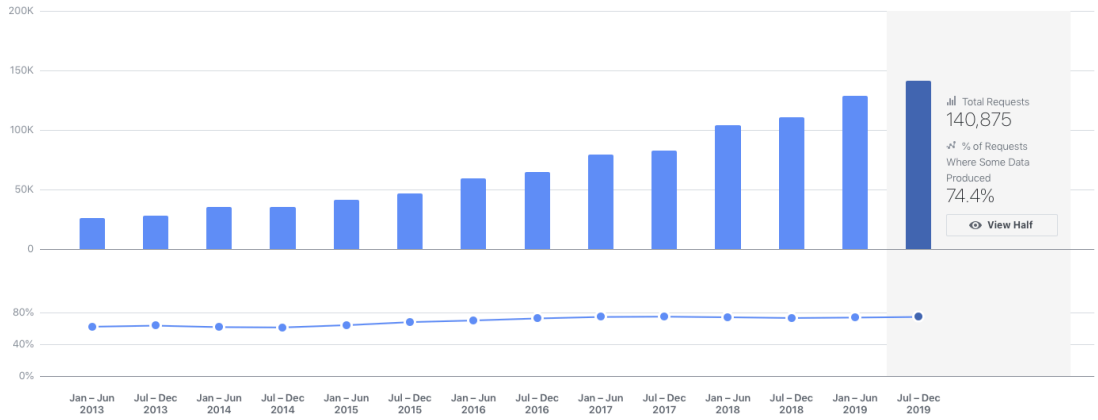


Switzerland



[386] Informácie o transparentnosti. Žiadosti od vládnych orgánov a súdov. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: https://transparencyreport.google.com/user-data/overview?hl=en

Zo štatistiky spoločnosti Facebook Inc. je rovnako zrejmý výrazný nárast žiadostí v minulom kalendárnom roku:[387]



Zvyčajne akceptujú poskytovatelia v rámci spolupráce so štátnymi orgánmi nasledujúce skupiny žiadostí:

- Žiadosti od štátnych orgánov týkajúce sa odstránenia obsahu
- Žiadosti týkajúce sa porušenia autorských práv
- Žiadosť o poskytnutie informácií o používateľoch

Žiadosť o poskytnutie informácií o používateľoch je ťažiskovým nástrojom pre získanie relevantných elektronických dôkazných prostriedkov. Prevádzkovatelia môžu spolupracovať tak vo veciach občianskeho procesného práva (napr. v angloamerickom práve ide o inštitút *ediscovery*), ako aj vo veciach trestného práva procesného. Tieto žiadosti je možné rozdeliť na žiadosti pochádzajúce zo štátu sídla poskytovateľa (napr. USA, členský štát EÚ – najčastejšie Írsko) a žiadosti mimo tento štát. Je pravidlom, že žiadosť musí byť vždy doplnená právoplatným a vykonateľným rozhodnutím štátneho orgánu. Typické rozhodnutia súdnych orgánov (v USA podľa anglo-amerického práva), na ktoré odkazujú napr. Google, Facebook, LinkedIn v prípade vydania informácií z účtu užívateľa, sú:[388]

Predvolanie (Subpoena)

- *ide o výsledok zjednodušeného procesu získavania prevádzkových údajov*

[387] Goverment requests report. Facebook Inc. [online]. [cit.1.9.2020]. Dostupné z: https://transparency.facebook.com/government-data-requests/jul-dec-2019

[388] Requests for user information. Legal process. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/legalprocess/

- *je vydané bez predchádzajúceho odsúhlasenia sudcom či úradníkom so súdnou právomocou*
- *predvolanie smeruje iba k špecifickému druhu prevádzkových informácii (taxatívne zákonom stanovených)*
- *vydáva sa v trestnoprávnych a občianskoprávnych záležitostiach*
- *Spoločnosť Google k tomuto nástroju uvádza, že „platné predvolanie týkajúce sa vašej adresy v službe Gmail nás môže donútiť k odhaleniu mena, ktoré ste uviedli pri vytváraní účtu, a adries IP, z ktorých ste účet vytvorili a z ktorých ste sa prihlásili alebo odhlásili (vrátane dátumu a času). Na prvý pohľad sa zdá, že zákon ECPA umožňuje orgánu vlády predvolaním alebo súdnym príkazom (viď popis nižšie) donútiť poskytovateľa komunikačných služieb k odhaleniu obsahu určitého typu e-mailov alebo iného druhu obsahu. Spoločnosť Google však v prípade obsahu služby Gmail a ďalších služieb vyžaduje príkaz k prehliadke vystavený na základe zákona ECPA. Sme totiž presvedčení, že len tak je to v súlade so štvrtým dodatkom Ústavy Spojených štátov, ktorý zakazuje neopodstatnenú prehliadku či konfiškáciu."*

Súdny príkaz na základe zákona ECPA (ECPA Court Order)

- *ide o zložitejší proces získavania prevádzkových a čiastočne aj obsahových údajov*
- *väčšinou tu je potrebný výslovný súhlas sudcu najčastejšie podľa trestného procesného práva*
- *žiadateľ musí pred súd predložiť konkrétne fakty dokazujúce, že požadované informácie sú relevantné a podstatné pre prebiehajúce vyšetrovanie trestného činu*
- *spoločnosť Google k tomuto nástroju uvádza, že „orgán vlády môže získať na základe takého súdneho príkazu tie isté informácie ako na základe predvolania a dodatočné podrobnejšie informácie o používaní účtu. K tým môže patriť adresa IP, ktorá je priradená ku konkrétnemu e-mailu odoslanému z daného účtu alebo sa použila na zmenu hesla k účtu, (s dátumom a časom) a časť hlavičky e-mailu, ktorá nie je súčasťou obsahu e-mailu, napríklad pole „Od:“, „Komu:“ a „Dátum“. Súdny príkaz na základe zákona ECPA je možné získať iba v prípade trestnoprávneho vyšetrovania."*

Príkaz k prehliadke (Search Warrant)

- *je to výstup z najprísnejšieho procesu získavania obsahových údajov*

- *žiadateľ musí získať súhlas súdu a musí preukázať dôvodné podozrenie, že „kontraband alebo určité informácie súvisiace so zločinom sa aktuálne nachádzajú na konkrétnom mieste, ktorého prehliadka sa požaduje".*
- *príkaz k prehliadke musí špecifikovať miestá, ktoré majú byť prehľadané, ako aj cieľ hľadania*
- *podľa spoločnosti Google „s príkazom k prehliadke je možné vynútiť sprístupnenie tých istých informácií ako s predvolaním na základe zákona ECPA či súdnym príkazom, ale aj sprístupnenie informácií o vyhľadávacích dopytoch používateľa alebo súkromného obsahu uloženého v účte Google, ako sú správy služby Gmail, dokumenty, fotografie či videá YouTube. Príkaz k prehliadke na základe zákona ECPA je k dispozícii iba v prípade kriminálneho vyšetrovania. Vo videu nižšie je uvedený prehľad, ako kontrolujeme a reagujeme na príkazy k prehliadke na základe zákona ECPA."*

Povolenie odpočúvania (Wiretap)

- *je to najkomplikovanejší spôsob získavania (zaznamenávanie) obsahových údajov v reálnom čase – ide o odpočúvanie obsahu komunikácie v reálnom čase (odpočúvanie a záznam telekomunikačnej prevádzky)*
- *vyšetrujúci orgán/OČTK musí preukázať, že a) používateľ sa dopustil zločinu uvedeného v zákone o odpočúvaní Wiretap Act[389], b) cieľom odpočúvania je získať informácie o danom zločine, c) odpočúvané telefónne číslo alebo účet súvisia s daným zločinom, a navyše súd musí stanoviť, že všetky „štandardné spôsoby vyšetrovania tohto zločinu zlyhali (alebo by pravdepodobne zlyhali), prípadne že sú predovšetkým príliš nebezpečné na to, aby sa realizovali“*
- *je si nutné uvedomiť, že existujú zákonné obmedzenia týkajúce sa doby (lehoty) na zákonné odpočúvania a tiež požiadaviek na informovanie odpočúvaných používateľov (za akých môžu byť s povolením oboznámení)*

Povolenie sledovania prichádzajúcej alebo odchádzajúcej komunikácie (Pen Register, and Trap and Trace)

[389] 18 U.S. Code Chapter 119 - Wire and electronic communications interception and interception of oral communications. [online]. [cit.1.9.2020]. Dostupné z: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

- *ide o pomerne jednoduchý proces získavania prevádzkových údajov v reálnom čase (IP, web adresa, logy atď.)*
- *žiadateľ musí preukázať, že informácie, ktoré sa získajú, budú relevantné pre aktuálne prebiehajúce vyšetrovanie trestného činu (opäť ako možnosť pre OČTK v trestnom konaní)*
- *zaujímavosťou je, že spoločnosť Google sa domnieva, že v tomto prípade ide o príliš nízky štandard ochrany práv jej užívateľov, a preto začala spolupracovať so združením Digital Due Process s cieľom zabezpečiť to, aby tieto povolenia podliehali súdnej kontrole*

V prípade, ak sa tuzemský OČTK rozhodne využiť inštitút právnej pomoci na základe medzinárodnej dohody o vzájomnej právnej pomoci (napr. prostredníctvom Ministerstva spravodlivosti USA), často musia jeho rozhodnutia alebo rozhodnutia súdov splniť vyššie uvedené štandardy (minimálne s nimi korešpondovať). Je potrebné dodať, že internetový poskytovatelia sa môžu rozhodnúť dobrovoľne spolupracovať, a to aj bez formálneho medzinárodného postupu právnej pomoci. Ide o prejav transparentnosti a právomoci poskytovateľa v kyberpriestore týkajúceho sa sociálnych sietí.[390]

Domnievame sa, že dobrovoľné vydávanie údajov definičnými autoritami – cezhraničná výmena osobných údajov bude ovplyvnená extrateritoriálnou politikou štátov alebo rozhodnutiami podobnými tým, akými sú napr. rozhodnutie SDEÚ vo veci Schrems II.[391] Niektoré krajiny sa vydali svojou vlastnou cestou. Napr. americký zákon CLOUD Act priniesol pre USA možnosť nového spôsobu prístupu k dátam uloženým

[390] Napr. spoločnosť Google uvádza, že *„údaje používateľa môže v reakcii na platný právny proces zo strany orgánov vlád iných krajín ako USA poskytnúť dobrovoľne, pokiaľ sú tieto žiadosti v súlade s medzinárodnými normami, americkým právom, pravidlami spoločnosti Google a zákonmi krajiny, z ktorej žiadosť pochádza."* Viď Request for user information. Legal process. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/legalprocess/

[391] V tomto prípade súd vyhlásil koncept rozhodnutia Európskej komisie o ochrane súkromia *(Privacy Shield)* za neplatný z dôvodu invazívnych programov dohľadu v USA, čím sa transfer osobných údajov do USA na základe tohto rozhodnutia stal nelegálnym. Niektoré americké sociálne siete doposiaľ uvádzajú, že sa spoliehajú práve na *Privacy Shield* pri cezhraničnom spracovaní osobných údajov. Je možné očakávať zmeny v ich pravidlách, resp. všeobecných podmienkach o ochrane osobných údajov, najmä v podobe návratu k modelovým zmluvným podmienkam v zmysle GDPR alebo k presunu ich spracovateľských činností do teritória EÚ. Viď Rozhodnutie SDEÚ vo veci Data Protection Commissioner v Facebook Ireland and Maximillian Schrems zo dňa 16.7.2020, C-311/18.

u amerických definičných autorít. Umožňuje federálnym orgánom prinútiť americké definičné autority prostredníctvom príkazu alebo predvolania k poskytnutiu požadovaných údajov uložených na servroch bez ohľadu na to, či sú údaje uložené v USA alebo na cudzej pôde. Vytvoril tým *„medzinárodnú normu cestou národnej regulácie."*[392]

5.4. Forenzná analýza

Odborná zahraničná literatúra v prípade forenznej analýzy „internetových dát" hovorí o nasledujúcich krokoch:[393]

- vyhodnotenie získaných dát,
- experimentovanie (pripustenie nových neortodoxných techník),
- spájanie informácií a hľadanie vzájomných súvislostí, a
- validácia (overovanie faktov a skutočností).

Forenzná analýza dát získaných od poskytovateľov sociálnych sietí je predovšetkým determinovaná výberom technického spôsobu odovzdania dát OČTK.

V prípade dobrovoľného odovzdania požadovaných dát ide o proces:

- odovzdania dátového nosiča (HDD, USB, CD, DVD atď.) spolu s preberacím protokolom,
- sprístupnenia vzdialeného úložiska s požadovanými dátami (SFTP, zabezpečená webstránka, SSH prístup atď.) a verifikovateľným logovacím systémom, a
- následnú kriminalistickú analýzu vykonanú povereným súdnym znalcom.

V prípade nedobrovoľného zaistenia požadovaných dát ide často o odňatie dátových nosičov (HDD, USB, CD, DVD atď.), resp. celých počítačových systémov (hardware) a servov. Taktiež nie je vylúčená možnosť kopírovania dát na mieste.

[392] KESSELOVÁ, Katarína. Cezhraničný prístup k elektronickým dôkazom v trestných veciach. Visí vo vzduchu európsky Cloud act?. Revue pro právo a technologie. 2019, č. 19, Str. 41-68.

[393] Ibid MASON, Stephen. Electronic evidence. London: LexisNexis. 2010. Str. 65.

Rovnako môže ísť o zaistenie priestorov (zapečatenie) a následnú analýzu tam nájdených počítačov (servrov).

Pri týchto úkonoch je nutné apelovať na uvedenú zásadu zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktorá sa premieta aj do práce poverených súdnych znalcov alebo znaleckých organizácií. Špecifikum skúmaných dát z osobných profilov je ich previazanosť s cudzími dátami (nezaujatými osobami), ku ktorým je nutné pristupovať obzvlášť opatrne. Navyše je možné doplniť, že skúmané dáta by v čase konania mali byť uložené na objektívne verifikovateľnom zdroji s tým, že každá zo strán by mala presne stanovené práva a povinnosti pri nahliadaní, resp. nakladaní s obsahom. Je zrejmé, že tieto úskalia sa dnes pomerne často odbíjajú znaleckým dokazovaním, ktoré si však žiada neúnosné časové nároky na priebeh sporu a často zbytočne, resp. nezákonne, prejudikuje právne otázky.

5.5. Vykonanie dôkazu

Každý dobre vykonaný dôkaz by mal predstavovať záruku reflektovania minulých dejov (slovami Holländera *„fair spôsob vedenia dôkazného konania"*).[394] Je preto zrejmé, že existuje úzka väzba kategórie pravdivosti na povahu konania, akým je práve vykonanie dôkazu prostredníctvom elektronického dôkazného prostriedku. Súd v trestnom konaní bude vykonávať dôkazy získané zo sociálnych sietí alebo webstránok najmä na základe ustanovení § 112 ods 1 a 2 TŘ (ako listinný dôkaz), § 105 TŘ (znalecké posudky, odborné vyjadrenia), resp. § 101 TŘ (ako výsluch svedka) alebo § 113 TŘ (ako obhliadku). Avšak súčasná prax často spočíva v tom, že vykonanie dôkazu osobného profilu alebo webstránky sa ohraničuje na tlač získaných informácií do listinnej podoby a jej predloženie súdu.[395] Z technického pohľadu sa tak zbytočne stráca širšia suma informácií (metadáta súborov, zdrojový kód atď.), ktoré nie sú síce

[394] HOLLÄNDER, Pavel. Filosofie práva. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, ISBN 80-868-9896-2. Str. 204.

[395] Typicky to je napr. v prípade stalkingu, kedy *„soudy obou stupňů vyšly především z doslovného znění obsahu výhrůžky, aniž by důsledně hodnotily okolnosti, za nichž jí bylo užito, a to ve spojení s poznatky o chování obviněného k poškozené. Soud prvního stupně z výpovědi svědkyně K. T., s níž korespondují i záznamy komunikace mezi ní a obviněným na facebooku založené ve spise, zjistil, že v komunikaci s ní se obviněný ve dnech 11. 2. a 12. 2. 2009 vyjádřil tak, že „ju zabije", přičemž z kontextu jeho sdělení bylo patrné, že tím míní poškozenou a že tak chce učinit za vulgární nadávky, jimiž ho označila právě poškozená (č. l. 29, 30)."* Usnesení NS ČR ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011.

okamžite viditeľné, ale môžu predstavovať zaujímavý zdroj informácií. ÚS ČR sa už dávnejšie zaoberal požiadavkami zákazu deformácie dôkazov a uviedol, že:[396]

„Podle názoru Ústavního soudu musí obecný soud dodržet vysoký standard i tam, kde jde o hodnocení vypovídací schopnosti a hodnověrnosti důkazu samotného. Jde¬li o hodnocení důkazů, procesní předpisy sice ponechávají volnost soudci obecného soudu, avšak nemůže jít o volnost absolutní, nevázanou na zkušenostmi prověřenou pravděpodobnost určitých skutečností. Důkaz musí být odrazem skutečných událostí a situací, což má garantovat, aby byl jednotlivec uznán vinným na podkladě objektivních a skutečnosti odpovídajících zjištění, protože pouze ona jsou způsobilá ospravedlnit krajní opatření spočívající ve zbavení jednotlivce jeho osobní svobody (nález Ústavního soudu, sp. zn. IV. ÚS 335/05, Sbírka nálezů a usnesení, svazek 41, str. 453). Právě z tohoto důvodu lze formulovat určité principy vážící se k provádění a hodnocení důkazů, např. princip opomenutého důkazu, princip možnosti verifikace důkazů směřujících proti obžalovanému či zásadu zákazu deformace důkazů; aplikace těchto principů je dovoditelná i z nálezu Ústavního soudu, sp. zn. III. ÚS 398/97, Sbírka nálezů a usnesení, svazek 11, str. 125, v němž jde o zákaz vyvozování z důkazu takových skutkových zjištění, která při racionálním zhodnocení z provedeného důkazu nevyplývají, a nejsou podporována ani obecnou zkušeností."

Ďalšou vlastnosťou elektronického dôkazu je aj to, že elektronický záznam sa môže pomerne jednoducho a nepozorovane (automaticky) modifikovať alebo zmeniť. A to aj v čase jeho vykonávania. Takáto zmena je spôsobená povahou alebo okolnosťami, za ktorých bolo s týmto záznamom nakladané. Inak povedané, už len samotným kopírovaním záznamu dát sa môže kontaminovať ich obsah.[397] Kľúčom k správnemu vykonávaniu elektronických dôkazov je pochopenie kategórie vlastnosti samotným súdom (potencionálnej ubiquity a volatility, spoľahlivosti a integrity, pravdivosti a vierohodnosti, platnosti a zákonnosti). Ide o správne chápanie dôkazného procesu od počiatočnej fázy – zaisťovania počítačových údajov až po hodnotenie dôkazov.

[396] Nález ÚS ČR ze dne 29. 4. 2009, sp. zn. I. ÚS 3094/08.

[397] ÚS ČR už dávnejšie uviedol, že *„účelem trestního řízení není jen náležité zjištění trestných činů a potrestání pachatelů, nýbrž i projednání věcí s plným šetřením práv a svobod zaručených Listinou a mezinárodními smlouvami o lidských právech a základních svobodách, jimiž je Česká republika vázána."* Nález ÚS ČR ze dne 25. 11. 2010, sp. zn. II. ÚS 889/10.

5.6. Hodnotenie dôkazu

Za dôkazný prostriedok je možné označiť zákonom upravený spôsob získania informácie (skutočnosti, ktorá má byť zistená – porov. § 89 ods. 1 TŘ). Za dôkaz môže slúžiť všetko, čo môže prispieť k objasneniu veci, najmä výpovede obvineného a svedkov, znalecké posudky, veci a listiny dôležité pre trestné konanie a ohliadka. Ako už bolo uvedené, každá zo strán môže dôkaz vyhľadať, predložiť alebo jeho vykonanie navrhnúť. Skutočnosť, že dôkaz nevyhľadal alebo nevyžiadal OČTK, nie je dôvodom na odmietnutie takéhoto dôkazu.

Trestné procesné právo týkajúce sa otázky dokazovania je vystavané na zásade voľného hodnotenia dôkazov, avšak len za predpokladu dodržania ostatných právnych zásad. Ako sme uviedli vyššie v našej práci, podľa Holländera má dokazovanie pre právne rozhodovanie okrem noetickej podstaty práve aj funkciu presvedčovania a argumentovania[398]. Preto je možné tiež hovoriť o oceňovaní dôkazu, resp. hľadaní jeho sily.[399] Tento proces je sfinalizovaný predložením úplného súhrnu dôkazov, avšak správna bonifikácia dôkazných partikularít je o to viac dôležitejšia ak ide o použitie elektronických dôkazných prostriedkov. Podľa Smejkala majú elektronické dôkazné prostriedky jednu zásadnú slabinu: *„ťažko ich priraďujeme ku konkrétnej osobe, pretože dokázať, kto „mal ruky na klávesnici" je možné len s využitím elektronického podpisu alebo iných autentizačných metód (použitie hesla, SMS, čipové karty atď.). Našťastie sú zvyčajne súčasťou kruhu ďalších, hoci nepriamych dôkazov a môžu aj v tomto prípade zohrať dôležitú úlohu v rámci príslušného konania."* [400] Práve informácie z osobných profilov (webstránok) môžu často priniesť ďalšie nepriame dôkazy, ktoré nasvedčujú dokazovaným skutočnostiam. Súdom riešený problém vytvorenia falošného Facebookového profilu (trestný čin poškodzovania cudzích práv) zdôraznil významný aspekt hodnotenia elektronických dôkazov v nadväznosti na ujmu práv poškodenej:[401]

[398] Ibid. HOLLÄNDER 2006. Str. 195.

[399]BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. Teorie práva. Vyd. 1. Praha: Eurolex Bohemia, 2001. ISBN 80-86432-13-0. Str. 132.

[400] SMEJKAL, Vladimír. Elektronické důkazy – současnost či budoucnost českého soudnictví? Bulletin-advokace.cz. [online]. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-dukazy-soucasnost-ci-budoucnost-ceskeho-soudnictvi

[401] Usnesení NS ČR ze dne 22. 7. 2014, sp. zn. 4 Tdo 815/2014-37.

„Není žádných pochyb o tom, že zpřístupnění fotografií, na nichž je poškozená zachycena nahá při provádění soulože bez souhlasu poškozené širokému okruhu osob, a to způsobem vyvolávajícím dojem, že tyto fotografie zpřístupnila samotná poškozená, vážnou újmu na uvedených právech poškozené způsobuje. O tom ostatně svědčí i popis dopadu jednání obviněného na poškozenou obsažený ve výpovědi poškozené, ale i dalších svědků. Pokud jde o tvrzení obviněného o absenci znaku uvedení v omyl, nelze se s tímto ztotožnit. Obviněný založil facebookový profil na jméno poškozené, uvedl zde kontaktní údaje na ni a zveřejnil její fotografie. Jednoznačně tímto způsobem byly osoby, kterým k profilu bylo umožněno přistoupit, uváděny v omyl ohledně majitele profilu. Obdobné závěry platí i o dopisech, které obviněný psal jménem poškozené v první osobě s uvedením adresy poškozené jako odesílatele na obálkách. Rovněž pokud soud prvního stupně dochází k závěru, že obviněný využil omylu poškozené, která nepředpokládala, že její intimní fotografie pořízené s jejím souhlasem obviněný tímto způsobem zneužije, je možno se s takovým závěrem ztotožnit. […] Nejvyšší soud po prostudování předmětného spisového materiálu zjistil, že soudy srozumitelně popsaly subjekty uvedené v omyl, jakož i subjekt, jemuž byla způsobena újma na právech a rovněž podrobně vyložily, proč bylo jednání obviněného JUDr. PhDr. I. S., PhD. kvalifikováno jako přečin poškození cizích práv podle § 181 odst. 1 písm. a), b) tr. zákoníku, ale také to, v čem spočívala vážná újma na právech a komu byla způsobena. Nutno uvést, že intenzita škodlivého následku rozhodně nebyla v posuzovaném případě zanedbatelná, neboť poškozená J. T. byla zveřejněním jejích intimních fotografií zesměšněna, v souvislosti s inkriminovanými dopisy musela podávat vysvětlení svým nadřízeným, byly prověřovány její odměny a byla řešena i její bezpečnostní prověrka u Národního bezpečnostního úřadu. Při posouzení uplatněné právní námitky proto Nejvyšší soud dospěl k závěru, že znaky skutkové podstaty přečinu poškození cizích práv podle § 181 odst. 1 písm. a), b) tr. zákoníku byly naplněny.“

Na záver možno už len dodať, že v priebehu trestného konania je nutné postaviť výsledky dokazovania do svetla poznania, ktoré bude založené na úsilí priblížiť sa zhode myšlienky so skutočnosťou (minulým dejom) v tej miere, ktorá zodpovedá tak požiadavkám overovania, ako aj falzifikovania, ktoré je možné v určitej dobe na túto mieru priblíženia položiť.[402] Tieto požiadavky overovania, ako aj falzifikovania, musia

[402] Ibid. HOLLÄNDER 2006, Str. 201.

primárne vychádzať zo zásad a princípov trestného práva, avšak rovnako musia brať na zreteľ existujúce technikality dôkazov pochádzajúcich z osobných profilov sociálnych sietí alebo webových prezentácií.

5.7. Špecifikum IP adresy

Rozhodovacia prax a odborná verejnosť ponúka v súčasnosti len náhodilé a útržkovité riešenia o elektronickom dôkaznom prostriedku a vyťaženom dôkaze v podobe IP adresy. Ako príklad môže poslúžiť otázka ochrany autorského práva a identifikácia jeho rušiteľa na internete. Pre identifikovanie osôb je často nevyhnutné získať IP adresu alebo okruh IP adries počítačov alebo zariadení, z ktorých je škodlivá činnosť vykonávaná alebo kde dochádza k porušovaniu autorských práv. Ide o otázku pasívnej legitimácie, ktorá sa v praxi obchádza zneužívaním nástrojov trestného práva procesného. Napríklad podľa výskumu stúpa počet žiadostí Policajného zboru SR o poskytnutie údajov o uskutočnenej telekomunikačnej prevádzke v oblasti porušenia autorských práv, ktoré sú odôvodnené ustanovením § 76a ods. 3 zákona č. 171/1993 Z.z. o Policajnom zbore alebo dokonca všeobecnou povinnosťou súčinnosti podľa § 76, resp. § 76a tohto zákona.[403] Je potrebné dodať, že využívanie databáz, ktoré existujú, na iné účely, než ktoré boli takto stanovené zákonodarcom, je v rozpore so zásadami ochrany osobných údajov.[404]

Otázkou zostáva, čo je to IP adresa a ako môže byť zaistená – identifikovaná, resp. či je spôsobilá prispieť k identifikácii škodcu alebo rušiteľa? Z technického hľadiska sú jednotlivé uzly internetovej siete, teda servre, ktoré poskytujú určité služby,

[403] Vzorové podanie na ÚS SR vo veci plošného sledovania občanov. In: European Information Society Institute. [online]. [cit.1.9.2020]. Dostupné z: https://www.eisionline.org/images/finish%20-%20podanie%20na%20ussr.pdf

[404] Vo svetle rozhodnutia Súdneho dvoru EÚ v spojených veciach Digital Rights Ireland C--293/12 a C-594/12[404], kde súd vyslovil, že smernica o data retention zasahuje mimoriadne závažným spôsobom do základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, tieto otázky zneužívania *data retention* iste nadobudnú nový spoločenský rozmer a neostanú bez povšimnutia. Dňa 23.4.2014 pozastavil ÚS SR účinnosť ustanovení § 58 ods. 5 až ods. 7 a § 63 ods. 6 ZEK, ktoré prikazovali operátorom sledovať komunikáciu svojich užívateľov. Urobil tak v konaní, ktoré s pomocou 30 poslancov Národnej rady SR iniciovala organizácia European Information Society Institute. Rozhodnutie ÚS SR zo dňa 29. apríla 2015, PL. ÚS 10/2014.

identifikované celosvetovou unikátnou IP adresou.[405] V praxi je uznávaný názor, že IP adresa identifikuje miesto pripojenia technického zariadenia, nie priamo osobu (škodcu, rušiteľa, resp. páchateľa). Táto skutočnosť by mala byť zrejmá stranám súdneho procesu pred vypracovaním znaleckého posudku v súvislosti s identifikáciou IP adresy, aby sa predchádzalo neželaným právnym záverom, ktoré nepatria do znaleckého posudku. Podľa Kovárníka *„IP adresa, odkiaľ boli vykonávané úkony na internete, dokazuje iba miesto pripojenia, teda počítač alebo sieť počítačov. Samotná IP adresa z princípu nemôže dokazovať činnosť konkrétnej osoby, pretože nie je zjavné, kto v danom okamihu pri počítači sedel a napr. posielal e-maily. Pri dokazovaní trestného činu potrebujeme IP adresu, na ktorú odkazujú dostupné záznamy sieťovej prevádzky, doplniť o ďalšie dôkazy, z ktorých vyplýva, že dotknutá osoba v predmetnom čase pracovala s počítačom majúcim túto IP adresu.“*[406] Je možné konštatovať, že tuzemská rozhodovacia prax zaujala obdobné stanovisko. NS ČR v staršom trestnom rozhodnutí vo veci porušovania autorského práva pomocou programu DC ++ v súvislosti s elektronickým dôkazným prostriedkom – záznamom o IP adrese „páchateľa“ ako nosného dôkazu okrem iného konštatoval, že: *[407]*

„S ohledem na shora uvedené závěry soudů obou stupňů v rámci průběhu trestního řízení musí konstatovat, že ačkoli oba soudy tvrdí opak, tyto závěry postrádají spolehlivý podklad právě pro jednoznačné a nezpochybnitelné určení osoby pachatele a tato otázka nemůže být náležitě vyřešena pouhými obecnými tvrzeními, že obviněný pracuje u výrobce počítačových komponentů, dále poukazem na pornografický charakter jednoho audiovizuálního díla a potřebné schopnosti pro práci s počítačovým programem DC++ a sdílení souborů na síti, které má podle názoru obou soudů jen obviněný, a to na rozdíl od své přítelkyně, která předmětný osobní počítač sice také užívala, ale vzhledem k jejímu vzdělání (pánská krejčová) a zájmům šlo nejpravděpodobněji o prohlížení snadno přístupného obsahu, jako např. webových

[405] Vďaka IP adresám možno ľahko využiť akúkoľvek internetovú službu, nájsť každú konkrétnu stránku. IP adresy sú tvorené akýmsi kódom: v prípade staršieho prenosového protokolu IPv4 má adresa podobu čísel oddelených bodkami, napr. 217.31.201.43, a v prípade novšieho protokolu IPv6 sa jedná o kombináciu čísel a písmen oddelených dvojbodkami, napr. 2001:200:8002: 203:47 ff: fea5: 3085. Viď Jak na internet. CZ.NIC, z.s.p.o. Doména, IP adresa, DNS [online]. [cit.1.9.2020]. Dostupné z: http://www.jaknainternet.cz/page/1261/domena,-ip-adresa,-dns/

[406] KYNCL, op. cit.

[407] Usnesení NS ČR ze dne 27. 1. 2010, sp. zn. 5 Tdo 31/2010.

stránek, přičemž sdílení souborů na síti vyžaduje hlubší zkušenosti s prací na počítači, které L. Š. Nemá.“

Záznam o IP adrese sa tak dostáva do postavenia podporného dôkazu. Na druhej strane o „výpovednej neschopnosti“ IP adresy je možné protirečiť judikatúrou SDEÚ, ktorý IP adresu považuje za osobný údaj.[408] Podobné stanovisko zaujal NSS ČR vo veci priestupku a identifikácie IP adresy. Vo svojom rozhodnutí uviedol, že: [409]

„Pro účely nyní posuzované věci lze z uvedeného závěru vyvodit, že jestliže může IP adresa za určitých okolností představovat osobní údaj, tedy údaj, na jehož základě lze identifikovat (přímo či nepřímo) nějakou konkrétní osobu, pak může sloužit také jako důkaz v přestupkovém řízení.“ Avšak zdôraznil, že „pouze jako důkaz nepřímého charakteru.“

Zaujímavou otázkou je možnosť manipulácie s IP adresou. Nakoľko elektronický dôkazný prostriedok má vysokú volatilitu, je nutné skúmať v procese dokazovania aj takúto skutočnosť, resp. námietku. Avšak tá musí byť založená na racionálnom argumente a v závislosti od toho-ktorého procesu dostatočne podložená dôkazom namietateľa. Nesmie zostať v rovine teoretických úvah. Podobná námietka bola riešená pred ÚS ČR, ktorého závery viedli ku konštatovaniu:[410]

„Rozhodující soudy obracely přiměřenou pozornost i k dalším technickým možnostem neautorizovaného přístupu k "domácímu" počítači stěžovatele. Je též akceptovatelný závěr obecných soudů, že stěžovatelovy úvahy ohledně možné manipulace s otiskem "pracovního" počítače představují jen teoretickou aobecnou konstrukci, a bez ústavněprávní relevance – vzhledem k výše konstatovanému – pak zůstává, že v řízení nebyly zajištěny některé z dosažitelných důkazů.“

Ďalej za ťažko udržateľnú námietku o zneužití IP adresy, najmä v prípade dôkaznej núdze, je nutné považovať aj tvrdenie spočívajúce v tom, že neznáma osoba sa

[408] Ten vo svojom rozhodnutí zo dňa 29. 1. 2008, sp. zn C-275/06, Produtores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU, považoval IP adresu v kontexte daného prípadu (Promusicae požadovala po Telefónice odhalenie identít osôb, ktorým poskytovala pripojenie na internet a ktorých bola známa ich IP adresa a dátum a čas pripojenia) za osobný údaj v zmysle predpisov na ochranu osobných údajov.

[409] Rozsudek NSS ČR ze dne 4. 2. 2009, č. j. 1 As 90/2008-189.

[410] Usnesení ÚS ČR ze dne 19. 9. 2013, sp. zn. III. ÚS 1077/13.

nedovoleným spôsobom pripojila do súkromnej WiFi siete.[411] Je zrejmé, že takéto tvrdenie musí byť podporené ďalšími dôkazmi, a to najmä technologickými možnosťami a formou zabezpečenia predmetného WiFi spotu. Opätovne je nutné zdôrazniť, že IP adresa má v tomto prípade len druhotný a podporný charakter a správne skúmanie technického pozadia celého prípadu môže priniesť ďaleko širšie informácie (MAC adresa, IP adresa za NAT atď.).

Súdna prax taktiež riešila otázku príkazu k domovej prehliadke podľa § 83 ods. 1 TŘ, kde bol priestor okrem iného identifikovaný nesprávnou IP adresou. ÚS ČR v konkrétnom prípade vo svojom odôvodnení uviedol: [412]

„Napadený příkaz k domovní prohlídce vyhovoval zákonným požadavkům, neboť z něj bylo zřejmé, kdo jej vydal, o podezření z jakého trestného činu se jednalo, kde se měla prohlídka vykonat, kdo mohl být pachatelem trestné činnosti a rovněž jaké byly důvody vzniku podezření ze spáchání konkrétního trestného činu. Pochybení v podobě nesprávně uvedené IP adresy nebylo takového rázu, aby, přihlédnuto k okolnostem případu, zakládalo pochybnosti o důvodnosti nařízení domovní prohlídky, resp. činilo příkaz k domovní prohlídce nepřezkoumatelným.“

V neposlednom rade je potrebné spomenúť rozhodnutie v správnom súdnictve, ktoré riešilo otázku zablokovania IP adresy konkrétnej osobe:[413]

„Zablokování určité IP adresy prostřednictvím jejího zařazení na tzv. blacklist poskytovatelem služeb v oblasti kybernetické bezpečnosti za účelem ochrany elektronické podatelny správního orgánu (§ 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů) není nezákonným zásahem do práv podatele, ledaže správní orgán zablokoval IP adresu svévolně.“

S týmto súvisí otázka či IP adresa môže predstavovať osobný údaj. Aj keď SD EÚ konštatoval, že IP adresa je osobným údajom,[414] súhlasíme s Haraštom a Míšekem, totiž „*pokud někde existuje informace, která může IP adresu doplnit tak, aby*

[411] Usnesení NS ČR ze dne 22. 3. 2012, sp. zn. 6 Tdo 89/2012.

[412] Usnesení ÚS ČR ze dne 14. 12. 2011, sp. zn. IV. ÚS 3225/09.

[413] Rozsudek Nejvyššího správního soudu ze dne 6. 3. 2019, č. j. 2 As 153/2018-31.

[414] Rozsudek SDEU z 19. 10. 2016, C-582/14, Breyer v. Německo.

identifikovala konkrétní zařízení a tím jedince, je IP adresa osobním údajem.“ Autori správne uvádzajú, že existujú okolnosti, za ktorých IP adresa nemôže byť individualizovaná, najmä v prípade *„fenomén Internet of Things. Jeho principem je připojení velkého množství zařízení, které však nejsou provázány s konkrétním člověkem. Jedná se například o různá čidla monitorující své okolí, elektronické spotřebiče, systémy řídící klimatizaci a podobně. V takovém případě není možné vytvořit podobnou vazbu mezi zařízením a člověkem jako například v případě mobilních telefonů, nebo osobních počítačů a nemůže se proto jedna o osobní údaje.“*[415] Domnievame sa, že záznam o IP adrese môže priniesť zásadne zistenia pre rozhodovanie súdu (napr. ak si domnelý vrah vyhľadáva obeť z počítača), ale takýto záznam nesmie ostať osamote, a to bez podpory iných dôkazov (napr. išlo o osobný mobil s rozpoznávaním tváre užívateľa pre jeho otvorenie). V opačnom prípade predstavuje riziko pre hľadanie práva. Inak povedané, v ideálnom prípade pôjde zväčša o podporný dôkaz (indíciu), ktorý je nutné poistiť ďalšími dôkazmi.

5.8. Zhrnutie kapitoly

V uvedenej kapitole bolo popísané, akým spôsobom je možné získať, analyzovať, vykonať a hodnotiť elektronický dôkazný prostriedok pochádzajúci z osobných profilov sociálnych sietí alebo webových stránok. Tieto „internetové dôkazy“ ukazujú špecifickú vlastnosť *ubiquity* kyberpriestoru, t.j. vlastnosť bez previazanosti na lokálnu jurisdikciu a jej právne zásady a princípy. Právny proces vydávania dát bude nepochybne podliehať najmä jurisdikcii sídla prevádzkovateľa alebo jeho pobočky. Na jej postup sa bude ďalej vzťahovať národné, ale aj medzinárodné právo. Otázkou však ostáva, čo ak právo štátu žiadateľa je v rozpore s právom štátu prevádzkovateľa a zároveň neexistuje žiadna medzinárodná zmluva alebo medzinárodným právom uznaná zásada ako postupovať? Môže sa zdať, že národné alebo medzinárodné právo vystupuje ako záchytný bod alebo garancia tradičných hodnôt. Avšak nie je možné ich bez ďalšieho automaticky premietať do virtuálnej sféry. Treba si totiž uvedomiť, že v prípade vydávania dát požíva prevádzkovateľ pomerne vysokú mieru samostatnej rozhodovacej právomoci. Už výber technológie pre spracovanie a odovzdanie požadovaných dát reguluje to, aký rozsah bude mať zásah do práv dotknutého subjektu.

[415] HARAŠTA, Jakub, MÍŠEK, Jakub. IP adresy v kybernetické bezpečnosti*. Revue pro právo a technologie. 2015, č. 12, s. 21-42, Obdobne viď NONNEMANN, František. IP adresa jako osobní údaj. Právní rozhledy. 2017, č. 3, s. 88-93.

Navyše, zahraničný poskytovateľ určuje aj procedúru prijatia žiadosti, jej spracovania a príp. odovzdania zaistených dát. Týmto sa stáva definičnou autoritou v pravom zmysle slova. Ovplyvňuje nie len regulovaného užívateľa, ale aj prípadné výsledky trestného vyšetrovania v prípade dopytu o poskytnutie dát. V neposlednom rade je potrebné mať na pamäti špecifikum „výpovednej neschopnosť“ IP adresy o tom, kto vlastne kontroloval koncové zariadenie s predmetnou adresou.

6. Zaistenie elektronického dôkazného prostriedku v vo svetle trestného poriadku ČR a SR*

6.1. Úvodné poznámky

Elektronický, resp. digitálny dôkazný prostriedok v súčasnom trestnom konaní predstavuje jeden z kľúčových nástrojov získavania dôkazov. V dobe rozmachu kyberkriminality a sofistikovaného organizovaného zločinu sa vyťažovanie počítačových systémov pre účely ďalšieho forenzného skúmania stalo dennou rutinou OČTK. Tie sú konfrontované s neutíchajúcim technologickým pokrokom a zvyšujúcou sa rafinovanosťou páchateľov. Avšak na druhej strane tu stojí základné právo na spravodlivý súdny proces vyšetrovanej osoby, ktorá sa v postavení účastníka konania aktívne zaujíma o spôsob, formu a účel zaistenia elektronického dôkazného prostriedku.[416] Napätie medzi týmito dvoma záujmami je riešené predovšetkým procesnou kodifikáciou trestného práva. Tá by mala predstavovať základ pre správne zbieranie (zaisťovanie), vykonávanie a hodnotenie dôkazov. Zmyslom dokazovania je overenie si určitého tvrdenia, čo predstavuje myšlienkový proces zrekonštruovania minulých dejov. Nový fenomén elektronického dôkazného prostriedku posúva paradigma vnímania procesu dokazovania do úplne novej roviny. Pri každom dokazovaní po získaní požadovanej informácie, pristupuje logická operácia podradenia skutkovej (dejovej) podstaty pod zodpovedajúcu právnu normu. Ako sme uviedli vyššie, dokazovanie elektronickými dôkaznými prostriedkami bude priliehavosť voľby právnej normy súdom okrem iného závislá aj na tom, ako dobre bude zistená samotná skutková podstata prostredníctvom vykonávania takýchto dôkazov. Aj preto je dôležité sledovať, ako bude vyzerať úprava zaisťovania elektronických dôkazných prostriedkov v novom procesnom kódexe ČR.

Pripravovaná rekodifikácia trestného poriadku v ČR si kladie za cieľ zrýchliť trestné konanie, posilniť význam štádia konania pred súdom, zvýšiť aktivitu procesných strán a stanoviť procesnú zodpovednosť štátneho zástupcu za nevykonanie

* Táto podkapitola vychádza z publikovaného článku ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. Revue pro právo a technologie, Masarykova univerzita, 2015, roč. 6, č. 11, Str. 29-48. ISSN 1804-5383.

416 Viď napr. RAMPÁŠEK, M. Ústavnoprávne garancie pri uchovaní a vydaní počítačových údajov. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 6. 2013.

dôkazu v potrebnom rozsahu (formálne dôkazné bremeno).[417] Okrem toho, že pred súdom bude zvýraznený princíp kontradiktórnosti, rekodifikácia trestného procesného práva počíta so samostatnou úpravou absolútne neúčinných dôkazov. Ako je vidieť, nový kódex precizuje dokazovanie a stranou neostáva ani súčasný inštitút zaistenia veci. Východiská a princípy nového trestného poriadku počítajú v nadväznosti na rozvoj používania elektronických prostriedkov s novou úpravou zaisťovania dát z počítača a iných elektronických zariadení, a to aj spôsobom na diaľku.[418]

Rozhodovacia prax ukázala, že zaisťovanie dát dostáva nový rozmer a vymaňuje sa zo zaužívaného inštitútu zaisťovania veci (paragrafové znenie rekodifikácie trestného procesného práva používa terminológiu dokazovania vecami, dátami alebo listinami).[419] Pre potreby tejto práce je potrebné predstaviť možnosti komparatívneho pohľadu so slovenskou procesnou úpravou.

6.2. Zaistenie dátového nosiča alebo dát?

Súčasná česká právna úprava v prípade využitia zaisťovacieho prostriedku v prípravnom konaní alebo konaní pred súdom počíta so všeobecnou edičnou povinnosťou zakotvenou v § 78 TŘ, resp. povinnosťou súčinnosti podľa §7b TŘ (povinnosť uchovávať dáta). V praxi sa často tento inštitút využíva spolu s domovou prehliadkou podľa § 82 až § 85b TŘ. Navyše, podľa zjednocujúceho stanoviska NSZ, zaistenie aktuálneho stavu emailovej schránky (online služba umožňujúca uloženie dát prijatej, rozpísanej, odoslanej a zmazanej elektronickej komunikácie) je možné

[417] Ministerstvo spravedlnosti ČR: Komise pro nový trestní řád. Věcný záměr trestního řádu - hlavní principy navrhované rekodifikace trestního práva procesního [online]. [cit.1.9.2020]. Dostupné z: http://www.ceska-justice.cz/wp-content/uploads/2014/04/hlavn%C3%AD_principy_1.pdf alebo Rekodifikace trestního práva procesního. Pracovní verze paragrafového znění, které je aktuální ke dni 1. 1. 2020. [online]. [cit.1.9.2020]. Dostupné z: https://tpp.justice.cz

[418] Provedení dokazování věcí, daty nebo listinou. Viď § y38 ods.2 písm.: *„Považuje-li to předseda senátu za potřebné nebo požádá-li o to některá ze stran, a) umožní stranám, aby si věc podrobně prohlédly, b) data uchovávaná v elektronické podobě nebo jejich část týkající se dokazované skutečnosti se přehrají nebo se promítne jejich obsah anebo se stranám jinak zpřístupní ve srozumitelné podobě, a to i formou písemného přepisu, prostřednictvím znaleckého posudku nebo výslechem znalce, c) listina nebo její část týkající se dokazované skutečnosti se přečte nebo se promítne anebo se jinak zobrazí její obsah.“* Pracovní verze paragrafového znění Rekodifikace trestního práva procesního.

[419] Príkladom môže byť rozhodnutie Ústavného súdu ČR, kde sa okrem povahy sociálnej siete riešil aj spôsob nešťastne predloženého elektronického dôkazu – printscreenu počítačovej obrazovky (sociálnej siete Facebook) policajným vyšetrovateľom. Rozhodnutí Ústavního soudu ČR ze dne 30.10.2014 sp. zn. III.ÚS 3844/13.

vykonávať aj v súlade s inštitútom sledovania osôb a vecí podľa § 158d ods. 1, 3 TŘ.[420] Domnievame sa, že vyšetrovacia prax stále nerobí rozdiel v otázkach zaistenia dôkazných prostriedkov medzi vecou a elektronicky uloženou informáciou, resp. dátami. OČTK sa k dôkazom dostávajú prostredníctvom vyťažovania zaistených elektronických nosičov (vecí) za využitia odbornej znaleckej expertízy. Táto koncepcia je však prekonaná, nakoľko už dávno nie sme svedkami toho, že by páchatelia nechávali svoje elektronické stopy len na USB kľúčoch, pevných diskoch, cédečkách alebo na už historicky znejúcich disketách (hmotných predmetoch). Kyberpriestor v súčasnosti predstavuje nový fenomén, ktorý umožňuje virtualizovanie dát do takej podoby, že tie sú fyzicky nelokalizovateľné.[421]

Budapeštiansky dohovor o počítačovej kriminalite (ďalej len ako „BD“)[422] definuje počítačové údaje ako akékoľvek znázornenie faktov, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu umožňujúcemu nariadiť výkon akejkoľvek funkcie počítačom. Ďalej o prevádzkových údajoch hovorí, že ide o akékoľvek počítačové dáta, ktoré súvisia s komunikáciou prostredníctvom počítačového systému, sú generované počítačovým systémom, ktorý tvoril súčasť reťazca komunikácie, s uvedením pôvodu, cieľa, trasy, času, dátumu, objemu, trvania komunikácie alebo typu základnej služby. Počítačové údaje môžu byť súčasťou jedného alebo viacerých dátových nosičov. Môžu byť zašifrované a navonok vystupovať ako prázdne nezapísané miesto dátového nosiča. Môžu byť rovnako schované v inom dátovom formáte (napr. steganografia). Navyše nemusia byť uložené v celku a na jednom fyzickom mieste (napr. packaging). Ich vlastnosťou je potencionálna *ubiquita* a *volatilita* (viď podkapitolu: 2.5 Kategória kvality elektronického dôkazného prostriedku).

---

[420] *„Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.“* Viď Stanovisko NSZ č.1/2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf

[421] Napr. cloud systém, ktorý využíva serverové farmy po celom svete a ani sám správca tohto systému nevie, kde sa nachádza ten ktorý sektor disku s požadovanou informáciou, nakoľko tieto môžu byť v neustálom pohybe.

[422] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č.104/2013 Sb. medzinárodných smluv ČR. [online]. [cit.1.9.2020]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=26438

Čo je však dôležitejšie, zaistenie dát na rozdiel od zaistenia veci (napr. celého hard disku počítača) môže priniesť omnoho šetrnejší a precíznejší zásah do práv vyšetrovaného. Ide o vyjadrenie zásady zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktoré sú vlastné trestnému právu.[423] Zákonom č. 287/2018 Zb. s účinnou od 1. 2. 2019, bol novelizovaný o § 7b TŘ, podľa ktorého OČTK má možnosť požadovať od osoby, ktorá drží alebo má pod svojou kontrolou dáta uložené v počítačovom systéme alebo na nosiči informácií, uchovávať takáto dáta v nezmenenej podobe po dobu stanovenú v príkaze a urobiť potrebné opatrenia, aby nedošlo k sprístupneniu informácie o tom, že bolo nariadené uchovanie dát, a tiež nariadiť, aby táto osoba znemožnila prístup iných osôb k takýmto dátam.[424] Podľa Sokola *„je zjevné, že v praxi budou či mohou vznikat spory, jaká data vydavatel příkazu mínil a případně co mínil nosičem informací nebo počítačovým systémem.*"[425] Ten uvádza, že aj keď TZ už pracuje s podobnými pojmami, ktoré sú riešené výkladom alebo súdnou praxou, je možne sa obávať, že zo strany OČTK a súdu bude tendencia k čo najširšiemu výkladu týchto pojmov. Ako niektorí autori poukazujú, stojí však za zamyslenie, či OČTK pri vydaní príkazu podľa § 7b TŘ a následnou žiadosťou o vydanie dát (akejkoľvek osobe) podľa § 158d ods. 1, 3 TŘ neobchádzajú zákonnú úpravu získania dát telekomunikačnej prevádzky a zneužívajú inštitút súčinnosti. Sledovanie osôb a vecí je úkonom trestného konania, ku ktorého realizácii sú povolané výlučne OČTK.[426] V tejto otázke sa je sa možné pozrieť na medzinárodnú úpravu.

[423] KOLOUCH, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. [online]. [cit.1.9.2020]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/zajistovaci_ukony-rtf.pdf

[424] Podľa §tb ods.1 TŘ: *„Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat."*

[425] Na jednoduchu otázku v prípade advokátaodpovedá: *„Daty tedy bude vše, co advokát drží v počítači, notebooku, mobilním telefonu či nosiči informací, jako je flash disk, DVD apod.*" Viď SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. Bulletin advokacie. 2019, č. 9, s. 15-19

[426] TLAPÁK NAVRÁTILOVÁ, Jana, GALOVCOVÁ, Ingrid. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?. Bulletin advokacie. 2019, č. 11, s. 36-39

V októbri 2018 Európska komisia zahájila legislatívne práce na návrhu smernice[427] a nariadenia [428] o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. Účelom je priamy a zjednodušený prístup k cezhraničným dôkazom. Tento navrhovaný právny rámec umožňuje, aby justičné orgány, resp. iné orgány so súhlasom justičných orgánov členského štátu EÚ mali právomoc dopytovať predloženie elektronických dôkazov, a to aj priamo od poskytovateľa služieb, resp. ním zvoleného zástupcu v inom štáte EÚ. Právny rámec sa snaží zjednodušiť systém spolupráce a odbúrava potrebu medzinárodnej justičnej spolupráce. Pôsobnosť je extra-teritoriálna (podobne ako americký *CLOUD Act*), uplatňuje sa na poskytovateľov služieb, ktorí ponúkajú služby v rámci EÚ bez ohľadu na ich sídlo. [429] Návrhy v zásade mieria na skupinu amerických podnikateľských subjektov, ktorá disponuje najväčšími svetovými cloudovými riešeniami, prezývanú *Big Tech (Amazon, Apple, Alphabet, Facebook a Microsoft).* V zmysle navrhovanej smernice členské štáty, v ktorých pôsobí poskytovateľ služieb (napr. poskytovateľ cloudu), zabezpečia, aby takýto poskytovateľ služieb určil aspoň jedného právneho zástupcu v EÚ, ktorý bude prijímať, dodržiavať a presadzovať rozhodnutia a príkazov vydaných príslušnými orgánmi v členských štátoch na účely zhromažďovania dôkazov v trestnom konaní.[430] Nariadenie priamo ukladá povinnosti a stanovuje pravidlá, na základe ktorých orgán členského štátu môže nariadiť poskytovateľovi služieb, aby predložil alebo uchoval elektronické dôkazy bez ohľadu na umiestnenie údajov.[431] Na rozdiel od BD, nie je rozhodné kde sa elektronické dôkazy nachádzajú, ale kto má nad

[427] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM/2018/226 final - 2018/0107 (COD). [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN

[428] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM/2018/225 final - 2018/0108 (COD). [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

[429] Čl.3 ods.1 návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[430] Viď čl. 3 návrhu smernice, ktorou sa stanovujú harmonizované pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

[431] Nariadením nie sú dotknuté právomoci vnútroštátnych orgánov nariadiť poskytovateľom služieb usadeným alebo zastúpeným na ich území dodržať súlad s podobnými vnútroštátnymi opatreniami. Viď čl. 1 ods. 1 návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

nimi kontrolu. Návrh nariadenia pracuje s dvoma záväznými príkazmi, ktoré musia byť vydané alebo overené súdnym orgánom členského štátu:

- *Európsky príkaz na predloženie dôkazov*
- *Európsky príkaz na uchovanie dôkazov.*

Návrh nariadenia definuje elektronické dôkazy ako dôkazy existujúce a uložené v elektronickej podobe poskytovateľom služieb alebo v jeho mene v čase prijatia osvedčenia[432] o príkaze na predloženie alebo uchovanie dôkazov. Ide o:[433]

- *uložené údaje o predplatiteľoch*
- *údaje o prístupe*
- *údaje o transakciách*
- *obsahové údaje*

Navrhované nariadenie reguluje iba uložené, resp. zapísané elektronické dôkazy (*at rest*) a nepokrýva elektronické dôkazy vysielané alebo komunikované v reálnom čase (*in transit*).[434] Návrh nariadenia ukladá poskytovateľom služieb pomerne prísne lehoty na odpoveď. [435] Ak požiadaný poskytovateľ služieb odmietne spolupracovať s justičným orgánom, ten ma možnosť požiadať o pomoc justičný orgán v mieste

[432] Osvedčenia o európskom príkaze na predloženie dôkazov a osvedčenia o európskom príkaze na uchovanie dôkazov slúžia na zaslanie príkazov adresátom vymedzeným v článku 7 návrhu nariadenia. Vzory oboch osvedčení sú stanovené v prílohách I a II k nariadeniu a musia byť preložené do jedného z úradných jazykov členského štátu, v ktorom sa nachádza adresát. Poskytovatelia služieb môžu vyhlásiť, že príkazy sa budú akceptovať aj v iných úradných jazykoch Únie. Cieľom týchto osvedčení je poskytnúť všetky potrebné informácie, ktoré sa majú zaslať adresátovi v štandardizovanej podobe, pričom sa minimalizuje možnosť pochybenia, umožní sa ľahká identifikácia príslušných údajov a v čo najväčšej možnej miere sa predíde uvádzaniu voľného textu, čím sa znížia náklady na preklad. Osvedčenie nebude obsahovať úplné zdôvodnenie nevyhnutnosti a primeranosti alebo ďalšie podrobné informácie o prípade, aby sa predišlo ohrozeniu vyšetrovania. Z tohto dôvodu je potrebný iba ako súčasť samotného príkazu, aby sa neskôr podozrivému umožnilo napadnúť príkaz počas trestného konania. Viď Návrh nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[433] Viď čl. 2 ods. 6 návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[434] Viď dôvodovú správu návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

[435] V štandardných prípadoch 10 dní, v v núdzových prípadoch adresát zašle požadované údaje bezodkladne, najneskôr do 6 hodín od prijatia osvedčenia o európskom príkaze na predloženie dôkazov. Viď čl.9 ods.2 návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach.

poskytovateľa. Rovnako neponúka možnosť priameho prístupu k elektronickým dôkazom bez spolupráce poskytovateľa služieb. Domnievame, že tento postup je správny, inak by nariadenie predstavovalo potenciálne riziko straty procesnej kontroly, ktorá je inak používaná v prípadoch odpočúvania a zázname telekomunikačnej prevádzky.[436] Návrh smernice a nariadenia nebránia použitiu doterajších postupov medzinárodnej spolupráce alebo dobrovoľnej spolupráce poskytovateľa s justičným orgánom (viď 3. kapitolu o informačnej suverenite štátu a cezhraničné dokazovanie). Vzhľadom na komplexnosť predloženej legislatívy, jednotlivé členské štáty najpravdepodobnejšie pristúpia k novelizácii svojich trestných poriadkov pri transponovaní dotknutej navrhovanej smernice.[437]

6.3. Zaisťovanie počítačových údajov podľa slovenského trestného práva

6.3.1. Zákonné ustanovenie

Slovenská právna úprava priniesla vo svojej rekodifikácii TP z roku 2005 v štvrtej hlave o zaistení osôb a vecí v § 90 špeciálnu úpravu uchovania a vydania počítačových údajov:

(1) Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby

a) také údaje uchovali a udržiavali v celistvosti,

[436] Debaty v rámci legislatívneho procesu potvrdili, že téma elektronických dôkazov *in transit* predstavuje senzitívnu a kontroverznú tému, ktorá vyvoláva neochotu zúčastnených a predstavuje riziko predĺženia rokovaní. Viď European Comission. Public consultation on improving cross-border access to electronic evidence in criminal matters. [online]. [cit.1.9.2020]. Dostupné z: https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en alebo Ministerstvo spravodlivosti SR. Riadne predbežné stanovisko k návrhu nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. LP/2018/566. [online]. [cit.1.9.2020]. Dostupné z: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2018/566/

[437] Ibid. Ministerstvo spravodlivosti SR. Riadne predbežné stanovisko k návrhu nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. LP/2018/566.

b) umožnili vyhotovenie a ponechanie si kópie takých údajov,

c) znemožnili prístup k takým údajom,

d) také údaje odstránili z počítačového systému,

e) také údaje vydali na účely trestného konania.

(2) V príkaze podľa odseku 1 písm. a) alebo písm. c) musí byť ustanovený čas, po ktorý bude uchovávanie údajov vykonávané, tento čas môže byť až na 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz.

(3) Ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné, vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovávania týchto údajov.

(4) Príkaz podľa odsekov 1 až 3 sa doručí osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, ktorým sa môže uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze.

(5) Osoba, v ktorej držbe alebo pod jej kontrolou sa nachádzajú počítačové údaje, vydá tieto údaje, alebo poskytovateľ služieb vydá informácie týkajúce sa týchto služieb, ktoré sú v jeho držbe alebo pod jeho kontrolou, tomu, kto vydal príkaz podľa odseku 1 alebo osobe uvedenej v príkaze podľa odseku 1.

Podľa tohto ustanovenia ide o situáciu, kedy na objasnenie skutočností závažných pre trestné konanie je nevyhnutné uchovanie, resp. vydanie uložených počítačových údajov vrátane prevádzkových údajov. Tento zaisťovací úkon nie je podmienený výpočtom špecifických trestných činov. Navyše, použitie § 90 TP nie je v aplikačnej praxi jednoznačné a prináša nedorozumenia, kedy sa toto ustanovenie má využiť.[438]

V nasledujúcej časti budú rozobraté jednotlivé podmienky použitia tohto ustanovenia.

[438] RAMPÁŠEK, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5. 2013. Str. 21-26.

6.3.2. Počítačové a prevádzkové údaje, otázka ich vzniku

Tak ako BD, aj TP rozlišuje dve samostatné kategórie údajov. TP priamo neuvádza, či v čase vydania príkazu už musia údaje existovať a musia byť uložené prostredníctvom počítačového systému. Dôvodová správa k TP sa obmedzuje na konštatovanie že, *„úprava reaguje na dohovor Rady Európy o počítačovej kriminalite, ktorý bol prijatý členskými štátmi Rady Európy dňa 23.11.2001 v Budapešti. Toto ustanovenie umožňuje vydať príkaz na uchovanie a vydanie počítačových dát pre účely trestného konania, najviac na 90 dní. Príkaz na uchovanie a vydanie počítačových dát, ak sú potrebné na účely trestného konania je možné vydať opätovne.“*[439] Súčasná odborná literatúra konštatuje, že *„účelom tohto inštitútu je najmä odhaľovanie a vyšetrovanie trestnej činnosti páchanej prostredníctvom internetu.“*[440] V praxi sa objavuje aj názor, že by mohlo ísť aj o údaje prenášané v reálnom čase (najmä z dôvodu možného zaistenia reálne prenášaných prevádzkových údajov). S týmto názorom sa však nie je možné stotožniť. Účel tohto ustanovenia smeruje iba k uchovaniu už prenesených (uložených) údajov (a to vrátane uložených prevádzkových údajov).[441] Teda ide o zaistenie počítačových údajov už zapísaných na pevnom nosiči. Taktiež, gramatickým výkladom je možné dospieť k tomu, že ide o minulé údaje (t.j. tie, ktoré boli uložené prostredníctvom počítačového systému). Navyše, BD rozlišuje medzi urýchleným uchovaním uloženým počítačových údajov (článok 16), urýchleným uchovaním a čiastočným sprístupnením prevádzkových údajov (článok 17), zhromažďovaním údajov v reálnom čase (článok 20) a zachytením obsahových údajov (článok 21). Predmetné zákonné ustanovenie však kopíruje povinnosti uvedené v ustanoveniach o

[439] Ministerstvo spravodlivosti SR. Dôvodová správa, Všeobecná časť, Podľa Plánu legislatívnych úloh vlády SR na rok 2003 sa predkladá do legislatívneho procesu návrh nového Trestného poriadku. Epi.sk. Elektronické právne informácie. [online]. [cit.1.9.2020]. Dostupné z: http://www.epi.sk/dovodova-sprava/Dovodova-sprava-k-zakonu-c-301-2005-Z-z.aspx

[440] MINÁRIK, Š. Trestný poriadok. Stručný komentár. 2010. Iura edtion s.r.o. Str. 315.

[441] Napriek existujúcim definíciám “počítačové údaje” a “počítačový systém”, prax k nim pristupuje odlišne. Viď. HALAS, Norbert, K uchovaniu a vydaniu počítačových údajov z obsahu mobilných telefónov v trestnom konaní. Justičná revue. 72. 2020. č.6-7. Str. 803-811.

urýchlenom uchovaní uložených počítačových údajov (článok 16)[442] a prehliadke o zaistení uložených počítačových údajov (článok 19).[443]

Otázka, čí mobilný telefón predstavuje počítač, bola riešená NS SR.[444] Ten rozhodol, že *„námietka, že na znalecké preskúmanie mobilných telefónov bol vzhľadom ku ich operačnému systému potrebný príkaz na uchovanie a vydanie počítačových údajov podľa § 90 Tr. por., a teda nepostačovalo vydanie, resp. odňatie veci podľa § 89, § 91 Tr. por., rovnako nie je dôvodná. Možno dodať, že napriek niektorým podobným alebo zhodným technickým komponentom a spôsobu prevádzky, mobilný telefón nemožno stotožniť s počítačom a tento rozdiel sa prejavuje i pri ponuke a predaji príslušných zariadení ako rozdielnych druhov tovaru.“* Táto úvaha je v rozpore s technickým stavom poznania a rovnako čl. 1 ods. 1 písm. b) BD, ktorý definuje, čo je to počítačový systém. K tejto otázke zaujal stanovisko NS SR, keď vyslovil, že *„na zabezpečenie informácií z mobilného telefónu, ktorý bol vydaný alebo odňatý ako vec dôležitá pre trestné konanie podľa § 89 a § 91 TP, a to aj pri domovej prehliadke alebo prehliadke iných priestorov alebo pozemku v zmysle § 105 ods. 4 TP, alebo ak je mobilný telefón zaistený ako vecná stopa pri obhliadke podľa § 154 TP, nie je potrebné (duplicitné) vydanie príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke podľa § 116 (ods. 2) TP.“* Súd argumentoval tak, že ak ide o páchateľa, resp. obvineného, príkazom podľa § 90 TP by nebolo možné údaje spoľahlivo zabezpečiť. Ten by mohol pri prevzatí príkazu (bez súčasného odňatia veci) počítačové údaje

[442] Čl. 16 ods. 1 BD: *„Každá strana prijme potrebné legislatívne a iné opatrenia, aby umožnila jej príslušným orgánom nariadiť alebo podobným spôsobom zabezpečiť urýchlené uchovanie určených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, najmä ak existujú dôvody domnievať sa, že hrozí osobitné riziko straty alebo pozmenenia týchto počítačových údajov.“*

[443] Čl. 19. ods. 3 BD: *„Každá strana prijme potrebné legislatívne alebo iné opatrenia na udelenie oprávnenia jej príslušným orgánom zaistiť alebo podobne zabezpečiť počítačové údaje, ku ktorým získali prístup podľa odseku 1 alebo 2. Tieto opatrenia zahŕňajú oprávnenie zaistiť alebo podobne zabezpečiť počítačový systém alebo jeho časť, alebo pamäťový nosič počítačových údajov, vyhotoviť a ponechať si kópiu týchto počítačových údajov, zachovať celistvosť relevantných uložených počítačových údajov, znemožniť prístup k takým počítačovým údajom alebo ich odstrániť z počítačového systému, do ktorého sa vstúpilo.“*

[444] Rozsudok NS SR zo dňa 26.11.2014, sp. zn. 2To/9/2014.

odstrániť, resp. ich zničiť.[445] Napriek tomuto rozhodnutiu sa domnievame, že ak ide o zabezpečenie počítačových údajov a sledovaný cieľ trestného konania tým bude naplnený, je potrebné vždy dať prednosť použitiu príkazu v zmysle § 90 TP pred zaistením celej veci (napr. počítača, mobilu).[446] Podobne tomu je aj pri zaistení kryptomien, resp. rôznych foriem elektronických platobných prostriedkov, ktoré majú byť zaistené na výkon trestu prepadnutia majetku podľa TP, kde je potrebné postupovať podľa ustanovenia o uchovávaní a vydaní počítačových údajov v zmysle § 90 TP.[447] Avšak ako Šamko uvádza „*ak je domová prehliadka vykonávaná s cieľom nájsť a zaistiť predmety, ktoré môžu byť dôkazmi (a to napr. aj konkrétne počítačové údaje, pri ktorých je odôvodnený predpoklad, že sa nachádzajú v priestore, ktorý sa má prehľadať) a pokiaľ je tento cieľ dosahovaný postupom podľa príslušných ustanovení, nemožno považovať za porušenie zákona skutočnosť, že okrem príkazu na vykonanie domovej prehliadky nebol vydaný ešte aj príkaz podľa §90.*“[448] Podľa Šamka, takýto procesný postup by znamenal, že na základe príkazu na domovú prehliadku by bolo možné len prehľadať byt alebo dom v ňom vymedzený, avšak na akékoľvek zaistenie hľadaných vecí by boli nutné osobitné príkazy. Je potrebné sledovať účel domovej prehliadky, nájdenie veci (napr. mobilného zariadenia) a nie sa formálne zamerať len na výkon samotného prehľadávania (činnosť OČTK).

[445] V ČR existuje podobná prax, nakoľko podľa stanoviska NSZ: *„v případě zákonným způsobem zajištěných mobilních telefonů a jejich součástí (což mohou být nejen SIM karty, ale i v mobilních telefonech vložené paměťové karty) se státní zástupci nadále i s ohledem na čl. 46 odst. 2 pokynu obecné povahy nejvyššího státního zástupce č. 8/2009 Sb., o trestním řízení, ve znění pozdějších pokynů,3) ve většině případů při zjišťování jejich obsahu řídí výkladovým stanoviskem poř. č. 4/2005 Sb. v. s. NSZ. Jeho obecná použitelnost je přitom akceptována i ohledně obsahu paměti výpočetní techniky (částí počítačového systému jako tzv. harddisky) a jiných nosičů informací (např. USB disky), které mohou obsahovat různé formy elektronické komunikace.4) Pouze ojediněle, sohledem na rozhodnutí Vrchního soudu v Olomouci ze dne 15. 6. 2010 sp. zn. 5 Tdo 42/2010,5) zejména pokud jde o státní zástupce činné v obvodu jeho působnosti, státní zástupci před zjišťováním obsahu mobilních telefonů a jejich součástí (SIM karty či paměťové karty) s pozitivním výsledkem navrhují vydání příkazů podle § 88 či § 88a trestního řádu.”* Viď Stanovisko NSZ č. 1/2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf

[446] KUBIČKA, Remig, KUBIČKA, Oliver. Počítačové údaje v trestnom konaní. In: Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov. Bratislava. 2018. Akadémia PZ v Bratislave. ISBN 978-80-8054-774-5. Str. 86. [online]. [cit.1.9.2020]. Dostupné z: https://www.akademiapz.sk/sites/default/files/KIM/ZBORNÍK%2021.3.2018%20WEB_0.PDF

[447] KURILOVSKÁ, L., KORDÍK, M. Zaistenie vecí a majetku. Právny obzor, 103, 2020, č. 1, Str. 29 - 41.

[448] ŠAMKO, P. Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestom konaní. Zo súdnej praxe. 2017, č. 6, Str. 248.

6.3.3. Oprávnený orgán a povinná osoba

Právomoc na vydanie tohto príkazu má pred začatím trestného stíhania alebo v prípravnom konaní prokurátor, v ostatných prípadoch predseda senátu. Príkaz môže smerovať voči osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú počítačové údaje alebo voči poskytovateľovi služieb.[449] Procesná legitimácia povinnej osoby je definovaná buď fyzickou držbou údajov alebo štatútom poskytovateľa služieb. Teda príkaz sa bude doručovať osobe, v ktorej držbe alebo pod ktorej kontrolou sa nachádzajú také údaje alebo poskytovateľovi takých služieb (napr. prevádzkovateľovi webhostingu, cloudovej služby, účtovných služieb atď.).

Je potrebné zdôrazniť, že príkaz nemusí smerovať len priamo voči osobe, ktorá je pôvodcom počítačových údajov. Z praktického hľadiska je možné rozlíšiť medzi:

- tretími osobami, t.j. operátorom (poskytovateľom telekomunikačnej služby podľa ZEK), inou osobou poskytujúcou online služby (napr. služby informačnej spoločnosti podľa zákona č. 22/2004 Zb. o elektronickom obchode) alebo vôbec neregulovanou osobou a

- podozrivým, resp. obvineným alebo obžalovaným v zmysle TP.

Nakoľko procesné podmienky v prípravnom konaní sú nenáročné (stačí príkaz prokurátora), prax ukázala, že využitím tohto inštitútu môže dôjsť k obchádzaniu iných informačnotechnických prostriedkov (napr. odpočúvanie a záznam telekomunikačnej prevádzky, sledovanie osôb a vecí), pre ktoré sú definované vyššie kontrolné mechanizmy na ich vykonanie.[450] V súčasnosti OČTK nemôžu bez súhlasu súdu žiadať od poskytovateľa telekomunikačnej služby (operátora) obsahové údaje. Podľa zrušeného § 116 ods. 4 TP, ustanovenia o zaistení prevádzkových údajov o uskutočnenej telekomunikačnej prevádzke sa primerane vzťahovali aj na obsahové

[449] Platná slovenská právna úprava pozná dva základné subjekty v oblasti telekomunikačnej (internetovej) prevádzky. Ide o telekomunikačného operátora, ktorý poskytuje elektronickú komunikačnú sieť alebo službu v zmysle § 5 ods. 1 ZEK. Ďalším je poskytovateľ služieb informačnej spoločnosti podľa zákona č. 22/2004 Z.z. o elektronickom obchode. Z dostupnej odbornej literatúry (Rampášek) vyplýva, že sa poskytovateľom služby na účely príkazu podľa § 90 TP rozumie podnik podľa zákona o elektronických komunikáciách. Rozdiel medzi uvedenými subjektmi je potrebný pre rozlíšenie medzi dvoma druhmi počítačových údajov, a to medzi obsahovými údajmi a prevádzkovými údajmi.

[450] Príkaz na odpočúvanie a záznam telekomunikačnej prevádzky vydáva predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora. Viď § 115 TP.

údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému. Táto skutočnosť bola zmenená rozhodnutím ÚS SR, v ktorom plénum vyhlásilo ustanovenia § 58 ods. 5 až ods. 7 a § 63 ods. 6 ZEK, ktoré doteraz prikazovali operátorom sledovať komunikáciu svojich užívateľov, ako aj § 116 TP a § 76a ods. 3 zákona č. 171/1993 Z.z. o policajnom zbore, ktoré umožňovali ich sprístupňovanie, za nesúladné s ústavne garantovaným právom obyvateľov na súkromie a ochranu osobných údajov.[451]

Je možné ešte dodať, že existujú rôzne odborné názory v interpretácií ustanovení inštitútu príkazu podľa § 90 TP. Rampášek uvádza, že *„napriek tomu, že Slovenská republika implementovala BD, implementácia predovšetkým oprávnení orgánov činných v trestnom konaní pri uchovávaní a vydaní počítačových údajov bola vykonaná nesprávne, miestami až v rozpore s účelom jednotlivých ustanovení BD, pretože pripúšťa širšie, a teda neprimerané použitie implementovaných oprávnení na uchovávanie a predovšetkým vydanie počítačových údajov.“*[452] Je naozaj potrebné prisvedčiť tomu, že povinnosť vydať prevádzkové údaje v zmysle § 90 TP nedosahuje legálny rámec nárokov ustanovenia § 116 TP.[453] Tu príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami. Navyše, tieto ustanovenia sa primerane vzťahuje aj na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému v zmysle §116 ods. 6.[454]

[451] Rozhodnutie ÚS SR sp. zn. PL. ÚS 10/2014 zo dňa 29.4.2015.

[452] Ibid. RAMPÁŠEK, M. Uchovanie a vydanie počítačových údajov v trestnom konaní.

[453] Ustanovenie §116 ods.1 TP bolo novelizované, a to tak, že: *„V trestnom konaní pre úmyselný trestný čin, za ktorý zákon ustanovuje trest odňatia slobody, ktorého horná hranica je najmenej tri roky, pre trestný čin ochrany súkromia v obydlí podľa § 194a, podvodu -po-dľa § 221, nebezpečného vyhrážania podľa § 360, nebezpečného prenasledovania podľa § 360a, šírenia poplašnej správy podľa § 361, podnecovania podľa § 337, schvaľovania trestného činu podľa § 338, pre trestný čin, ktorým bola spôsobená ťažká ujma na zdraví alebo smrť alebo pre iný úmyselný trestný čin, pri ktorom na konanie zaväzuje medzinárodná zmluva, možno vydať príkaz na zistenie a oznámenie údajov o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú nevyhnutné na objasnenie skutočností dôležitých pre trestné konanie. Príkaz možno vydať, ak nemožno sledovaný účel dosiahnuť inak alebo ak by bolo jeho dosiahnutie iným spôsobom podstatne sťažené.“* Paradoxne, v zmysle § 90 TP môže v súčasnosti prokurátor vydať príkaz na vydanie prevádzkových údajov osobe, ktorá poskytuje telekomunikačné služby, ale už nemá povinnosť tieto údaje uchovávať v zmysle zákona o elektronických komunikáciách.

[454] Porovnaj MIHÓK, Alexander. Príkaz na zaistenie a oznámenie údajov o uskutočnenej prevádzke a vybrané problémy aplikačnej praxe. Justičná Revue. 71. 2019. č.12. Str. 1241-1253.

6.3.4. Povinnosti uvedené v príkaze

Príkaz musí byť v prvom rade odôvodnený skutkovými okolnosťami. Rozsah skutkových okolností síce nie je presne definovaný, avšak príkaz musí rešpektovať základné zásady trestného procesu, najmä zásadu stíhania len zo zákonných dôvodov, kedy OČTK môžu stíhať páchateľov len spôsobom, ktorý stanoví trestný poriadok a vykonávať na to nadväzujúce úkony. Príkaz smeruje k uloženiu taxatívne určených povinností, a to aby:[455]

a) také údaje uchovali a udržiavali v celistvosti
b) umožnili vyhotovenie a ponechanie si kópie takých údajov
c) znemožnili prístup k takým údajom
d) také údaje odstránili z počítačového systému
e) také údaje vydali na účely trestného konania

Za najzásadnejší prienik do základných práv dotknutého subjektu sa považuje posledná povinnosť pod písm. e), t.j. vydania počítačových údajov. Pôvodným účelom príkazu bolo v zmysle článkov 16 až 18 BD urýchlené uchovanie uložených počítačových údajov, teda zabezpečenie elektronického dôkazného prostriedku pre budúce dokazovanie. V odbornej literatúre sa objavuje názor, že toto ustanovenie slúži aj na predĺženie plynutia šesť mesačnej lehoty podľa zákona o elektronických komunikáciách, počas ktorej podnik uchováva uvedené údaje s tým, že prokurátor môže týmto príkazom zabezpečiť, aby sa tieto legálne uchovávali aj dlhšie (jedným príkazom môže prokurátor prikázať uchovanie údajov až na 90 dní).[456] Avšak táto skutočnosť bola zmenená spomenutím rozhodnutím ÚS SR.

Čo sa týka časového aspektu, v príkaze podľa § 90 odseku 1 písm. a) alebo písm. c) TP musí byť ustanovený čas, po ktorý bude uchovanie údajov povinnou osobou vykonávané. Avšak ide už o uchovanie uložených údajov. Tento čas môže byť až 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz. Táto špecifikácia bola doplnená až novelou č. 262/2011 Z.z. účinnou od 1. 9. 2011. Dovtedy platilo, že v akomkoľvek príkaze musí byť ustanovený presný čas, po ktorý bude uchovanie údajov vykonávané, čo vyvolávalo mnohé interpretačné pochybnosti.[457]

[455] Podobné povinnosti sú stanovené v článku 16 a 21 BD.

[456] Ibid. RAMPÁŠEK, M. Uchovanie a vydanie počítačových údajov v trestnom konaní.

[457] Nález ÚS SR zo dňa 25. augusta 2010, sp. zn. III. ÚS 68/2010.

Avšak v súčasnosti je zrejmé, že pre potreby trestného konania, predstavuje edičná povinnosť uvedená pod písm. b) a e) najpoužívanejší spôsob zadováženia elektronického dôkazného prostriedku v trestnom konaní bez ohľadu na povinný subjekt (ktorý má počítačové údaje v držbe, resp. pod kontrolou).[458]

6.3.5. Procesné podmienky vydania príkazu

Príkaz predstavuje rozhodnutie *sui generis*, voči ktorému nie je prípustný riadny opravný prostriedok. Avšak ústavná sťažnosť za predpokladu splnenia určitých podmienok nie je vylúčená.[459] Príkaz musí byť písomný. Na rozdiel od veci, ktorú dotknutá osoba vydáva policajtovi, prokurátorovi alebo súdu, počítačové údaje je osoba, v ktorej držbe alebo pod ktorej kontrolou sa tieto nachádzajú, povinná vydať tomu, kto vydal príkaz (predseda senátu alebo prokurátor) alebo osobe uvedenej v príkaze.[460]

Ďalej je potrebné uviesť, že použitie tohto príkazu nie je obmedzené špecifickým výpočtom trestných činov, pri ktorých je tento príkaz možné použiť (napr. ako to je pri odposluchu alebo pri inom informačno–technickom prostriedku). Ako už bolo uvedené, príkaz v prípravnom konaní nevyžaduje súhlas sudcu alebo senátu. Táto skutočnosť sa môže negatívne odraziť aj v tom, že súčasťou zaistených počítačových údajov môže byť napr. neotvorená alebo rozpísaná pošta v cloude (resp. uložená na diskovom poli servera), uložený textový rozhovor (*messenger* alebo *chat*), uložená streamovaná telefonická videokonferencia viacerých účastníkov atď. Je nutné poukázať na znenie BD v čl. 14. Rozsah procesných ustanovení, ktoré sa snaží definovať hranice signatárov v prijímaní potrebných legislatívnych a iných opatrení. BD nepriamo identifikuje trestné činy, voči ktorým sa rozsah procesných ustanovení uplatňuje. Totiž každá strana uplatní právomoci a postupy uvedené len na tieto trestné činy, iné trestné činy spáchané prostredníctvom počítačového systému alebo zhromažďovanie dôkazov o trestnom čine v elektronickej forme. V tomto prípade je nutné apelovať na to, aby slovenský zákonodarca v budúcnosti revidoval pôsobnosť tohto ustanovenia v zmysle BD a

[458] NOVOCKÝ, J. Zaistenie majetku a vecí v trestnom konaní – aplikačné problémy, Justičná akadémia 2013. [online]. [cit.1.9.2020]. Dostupné z: https://www.ja-sr.sk/files/Zaistenie_majetku_a_veci_v_trestnom_konani_aplikacne_problemy.pdf

[459] Nález ÚS SR zo dňa 25. augusta 2010, sp. zn. III. ÚS 68/2010.

[460] HASÍKOVÁ, J. Počítačový údaj - zdroj dokazovania. Bulletin slovenskej advokácie. 1-2/2013. Bratislava. Str. 29. Obdobne Minárik, Š. Trestný poriadok, stručný komentár. Druhé, prepracované a doplnené vydanie. Iura Edition, Bratislava. 2010. Str. 315.

taktiež rozhodnutia ÚS SR ohľadom vydávania prevádzkových údajov od osôb podnikajúcich podľa ZEK.

6.3.6. Ukončenie príkazu

Zákon ďalej pozná ukončenie tohto príkazu, a to pre prípad ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné. V tomto prípade vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovania týchto údajov. Je potrebné dodať, že ide o vágnu formuláciu, ktorá navyše bude ťažko podliehať procesnej kontrole zo strany účastníkov alebo povinných. Tu je potrebné pripomenúť zásadu oficiality, kedy OČTK vykonávajú úkony zo svojej úradnej povinnosti. Čiže tie sú povinné sústavne skúmať dôvodnosť vydaného príkazu a v prípade potreby ho revidovať.

6.3.7. Povinnosť mlčanlivosti

Špeciálne je upravená povinnosť mlčanlivosti. Ako už bolo spomenuté, príkaz môže smerovať voči prevádzkovateľovi počítačového systému a nie voči pôvodcovi počítačových údajov. Preto popri tomto príkaze sa mu môže uložiť aj povinnosť zachovať v tajnosti opatrenia uvedené v príkaze. Tajnosť opatrenia smeruje k snahe zabrániť zmareniu zaistenia dôkazného prostriedku. Neuposlúchnutie príkazu je sankcionované poriadkovou pokutou v zmysle § 70 ods.1 TP.[461]

Pre doplnenie je možné uviesť, že povinnosť mlčanlivosti smeruje vždy do budúcnosti oproti zaisťovaniu minulých (zapísaných) údajov. Je obzvlášť potrebné si dať pozor na zle formulovaný príkaz (napr. *„prikazujú sa uchovávať všetky v budúcnosti získané počítačové údaje a zachovávať o tom mlčanlivosť“*). Tu môže dôjsť k tomu, že sa vykoná závažnejší zásah do práv vyšetrovaného bez procesnej kontroly súdu. Totiž takýto príkaz by *de facto* nahradil odpočúvanie (napr. streamované hovory, budúca prenášaná elektronická pošta atď.)

[461] § 70 ods. 1 TP: *„Kto napriek predchádzajúcemu napomenutiu ruší konanie alebo kto sa voči súdu, prokurátorovi, alebo policajtovi správa urážlivo, alebo kto bez dostatočného ospravedlnenia neposlúchne príkaz, alebo nevyhovie výzve alebo predvolaniu podľa tohto zákona, toho môže sudca a v prípravnom konaní prokurátor alebo policajt potrestať poriadkovou pokutou do 1 650 eur; ak ide o právnickú osobu, až do 16 590 eur. Na možnosť uloženia poriadkovej pokuty musia byť dotknuté osoby vopred upozornené.“*

6.3.8. Výkon príkazu

V prípade ak subjekt nevyhovie dobrovoľne príkazu, OČTK postupuje podľa § 91 TP (čo je spoločný postup pre vydanie veci). Podľa tohto ustanovenia, ak vec dôležitú pre trestné konanie alebo počítačové údaje na vyzvanie nevydá ten, kto ju má pri sebe, môže mu byť na príkaz predsedu senátu a v prípravnom konaní na príkaz prokurátora alebo policajta odňatá. Policajt potrebuje na vydanie takého príkazu predchádzajúci súhlas prokurátora. Bez predchádzajúceho súhlasu ho môže vydať len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť a vec neznesie odklad. K odňatiu veci sa podľa možnosti priberie nezúčastnená osoba. Otázkou ostáva, čo predstavujú pojmy „pri sebe“ a „podľa možnosti“ vo svetle počítačových údajov? Taktiež je dôležité sledovať, ako bude táto skutočnosť vyhodnotená súdom, resp. či bude mať vplyv na následnú zákonnosť dôkazu.[462] Problémom však ostáva, ako OČTK vykoná príkaz na odňatie počítačových údajov, ktoré sú nelokalizovateľné alebo v sústavnom pohybe (napr. cloud, ktorého dáta sa môžu fyzicky nachádzať na viacerých miestach – serverových farmách). Súdna prax o aktuálnych riešeniach týchto praktických otázok zatiaľ mlčí.

V prípade ak sa počítačové údaje nachádzajú na území SR, ich zaisteniu bude predchádzať dobre zvolená kriminalistická taktika - určenie typu požadovaných údajov, určenie ich pôvodcu a najmä zistenie ich aktuálneho držiteľa.[463] V prípade ak pôjde o údaje uložené na zahraničných serveroch (najčastejší prípad využívania služieb cloud storage akými sú DropBox, GoogleDrive, OneDrive atď.), je nutné využiť existujúci zmluvný rámec medzinárodnej spolupráce v trestných veciach a poznať *best practices* v oblasti vydávania údajov jednotlivých poskytovateľov týchto informačných služieb. Buď pôjde o vykonávanie jednotlivých úkonov právnej pomoci na základe

[462] Päť kritérií zákonnosti dôkazu v trestnom konaní podľa Repíka. Viď REPÍK, B. Procesní důsledky porušení předpisů o dokazování v trestním řízení, Bulletin advokacie, 1982, Str. 125-126 alebo MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P. a kol. Kurs trestního práva. Trestní právo procesní, 2003, Str. 408.

[463] Je potrebné dodať, že pôjde o odlišný postup podľa TP. Podľa Šamka *„obdobné ako pri zisťovaní obsahu emailovej komunikácie (z hľadiska možného využitia príkazu podľa) to bude aj v prípadoch, v ktorých sa budú údaje dôležité pre trestné konanie (napr. rôzne účtovné dokumenty) nachádzať na rôznych webových úložiskách (tzv. cloud computing), ktoré umožňujú užívateľom ukladať a zdieľať súbory.”* Ibid. ŠAMKO, P. Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestom konaní. 2017.

medzinárodnej zmluvy alebo o realizáciu právnej pomoci bez zmluvného základu (viď 3. kapitolu o informačnej suverenite štátu a cezhraničnom dokazovaní).[464]

Je možné ešte spomenúť prípad riešený pred ÚS SR, kedy Protimonopolnému úradu SR vo veci *dawn raid* bolo zakázané pokračovať ďalej v prehliadaní dátového nosiča vyšetrovaného subjektu NS SR (bolo rozhodnuté o nezákonnom zásahu orgánu štátnej správy). Avšak tento skúmaný dátový nosič v zmysle ustanovenia § 89 TP Protimonopolný úrad SR následne vydal vtedajšiemu Úradu boja proti korupcii, ktorý až po jeho dôslednom prezretí vydal príkaz v zmysle § 90 TP na vydanie počítačových údajov. Takéto konanie vykazovalo znaky excesu OČTK. Napriek tomu ÚS SR k námietke nezákonného dôkazu konštatoval, že *„v tomto kontexte neobstojí námietka sťažovateľov o tom, že orgán činný v trestnom konaní zadovážil dôkaz „z otráveného stromu.“* Protimonopolný úrad SR bol povinný nepokračovať v prezeraní dátového nosiča, na druhej strane však týmto rozhodnutím nebola obmedzená jeho edičná povinnosť podľa § 89 TP a neboli ním limitované ani oprávnenia OČTK na postup podľa § 89 a § 90 TP.[465] Aj keď ustanovenie je pokrokové a počíta s odňatím počítačových údajov, jeho faktická realizácia môže byť komplikovaná. Zdá sa, že pri odňatí je celá koncepcia prísne viazaná na dátový nosič – vec.

Zákon pre vykonanie procesných úkonov stanovuje náležitosti zápisnice. Zápisnica alebo potvrdenie o zaistení počítačového údaja často predstavuje ťažiskový dokument pre kontrolu legálnosti takéhoto zásahu. Zápisnica musí obsahovať

[464] Príkladom môže byť spolupráca členských štátov EÚ, kde základom sú články 82 a 86 Zmluvy o fungovaní Európskej únie. Dňa 29. mája 2000 Rada ministrov EÚ schválila Dohovor o vzájomnej pomoci v trestných veciach, ktorého cieľom je podporovať spoluprácu medzi justičnými, policajnými a colnými orgánmi v rámci Únie doplňovaním ustanovení v existujúcich právnych nástrojoch z 20.4.1959. Taktiež významnú rolu zohráva aj budapeštiansky Dohovor o počítačovej kriminalite zo dňa 23.11.2001. V neposlednom rade ide o Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, vypracovaný Radou v súlade s článkom 34 Zmluvy o EÚ. Justičná spolupráca v trestných veciach v rámci Európskej únie stojí na dvoch kľúčových princípoch: na uznávaní rozsudkov a súdnych rozhodnutí a taktiež na zbližovaní právnych predpisov členských štátov. Ide najmä o úpravu v prípade príkazu na zaistenie majetku a dôkazov v prípade zaisťovania elektronických dôkazov v pôsobnosti cudzieho prevádzkovateľa sociálnej siete. Vyjadrenie týchto princípov vo sfére dokazovania bolo zavŕšené v smernici Európskeho parlamentu a Rady č. 014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. Viď Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. [online]. [cit.1.9.2020]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0041&qid=1430677259904&from=EN alebo Návrh nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [online]. [cit.1.9.2020]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/sk/pdf

[465] Uznesenie ÚS SR, sp. zn. III. ÚS 24/2012-53 zo dňa 17.1.2012.

dostatočne presný opis vydanej veci, odňatej veci, prevzatej veci (dátového nosiča) alebo počítačových údajov (napr. meno a špecifikáciu zaistených súborov, resp. partícií diskov), ktoré umožnia určiť ich totožnosť. Osobe, ktorá vec alebo počítačové údaje vydala alebo ktorej boli vec alebo počítačové údaje odňaté, alebo od ktorej boli vec alebo počítačové údaje prevzaté, vydá orgán, ktorý úkon vykonal, ihneď písomné potvrdenie o prevzatí veci alebo počítačových údajov alebo rovnopis zápisnice. Podstatné je ustanovenie ods. 2 druhá veta § 93 TP, ktoré hovorí, že *„osobu, ktorej počítačové údaje boli zaistené, o tom písomne vyrozumie orgán, ktorý počítačové údaje prevzal.“* Toto ustanovenie môže spôsobovať interpretačný problém, či ide o osobu, ktorá má tieto údaje v držbe alebo o osobu, ktorá je ich pôvodcom. Aj keď gramatickým výkladom sa dá vyvodiť záujem zákonodarcu chrániť procesné postavenie pôvodcu (zákonná záruka), prax OČTK ukazuje na to, že tie sú na akékoľvek informácie skúpe a tieto dotknuté osoby žiadnym spôsobom neinformujú v prípade, ak zaisťujú počítačové údaje v detencii tretích osôb.[466] Správny postup by mal byť ten, kedy OČTK informuje pôvodcu údajov. Takáto informácia môže byť vykonaná ústne, elektronicky alebo písomne, avšak musí byť vierohodne zaznamená vo vyšetrovacom alebo súdnom spise.

6.4. Úvaha *de lega ferenda*

Aj keď súčasná judikatúra ESĽP nevyžaduje explicitnú zákonnú úpravu pre zaistenia počítačových údajov,[467] je v závere vhodné poukázať na niektoré pozitíva tohto inštitútu oproti všeobecnej edičnej povinnosti podľa § 89 TP (resp. § 78 TŘ) alebo domovej prehliadke podľa § 99 TP (resp. § 82 TŘ).[468] V prípade zaistenia počítačových údajov priamo z dátového nosiča – veci (napr. viaceré diskové polia,

[466] Svedčí o tom prípad, kedy príkaz na uchovávanie počítačových údajov špeciálna prokuratúra adresovala samotnému vyšetrovateľovi policajného zboru: *„V súvislosti s vybavením podnetu prokurátor konštatoval, že je pravdou, že 18. mája 2011 protimonopolný úrad „zápisnične“ vydal inkriminovaný disk vyšetrovateľovi úradu boja proti korupcii, ale zároveň dodal, že pri postupe podľa § 89 ods. 1 Trestného poriadku nedochádza k vydaniu rozhodnutia. […] Okrem toho prokurátor konštatoval, že vzhľadom na to, že sa javilo, že na vydanom disku sa nachádzajú počítačové údaje a že tieto je potrebné uchovať, udržiavať v celosti, prípadne vyhotoviť a ponechať si orgánmi činnými v trestnom konaní kópie takých údajov, 27. mája 2011 vydal [prokurátor špeciálnej prokuratúry] v súlade s § 90 Trestného poriadku príkaz na uchovanie a vydanie počítačových údajov.“* Viď Uznesenie ÚS SR, sp. zn. III. ÚS 24/2012-53 zo dňa 17.1.2012.

[467] Vec Wieser a Bicos Beteiligungen GmbH proti Rakúsku. Rozhodnutie ESĽP zo dňa 16.10.2007, sp. zn. 74336/01 [online]. [cit.1.9.2020]. Dostupné z: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82711

[468] Výkladové stanovisko NSZ por. č. 9/2001 Zb. tvrdí, že ako vec dôležitú pre trestné konanie je možné zaistiť aj výpočtovú techniku a záznamové médiá. Viď § 82 ods. 1 TŘ. ŠÁMAL, P. a kol.: Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013, Str. 1114.

vysoko kapacitné úložiská), OČTK má zákonnú možnosť selektovať a citlivo vyberať tie údaje, ktoré sú pre trestné konanie naozaj dôležité. Je zrejmé, že odstavením celého počítačového systému môže dôjsť k závažným ekonomickým škodám na strane povinného alebo iných tretích osôb. Je pravda, že tento postup tu bolo možné dovodiť aj pred zakotvením tohto inštitútu. Avšak povinnosti, akými sú uchovanie a udržiavanie v celistvosti, umožnenie vyhotovenia a ponechania si kópie údajov, znemožnenie prístupu k údajom alebo povinnosť odstránenia údajov z počítačového systému dávajú OČTK celú novú škálu nástrojov pre boj s počítačovou kriminalitou.

Ďalej to je otázka ústavnoprávnej proporcionality zásahov. ÚS SR v prípade prehliadky advokátskej kancelárie judikoval, že *„záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov zaistenia osôb a vecí musí byť uvedený do rovnováhy so závažnosťou zásahu do tohto práva. Odkázal tak na princíp proporcionality.“* Podľa jeho názoru to znamená *„zvoliť si pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa. Je preto potrebné uprednostniť úkon uchovania a vydania počítačových údajov pred inštitútom vydania, resp. odňatia veci. V opačnom prípade znamená neproporcionálny postup konajúceho orgánu porušenie garancií práva na súkromie a spravodlivého procesu.“*[469] Je možné zhrnúť, že pokiaľ existujú prostriedky, ktoré umožnia realizáciu citovaného cieľa a zároveň predstavujú menej radikálny zásah do chránených práv, je nevyhnutné použiť práve tieto prostriedky. Menej radikálny zásah do chránených práv je práve inštitút uchovania a vydania počítačových údajov oproti všeobecnej edičnej povinnosti podľa § 89 TP (resp. § 78 TŘ). Umožňujú totiž voči tretím osobám uplatňovať miernejší prostriedok zásahu (vydanie konkrétnych počítačových údajov pred vydaním celistvého dátového nosiča, čo predstavuje krajné riešenie). Na druhú stranu je však nutné podotknúť, že praktická aplikácia princípu proporcionality v otázkach zaisťovania počítačových údajov je obzvlášť náročná v prípade osoby, ktorá je v postavení podozrivého (resp. obvineného alebo obžalovaného). OČTK v tomto prípade môžu čeliť obvyklému problému – rezistencii týchto osôb a musia postupovať pomocou efektívnejších zaisťovacích mechanizmov (domová prehliadka, sledovanie osôb a vecí atď.) v záujme naplnenia základného účelu trestného procesu.

[469] Ibid. Nález ÚS SR zo dňa 25. augusta 2010, sp. zn. III. ÚS 68/2010.

V neposlednom rade je možné odporučiť, aby technická forma realizácie zaistenia počítačových údajov bola popísaná vo verejne dostupnom odporúčaní - smernici alebo vnútornom predpise policajného zboru. Každé zaistenie počítačových údajov by malo vychádzať z princípu zachovania proporcionálneho postupu, t.j. mal by byť zvolený taký postup OČTK, ktorý nepredstavuje väčší zásah do práv ako sú tie záujmy, ktoré sa týmto procesným postupom chránia.

Taktiež by sa mala uplatňovať zásada nezmeniteľnosti otlačku počítačového údaja od jeho prvého zaistenia až po jeho vykonanie (resp. odovzdanie znalcovi). Práve táto skutočnosť by mala byť reflektovaná nielen v možnosti dotknutej osoby získať opis zápisnice alebo potvrdenia pri zaistení počítačového údaja s otlačkom (kópiou), ale aj v samotnej možnosti vyhotoviť si rovnocenný otlačok (kópiu) pre vlastnú potrebu toho, čo si odniesol OČTK. Zaistené počítačové údaje sú súčasťou trestného spisu a osoba (najmä ak ide o osobu odlišnú od páchateľa) by mala mať postavenie zúčastnenej osoby, a teda právo do takéhoto spisu nazerať.

V neposlednom rade je nevyhnutná transparentnosť v procese nakladania so zaistenými počítačovými údajmi a taktiež reálna možnosť procesnej kontroly nad spôsobom ich zaisťovania a nakladania s nimi.

6.5. Zhrnutie kapitoly

V predloženej kapitole sme osvetlili zaistenie elektronického dôkazného prostriedku podľa trestných poriadkov ČR a SR. Zamerali sme sa na zaistenie dát a analyzovali jednotlivé procesné inštitúty v slovenskom trestnom poriadku v komparácii s existujúcou, ale aj budúcou českou úpravou.

Zistenie skutkového stavu, o ktorom neexistujú dôvodné pochybnosti, a to v takom rozsahu, ktorý je nevyhnutný pre rozhodnutie, predstavuje vyjadrenie cieľu trestného práva procesného.[470] Voľba prostriedkov pre dosiahnutie tohto cieľu musí spĺňať základné požiadavky ústavnosti. Ak česká rekodifikačná komisia uvažuje o zavedení nového inštitútu zaistenia počítačových údajov s úmyslom zrýchliť a zjednodušiť procesné štádium zaisťovanie a vykonávania dôkazov, je možné poukázať na príklad

[470] Zásada materiálnej pravdy. Viď Ministerstvo spravedlnosti ČR: Komise pro nový trestní řád. Východiska a principy nového trestního řádu [online]. [cit.1.9.2020]. Dostupné z: http://portal.justice.cz/Justice2/soubor.aspx?id=112883 Str. 33.

slovenskej úpravy ako jeden z možných exemplárov.[471] Aj keď niektoré otázky slovenská súdna prax stále nevyriešila, definícia počítačových údajov sa zdá byť vhodná. Text zákona nemusí vždy za každú cenu dobiehať stav technológie (mnohé podstatné otázky sú aj tak vyriešené), ale spresnenie termínov a príkazov smerujúcich k počítačovým údajom, no najmä ich terminologické oddelenie od dátového nosiča, prispievajú lepšiemu pochopeniu procesu dokazovania. Práve jasná definícia procesných záruk dotknutej osoby pri zaisťovaní počítačových údajov predstavuje jednu z možných ciest pre budúci vývoj. Aj keď sa môže zdať, že záruky prvotne vyznievajú v prospech páchateľa, ich zakotvenie v procesnom poriadku nielenže stanoví limity špekulatívnej obhajoby, ale súčasne aj dodá sebaistotu OČTK vstupovať do situácií, ktoré sa predtým zdali byť nejasné.

[471] Možným elegentným riešením je práve §e42 ods. 2 paragrafového znenia návrhu rekodifikácie trestného práva procesného keď *„ustanovení o věcech se vztahují i na data uchovávaná v elektronické podobě, nevyplývá-li z jednotlivých ustanovení trestněprocesního zákona něco jiného.“* Pracovní verze paragrafového znění, které je aktuální ke dni 1. 1. 2020. [online]. [cit.1.9.2020]. Dostupné z: https://tpp.justice.cz

7. Vnútorná informácia súkromnej spoločnosti o kyberútoku ako elektronický dôkazný prostriedok*

7.1. Úvodné poznámky

V marci 2016 došlo ku masívnemu kyberútoku na viaceré americké advokátske kancelárie, ktoré zastupujú najväčšie verejne obchodovateľné korporácie (Cravath, Weil Gotshal). [472] Obdobne v roku 2017 kybernetický útok ochromil operácie spoločnosti jednej z najväčších advokátskych kancelárií.[473] Zaujímavosťou tohto útoku je, že na rozdiel od nedávneho prípadu odcudzenia množstva kreditných kariet a osobných údajov z banky JP Morgan Chase,[474] tento učebnicový hackerský útok smeroval k získaniu dôverných a vnútorných informácií klientov. Išlo vlastne o protiprávne zbieranie uzavretých elektronických dôkazov o tom, ako sa darí alebo nedarí rôznym komerčným subjektom (vnútorná informácia). Účelom útoku bola ich analýza a následné zobchodovanie. Držanie vnútornej informácie a vyčkávanie na jej vhodné použitie má niekoľko následkov. Za prvé, táto taktika útočníkov sťažuje prácu OČTK. Za druhé, následok tohto činu je nekontrolovateľný, a to najmä v prípade neochoty advokátskych kancelárií informovať o útoku svojich klientov alebo verejnosť. V USA tento prípad otvoril diskusiu o tom, či má právny zástupca klientov - verejne obchodovateľných spoločností povinnosť informovať širokú verejnosť v prípade kyberútoku.[475] Otázkou ostáva, akým spôsobom a aké elektronické dôkazy o tomto útoku má zaistiť a vysvetliť? Takáto povinnosť sa už však dávno vzťahovala

* Táto kapitola vychádza z publikovaného článku ABELOVSKÝ, Tomáš. Kyberútok ako vnútorná informácia alebo kedy s pravdou von. Revue pro právo a technologie. [Online]. 2017, č. 15, Str. 33-49.

[472] HONG, N. a Sidel, R., Hackers Breach Law Firms, Including Cravath and Weil Gotshal. The Wall Street Journal. [Online]. [cit.1.9.2020]. Dostupné z: http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

[473] DLA Passes Third Day Without Email After Malware Attack. Law360, New York. June 29, 2017. [Online]. [cit.1.9.2020]. Dostupné z: https://www.law360.com/articles/939824/dla-passes-third-day-without-email-after-malware-attack

[474] What lies behind the JPMorgan Chase cyber-attack. The Economist. [Online]. [cit.1.9.2020]. Dostupné z: http://www.economist.com/news/business-and-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itself-what-lies-behind

[475] 47 štátov má vlastnú legislatívu týkajúcu sa porušenia osobných údajov (security breach notification laws), ktorá ma pôvod v kalifornskej úprave. Viď Cal. Civ. Code 1798.82 and 1798.29. [Online]. [cit.1.7.2020]. Dostupné z: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

na subjekty regulované americkou komisiou pre cenné papiere a burzu (SEC).[476] Nasledujúca kapitola sa snaží odpovedať na otázku, kedy a či vôbec má tuzemský emitent finančného nástroja (povinná osoba)[477] povinnosť uverejniť informáciu o kyberútoku na jej informačný systém.[478] Rovnako sa snaží vysvetliť to, že nie len súdy alebo štátne orgány majú záujem na kvalitnom objasnení elektronického dôkazného prostriedku, ale môžu to byť práve aj súkromné subjekty, ktoré si vo vlastnom záujme nastavia procesy a postupy tak, aby boli schopné presvedčiť verejnosť, ich veriteľov, vlastníkov, zákazníkov a regulátorov o tom, čo sa odohralo pri nechcenom kyberútoku.

7.2. Povinná osoba

Právna úprava kapitálového trhu definuje širokú skupinu povinných osôb, ktoré majú notifikačnú povinnosť či už voči dozornému orgánu alebo verejnosti. Ako príklad môže poslúžiť akciová spoločnosť, ktorá je emitentom investičného nástroja obchodovaného na regulovanom trhu EÚ (napr. na Burze cenných papírů Praha).[479] Táto obchodná spoločnosť má zákonnú povinnosť bezodkladne zverejňovať a oznamovať tie vnútorné informácie, ktoré sa jej priamo týkajú.[480] Je možné predpokladať, že emitent, ktorý má kapitálovú účasť širšej verejnosti, si nesie dôležitú

[476] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance. 2011. [Online]. [cit.1.9.2020]. Dostupné z: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[477] Emitentom je právnická osoba, ktorá sa riadi súkromným alebo verejným právom a ktorá emituje finančné nástroje alebo navrhuje ich emisiu, pričom emitent je v prípade depozitných certifikátov zastupujúcich finančné nástroje emitentom zastupovaných finančných nástrojov.

[478] Právny problém bude analyzovaný vo svetle platnej právnej úpravy ČR (zákon č. 256/2004 Sb. o podnikání na kapitálovém trhu), SR (zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov, zákon č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov.) a nariadenia Európskeho parlamentu a rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (MAR) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES. Český zákon používa pojem *„vnitřní informace“*, slovensky *„dôverná informácia“* a nariadenie *„inside information“* (Article 7). Pre potreby tejto práce bude používaný promiskue pojem *„dôverná informácia“* aj keď je jeho význam v obchodnoprávnych vzťahoch odlišný. Viď KOTÁSEK, Josef. Ochrana vnitřních informací. Brno: Tribun EU, 2008. 255 s. ISBN 978-80-7399-355-9. Str. 77 an.

[479] Napr. obchodník s cennými papierami a inštitucionálny investor, organizátor regulovaného trhu, emitent cenných papierov, osoba podieľajúca sa na rozhodovaní emitenta a osoby jej blízke, akcionár v špecifickej situácii, zamestnanci alebo iné osoby pri výkone svojho zamestnania, povolania alebo funkcie, alebo osoby v súvislosti s plnením svojich povinností na obchodoch s investičnými nástrojmi. Podľa na nariadenia o zneužívaní trhu je *„emitent“* právnická osoba, ktorá sa riadi súkromným alebo verejným právom a ktorá emituje finančné nástroje alebo navrhuje ich emisiu, pričom emitent je v prípade depozitných certifikátov zastupujúcich finančné nástroje emitentom zastupovaných finančných nástrojov.

[480] MAR ukladá emitentom finančných nástrojov v čl. 17 ods. 1 povinnosť uverejňovať tzv. vnútorné informácie, ktoré sa ich priamo týkajú.

povinnosť čo najskôr informovať akcionárov alebo investorov o vnútorných informáciách, ktoré môžu mať vplyv na cenu jej emitovaných finančných nástrojov (napr. akcií).

Filozofia tejto úpravy spočíva v tom, že ide jednak o prevenčný boj s *insider tradingom*, ale rovnako aj o záväzok kapitálovej spoločnosti voči svojím akcionárom, ale aj potencionálnym investorom. Spoločnosť môže svoje financovanie hľadať na kapitálových trhoch – burzách, čo však na rozdiel od USA nie je zvykom pre kontinentálne burzy. Napokon aj prísna verejná regulácia emitenta (napr. akciovej spoločnosti) je znakom toho, že štát má záujem na transparentnosti obchodných transakcií takejto spoločnosti. Vyššie uvedená povinnosť trvá aj z dôvodu, že spoločnosť si potrebuje sústavne budovať vlastnú dôveru u svojich akcionárov, potencionálnych investorov, partnerov, zákazníkov a v neposlednom rade trhu ako takého. Americká teória pri zákaze *insider tradingu* hovorí o *fiduciárnej povinnosti* voči investorom (akcionárom), resp. o rovnom a férovom prístupe k obchodovateľným nástrojom (*equal access*), ale aj o predchádzaní zneužitia takejto informácie (prípady *Chiarella*, *Dirks*).[481] Je zrejmé, že táto teória ovplyvnila aj európsku reguláciu. Tá akcentuje zákaz transakcií zasvätených osôb (s výnimkami pre určité osoby a určité transakcie, v režime *safe harbour*), s určitými prvkami transparentnej evidencie (vedenie zoznamov zasvätených osôb, oznamovanie transakcií).[482]

7.3. Kyberútok ako vnútorná informácia

Kyberútok je možné definovať ako čin s použitím počítača alebo súvisiacich technológií, siete alebo systémov, smerujúci k narušeniu, odcudzeniu alebo zničeniu informačného systému (resp. tam uložených dát) a majetku. Pre potreby tejto kapitoly bude používaný zjednodušený pojem kyberútok. [483] Kyberútok voči súkromnej

[481] SCHEPPELE, Kim Lane. „It's Just Not Right": The Ethics of Insider Trading. Law and Contemporary Problems, Vol. 56, No. 3, Modern Equity, Summer, 1993. Str. 124 an. alebo Ibid. KOTÁSEK, Str. 41 an.

[482] Ibid. KOTÁSEK, Str. 51 an.

[483] Český zákon o kybernetickej bezpečnosti rozoznáva kybernetickú bezpečnostnú udalosť a incident. *„Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. "* Viď § 7 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

spoločnosti je väčšinou motivovaný nedovoleným obohatením na úkor napadnutej osoby. Trestný zákon definuje trestný čin neoprávneného prístupu k počítačovému systému alebo nosiču informácií pomocou prekonania bezpečnostného opatrenia a tým neoprávnené získanie prístupu k počítačovému systému alebo k jeho časti.[484] Predmetom tohto činu v prípade akciovej spoločnosti môže byť široká paleta vnútorných informácií alebo osobných údajov, ktoré spravujú zasvätené osoby:[485] napr. vnútorná databáza partnerov a ich platby, nezverejnené účtovníctvo a súvisiace správy, pripravované podnikateľské zámery a projekty, pripravovaný odpredaj podniku atď. Je zrejmé, že každá z týchto informácií má potenciál ohroziť úplnú a riadnu transparentnosť trhu. Najmä v prípade, ak by sa dostala do rúk len niektorých účastníkov trhu (zneužívanie trhu).[486] Základným motívom je zvyčajne obchodovanie s využitím týchto vnútorných informácií. Útočníkom môže byť externá osoba, ale aj zamestnanec, resp. zasvätená osoba emitenta. Zainteresované subjekty (napr. hacker) tak získavajú nespravodlivú výhodu na úkor poškodenej osoby na základe vnútornej informácie, o ktorej pred útokom nevedeli, a v dôsledku toho narušujú integritu finančných trhov a dôveru investorov.[487]

Otázkou zostáva, či odhalený kyberútok na akciovú spoločnosť je sám o sebe dôvernou informáciou, ktorú má táto spoločnosť zverejniť, resp. sprístupniť a akú kvalitu musí mať taká informácia (resp. získaný dôkaz)?

[484] § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací), § 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) a § 232 (Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti) TZ ČR alebo § 247 (Neoprávnený prístup do počítačového systému), § 247a (Neoprávnený zásah do počítačového systému), § 247b (Neoprávnený zásah do počítačového údaja), § 247c (Neoprávnené zachytávanie počítačových údajov) a § 247d (Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov) TZ SR.

[485] Zasvätenou osobou môže byť osoba, ktorá získala dôvernú informáciu. Viď Vykonávacie nariadenie Komisie (EÚ) 2016/347 z 10. marca 2016, ktorým sa stanovujú vykonávacie technické predpisy, pokiaľ ide o presný formát zoznamov osôb, ktoré majú dôverné informácie, a pre aktualizáciu zoznamov osôb, ktoré majú dôverné informácie, v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 596/2014.

[486] Zneužívanie trhu je pojem, ktorý zahŕňa neoprávnené konanie na finančných trhoch a na účely tohto nariadenia by sa mal chápať tak, že pozostáva z obchodovania s využitím dôverných informácií, neoprávneného zverejňovania dôverných informácií a manipulácie s trhom. Takéto konanie bráni úplnej a riadnej transparentnosti trhu, ktorá je predpokladom pre obchodovanie všetkých hospodárskych subjektov na integrovaných finančných trhoch. Viď rec. 7. MAR.

[487] Rec. 23. MAR.

Aby informácia o kyberútoku bola vnútornou informáciou, musí vykazovať nasledujúce znaky, ktoré musia byť splnené súčasne:[488]

a) *týka sa skutočnosti významnej pre vývoj kurzu či inej ceny finančného nástroja alebo jeho výnosu,*
b) *nie je verejne známa,*
c) *je presná a*
d) *mohla by potom, čo by sa stala verejne známou, významne ovplyvniť kurz, inú cenu alebo výnos finančného nástroja alebo iného nástroja, ktorého hodnota sa odvodzuje od tohto finančného nástroja.*

Z pohľadu možných následkov, nie je kyberútok odlišný od iného protiprávneho konania smerujúceho k poškodeniu majetku napadnutej osoby.[489] Ide o virtualizovaný útok na virtualizované záujmy obete, ktorého následok sa vždy aktualizuje do úbytku aktuálnych hodnôt. Odlišnosť je možné vidieť v povahe následkov, nakoľko samotný kyberútok nemusí byť odhalený vôbec. Medzi najčastejšie následky patrí priama a vyčísliteľná škoda (napr. odcudzenie hodnotných vnútorných údajov), ušlý zisk (napr. zmarená transakcia), zvýšené náklady na kybernetickú ochranu, náklady na konzultačnú činnosť expertov a právnikov, súdne poplatky a v neposlednom rade nemajetková škoda na povesti. Štatisticky sa uvádza, že útok je zistený v priemere až po 205 dňoch.[490] Tým, že vo virtualizovanom móde je každá informácia *potenciálne ubiquitná*, jej odcudzenie vo fyzickom zmysle slova nehrozí. Avšak jej zneužitie je ďaleko škodlivejšie. Pri odhaľovaní kyberútokov sa bezpečnostní analytici sústredia na kontamináciu alebo narušenie systému podozrivými inštrukciami alebo na chovanie operačného systému a analyzujú sieťovú prevádzku. Takýto bezpečnostný incident

[488] Čl. 7 ods. 1 písm. a) MAR.

[489] Metodika ČNB uvádza ako príklad kurzotvornej informácie *„informace o zahájení nebo ukončení soudních, správních nebo rozhodčích řízení, které mají nebo by mohly mít významný vliv na finanční situaci nebo ziskovost emitenta finančního nástroje, např. uložení významné pokuty nebo povinnosti k náhradě škody významného rozsahu, včetně řízení svýznamným dopadem na reputaci emitenta finančního nástroje apod.“* pod ktorú je možné následky kyberútoku podradiť. ČNB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018. [Online]. [cit.1.9.2020]. Dostupné z: https://www.cnb.cz/cs/casto-kladene-dotazy/Soubor-odpovedi-na-dotazy-souvisejici-s-regulaci-ochrany-proti-zneuzivani-trhu-a-transparentnosti-28.-11.-2018/

[490] BITGLASS. “Where’s your data?” experiment. [Online]. [cit.1.9.2020]. Dostupné z: https://pages.bitglass.com/rs/bitglass/images/BR-Bitglass_Wheres_Your_Data.pdf

však ešte nemusí spôsobiť priamu škodu. Je preto odlišný od prípadu, kedy sa do archívu spoločnosti vláme zlodej a odcudzí doklady pripravovanej fúzie. Identifikácia chýbajúceho fyzického dokumentu je možná a navyše je zrejmé, s akou sumou informácií sa mohol zlodej oboznámiť v danom čase a na danom mieste. Kyberútoky sú častokrát koncipované vo vrstvách. Každá vrstva odhaľuje ďalšiu vrstvu iného útoku na iné záujmy v napadnutom informačnom systéme. Avšak nie vždy sa podarí vypátrať všetky vrstvy.

Aby kyberútok mal význam pre notifikačnú povinnosť, informácia o ňom musí predstavovať vnútornú informáciu, ktorá sa ho priamo týka. Ide o informáciu, ktorá sa priamo dotýka emitenta finančného nástroja, jeho hospodárskej situácie a vyhliadok do budúcnosti, prípadne ktoré sa týkajú práv plynúcich z finančného nástroja. Podľa usmernenia ČNB ide: [491]

„Např. o rostoucí ceně ropy, změně úrokových sazeb, uzavření dohody regulovaného trhu s tvůrcem trhu o zajištění likvidity k akciím emitenta finančního nástroje aj. Naprostá většina takových informací se šíří nezávisle na emitentovi finančního nástroje. Pokud by však nastala situace, kdy se emitent finančního nástroje nebo kdokoliv jiný dozví přesnou neveřejnou informaci, která může mít významný vliv na hospodaření emitenta finančního nástroje a výnosy z účasti na něm a je cenotvorná, je povinen nakládat s ní jako s vnitřní informací.“

Informácia, ktorá sa emitenta finančného nástroja týka nepriamo, zostáva vnútornou informáciou do doby, pokiaľ nebude verejne dostupná. Emitent finančného nástroja ju však uverejniť nemusí.

Preto informácia o kyberútoku musí splniť nasledujúce podmienky:

- *kyberútok je cielený na informačný systém v kompetencii emitenta (priamo alebo nepriamo spojený s emitentom); a*
- *následok zverejnenia informácie emitentom o prebiehajúcom kyberútoku má sám o sebe potenciál ovplyvniť cenu finančného nástroja (hovoríme o teste*

[491] Ibid. ČNB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018.

cenovej citlivosti na možnú škodu alebo iný následok vyvolaný kyberútokom).

Vyššie uvedený potenciál v zmysle MAR je definovaný tak, že následok (ne)zverejnenia má pravdepodobný vplyv na cenu finančného nástroja.[492] Je zrejmé, že táto pravdepodobnosť nebude hraničiť s istotou, avšak musí vyznieť dostatočne presvedčivo. Bude posudzovaná individuálne od prípadu k prípadu. Je možné zhrnúť, že ak emitent vie o kyberútoku, ktorý prebehol alebo prebieha v takom rozsahu, že každý riadny hospodár, resp. uvážlivý investor by nadobudol presvedčenie o tom, že takýto útok ovplyvní hodnotu jeho podniku z pohľadu jeho majetku, bezpečnosti, ušlého zisku, prípadných sporov alebo povesti, má tento útok pravdepodobný vplyv na cenu.

7.4. Dostupnosť informácie o kyberútoku

Informácia o kyberútoku sa stáva verejnou informáciou v čase, keď bola sprístupnená tej časti investorov, ktorí sa zhromažďovaním informácií tohto typu a ich hodnotením aktívne zaoberajú (napr. sledujú odvetvie, v ktorom pôsobí emitent). Všeobecne sa považuje informácia za verejne známu, ak je zverejnená voči širokému publiku investorov neurčitého počtu. Ďalej je verejne známa aj taká informácia, ktorá je dostupná súčasným i potenciálnym investorom, aj keď nebola zverejnená emitentom včas a riadne. Navyše nie je podstatné, či informáciu uverejnil emitent finančného nástroja alebo či sa stala známou z iných zdrojov.[493]

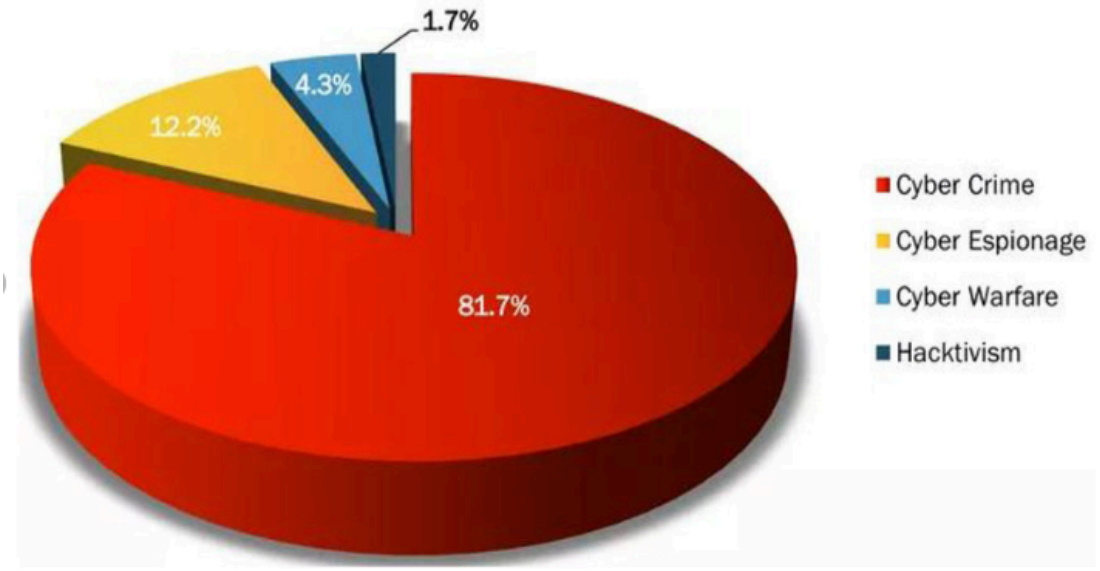
Môže sa stať, že kyberútok je vykonaný v tichosti a samotná informácia o ňom nemá dôvod preniknúť na verejnosť. Avšak motívy útočníkov sú rôznorodé. Niektorí predbehnú v informovaní o útoku svoje obete, iní využijú strach zo straty reputácie a pokračujú v tichom vydieraní. Najčastejšie motívy sú vždy kriminálne s úmyslom obohatiť sa, čo dokresľuje nasledovná štatistika:[494]

---

[492] Článok 7 ods. MAR.

[493] Ibid. ČNB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018.

[494] KARIE, Nickson. KEBANDE, Victor. VENTER, H. Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy. 2019. [Online]. [cit.1.9.2020]. Dostupné z: https://www.researchgate.net/publication/332220947_Diverging_deep_learning_cognitive_computing_techniques_into_cyber_forensics



Major motivation of attacks (Source: Hackmageddon, (2018), Cyber Attacks Statistics).

Príkladom medzinárodnej špionáže spolu s kriminálnou činnosťou bol masívny kyberútok na spoločnosť Sony v roku 2014. Informácia o kyberútoku prenikla na verejnosť v novembri 2014, keď hackerská skupina *Guardians of Peace* začala zverejňovať skopírované dáta. Samotná spoločnosť v tom čase už o útoku vedela, ale zvolila vyčkávaciu taktiku (resp. bola ním zaskočená do takej miery, že nevedela čo robiť).[495] Je zrejmé, že útočník má často v rukách rozhodnutie o tom, či informácia o kyberútoku zostane vnútorná alebo verejná. Sám je viazaný povinnosťou mlčanlivosti. Spáchaním trestného činu, t.j. kyberútoku, sa dostal do rovnakého postavenia ako emitent, t.j. do postavenia zasvätenej osoby. Bolo by však naivné sa domnievať, že útočník po spáchaní kyberútoku dodrží povinnosť mlčanlivosti.[496] To

[495] SEAL, Mark. An Exclusive Look at Sony's Hacking Saga. Vanity Fair. Retrieved February 4, 2015.[Online]. [cit.1.9.2020]. Dostupné z: http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

[496] *Insider trading* sa vyznačuje tým, že zasvätená osoba poruší nejakú z nasledujúcich povinnosti: nesmie využiť vnútornú informáciu k svojmu alebo cudziemu prospechu, nesmie ju oznámiť alebo sprístupniť inej osobe a nesmie dávať odporúčania inej osobe na základe znalosti vnútornej informácie.

má však už aj trestnoprávny rozmer v naplnení niektorých ďalších trestných činov a poškodený musí predvídať takéto konanie.[497]

7.5. Presnosť informácie o kyberútoku

Presnosť informácie je žiadúca najmä z dôvodu, aby sa predišlo nedorozumeniu o tom, či ide o exaktnú informáciu alebo o špekulácie a fámy. Navyše táto presnosť je naviazaná na potenciál informácie ovplyvniť trh s finančnými nástrojmi. MAR hovorí, že *„právna istota pre účastníkov trhu by sa mala zvýšiť prostredníctvom užšieho vymedzenia dvoch z prvkov nevyhnutných pre vymedzenie dôvernej informácie, a to presnosti tejto informácie a významnosti jej možného účinku na ceny finančných nástrojov, súvisiacich spotových zmlúv týkajúcich sa komodít alebo dražených produktov založených na emisných kvótach.“*[498] Kotásek uvádza, že *„do istej miery možno dostatočnú záruku presnosti informácií vidieť [aj] v tom, že sú vnímané ako informácie, ktorých obsahom sú "skutočnosti", t.j. preukázateľné a dôkazom prístupné udalosti a stavy vonkajšieho sveta.“*[499] Žiaľ z právnej úpravy nemôžeme dovodiť to, že by informácia mala byť úplne exaktná. Môžeme sa pýtať, ako veľmi presná má byť informácia o kyberútoku na to, aby išlo o vnútornú informáciu, ktorá bude mať vplyv na kurz alebo cenu príslušného nástroja? Všeobecne pôjde o takú mieru presnosti, ak je natoľko určitá a spoľahlivá, že sa na jej základe môže investor rozhodovať. ČNB uvádza dva príklady:[500]

„Přesná tedy může být informace o tom, že kótovaná společnost jedná o převzetí jiné společnosti, přestože zatím konečné rozhodnutí nepadlo a k převzetí třeba ani nedojde. Podobně může být přesná informace o tom, že se okruh zájemců o strategické partnerství zúžil bez ohledu na to, že konečný vítěz zatím není znám. Podmínkou přesnosti tedy není definitivnost informace.“

[497] V ČR môže ísť o trestný čin neoprávněné nakládání s osobními údaji (§ 180 TZ), poškození cizích práv (§ 181 TZ), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ), porušení předpisů o pravidlech hospodářské soutěže (porušování obchodního tajemství, § 248(1)h TZ), na SR to bude zrkadlovo najmä ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva (§ 264 TZ).

[498] Rec. 18 MAR.

[499] Ibid. KOTÁSEK, Str. 107.

[500] Ibid. ČNB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018.

Odpoveď je možné nájsť v prípade *Lafont,* kde SDEÚ dovodil, že podmienka presnej informácie nevyžaduje, aby z nej bolo zrejmé, v akom smere bude mať táto informácia vplyv na kurz alebo cenu príslušného nástroja (či bude klesať alebo stúpať). Súd uviedol, že informácia o pláne spoločnosti kúpiť významný podiel v inej spoločnosti *„môže byť totiž uvážlivým investorom použitá ako súčasť základne jeho investičných rozhodnutí.“*[501] Tento prístup prekonal doteraz platný názor Európskeho orgánu pre trhy cenných papierov, podľa ktorého „*informácia samotná nemusela síce indikovať, v akom rozsahu bude mať vplyv na kurz finančného nástroja, aby však bola presná, musela z nej byť zrejmá aspoň indikácie možného smeru vývoja tohto kurzu.“*[502] Toto rozhodnutie je v súlade s názorom Kotáska, *„či je vôbec nutné klásť na vnútorné informácie požiadavku "presnosti" (keď presné informácie bude [sám] trh schopný vyhodnotiť ako informácie s kurzotvornou relevanciou).“*[503] Pootvorenie dverí pre širší výklad nároku na presnosť umožňuje vidieť informáciu o kyberútoku ako vnútornú informáciu poškodeného emitenta. Aj keď ten v čase útoku nevie zhodnotiť skutočnú škodu a ušlý zisk spôsobený týmto útokom, musí sa riadiť tým, že daná informácia môže byť uvážlivým investorom použitá ako súčasť základne jeho investičných rozhodnutí. Napríklad informácia o kyberútoku na spoločnosť Sony spôsobila prepad jej akcii na japonskom trhu o 10%.[504] K podobnému názoru dospeli Arcuri, Brogi a Gandolfi, ktorí skúmali verejne dostupné dáta o kyberútokoch medzi rokmi 1995 až 2012.[505] Tu však treba spomenúť aj opačný názor. Kvochko a Pant poukazujú na to, že kyberútok ma tendenciu byť zamlčaný, resp. komunikovaný s dlhým časovým odstupom, a preto nemá žiaden kurzotvorný (cenotvorný) potenciál ako taký.[506]

[501] Rozsudok SDEÚ vo veci C‑628/13 zo dňa 11.3.2015, Jean-Bernard Lafonta proti Autorité des marchés financiers, Ods. 33.

[502] ŠOVAR, Ján. Soudní dvůr Evropské unie k insider tradingu: Jak moc nepřesná informace je ještě přesná? .[Online]. [cit.1.9.2020]. Dostupné z: https://www.patria.cz/pravo/2949748/soudni-dvur-evropske-unie-k-insider-tradingu-jak-moc-nepresna-informace-je-jeste-presna.html

[503] Ibid. KOTÁSEK, Str. 80.

[504] PAUL, Monica. Sony hack sends stock down 10% in past week. .[Online]. [cit.1.9.2020]. Dostupné z: http://money.cnn.com/2014/12/15/investing/sony-stock-hack/

[505] ARCURI, Brogi a GANDOLFI. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? [Online]. [cit.1.9.2020]. Dostupné z: http://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2014-Rome/papers/EFMA2014_0408_fullpaper.pdf

[506] KVOCHKO, Elena. PANT, Rajiv. Why Data Breaches Don’t Hurt Stock Prices. Harvard Business Review .[Online]. [cit.1.9.2020]. Dostupné z: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Zastávame názor prvej skupiny. Je len otázkou času a technologického pokroku, kedy investori dokážu jednoduchým spôsobom zmerať rozsah a výšku škody kyberútoku a bezprostredne na to reagovať. Navyše, nič nie je horšie pre investora technologickej spoločnosti, ako keď sa až s odstupom času dozvie, že jeho investícia bola terčom kyberútoku. Podobne sa ďalšie odborné výskumy odohrávajú aj v oblasti zaisťovníctva a poisťovacích služieb, ktoré udávajú smer poistnej matematiky a hľadajú spôsob ako kvantifikovať kybernetické riziká.[507]

7.6. Notifikačná povinnosť

V prípade kyberútoku je možné uvažovať o existujúcich notifikačných povinnostiach: oznam o porušení ochrany osobných údajov,[508] oznámenie trestného činu alebo reportovanie o IT incidente regulátorovi.[509] Podnikanie na kapitálovom trhu rozlišuje dva druhy notifikácií emitentov: pravidelné notifikačné povinnosti a priebežné (*ad hoc*) notifikačné povinnosti emitenta. Pravidelne zverejňované informácie (napr. výročné správy) sa v dnešnom digitálnom svete veľmi rýchlo stávajú obsolentnými. Stávajú sa z nich skôr formálne potvrdenia o predvídanej skutočnosti. Je zrejmé, že investori by neboli schopní urobiť svoje rozhodnutia len na základe týchto správ. Priebežne zverejňované informácie sú práve korektívom toho, čo sa stalo medzi pravidelnými hláseniami a zároveň šikovným nástroj na „zneškodnenie“ vnútorných informácií. V zmysle MAR informuje emitent čo najskôr (bez odkladu) verejnosť o vnútorných informáciách, ktoré sa ho priamo týkajú. Emitent zabezpečí tiež sprístupnenie vnútorných informácií verejnosti, ktoré umožní rýchly prístup a úplné, správne a včasné posúdenie informácií zo strany verejnosti. Emitent nesmie spájať sprístupnenie vnútorných informácií verejnosti s trhovým zviditeľňovaním svojich činností. Navyše, emitent má povinnosť uverejniť a uchovať na svojej webovej stránke najmenej päť rokov všetky vnútorné informácie, ktoré je povinný sprístupniť

[507] Swiss Re Corporate Solutions joins forces with IBM to offer cyber risk protection. [Online]. [cit.1.9.2020]. Dostupné z: http://www.swissre.com/corporate_solutions/Swiss_Re_Corporate_Solutions_joins_forces_with_IBM_to_offer_cyber_risk_protection.html

[508] Čl. 33 (Oznámenie porušenia ochrany osobných údajov dozornému orgánu) a čl. 34 (Oznámenie porušenia ochrany osobných údajov dotknutej osobe) GDPR.

[509] Napr. ESAs: Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT). [Online]. [cit.1.9.2020]. Dostupné z: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

verejnosti. Vnútorné informácie uverejňované emitentom by sa mali šíriť tak, aby k nim bol zaistený neuprednostňujúci, ľahký a bezodplatný prístup. To znamená, že rovnaká informácia by mala byť zároveň zaslaná (v elektronickej podobe) Českej Národnej Banke, príp. organizátorom regulovaných trhov, na ktorých sú finančné nástroje emitenta prijaté na obchodovanie, a zároveň uverejnená v obvyklom formáte, t.j. tak, aby všetkým investorom boli poskytnuté informácie obsahovo zhodné a v rovnakom čase. Nesplnenie notifikačnej povinnosti je prísne sankcionované dozorným orgánom.[510]

Americká SEC už v roku 2011 prijala (nezáväzné) odporúčanie o tom, ako by mal postupovať emitent v prípade informácie o kyberútoku.[511] Kyberútok už dávno nie je len záležitosťou IT oddelenia, ale stal sa vecou záujmu akcionárov, investorov a širšej verejnosti. Zaujímavosťou je, že notifikačná povinnosť sa v USA nevzťahuje len na samostatný útok, ale pokrýva aj hrozbu útoku a vytvára rámec pre *cybersecurity governance*: [512]

„Registrujúci by mali zverejniť riziko kybernetických incidentov, ak tieto otázky patria medzi najvýznamnejšie faktory, ktoré tvoria špekulatívnu alebo riskantnú investícu […] Pri určovaní toho, či sa vyžaduje zverejnenie rizikových faktorov, očakávame, že registrujúci zhodnotia svoje riziká týkajúce sa kybernetickej bezpečnosti a zohľadnia všetky dostupné relevantné informácie vrátane predchádzajúcich kybernetických incidentov a závažnosti a frekvencie týchto incidentov.“

Emitent (*registrant*) v USA musí pred zverejnením informácie o kyberútoku posúdiť riziká zistených dôkazných prostriedkov, t.j. dospeť k pravdepodobnosti takého incidentu. Musí zohľadniť kvantitatívne a kvalitatívne hľadisko hroziaceho rizika, ďalšie potencionálne náklady na jeho odstránenie a iné aspekty súvisiace so zneužitím vnútorných informácií. Tieto povinnosti logicky tlačia povinné osoby k tomu, aby prijali najvyššie možné preventívne opatrenia voči kyberútokom. Emitent má taktiež povinnosť identifikovať, ktoré oblasti jeho podnikania sú rizikové z pohľadu

[510] Čl. 30 MAR.

[511] Ibid. SEC, CF Disclosure Guidance.

[512] Podobne ako tomu je pri inštitúte *e-discovery hold* v prípade hroziaceho súdneho sporu, kedy strana, ktorá môže byť zažalovaná, má povinnosť uchovávať všetky elektronické informácie pre budúci spor.

možného kyberútoku. Adekvátne opatrenia sú posudzované samotným SECom. Už len zanedbanie prijatia takéhoto opatrenia môže podliehať enormným sankciám. V čase ohrozenia alebo odhalenia nestačí kyberútok nahlásiť, ale emitent musí preukázať taktiež všetky preventívne a reaktívne kroky.

Na záver sa je možné spýtať, čo v prípade, že by bol kyberútok odvrátený? Má emitent rovnakú informačnú povinnosť? Tu sa je možné inšpirovať znením GDPR v prípade notifikačnej povinnosti o porušení osobných údajov, kde sa oznámenie nevyžaduje, ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia.[513] V prípade kyberútoku by malo ísť o také následné opatrenia, ktorými sa zabezpečí, že riziko zneužitia informácie o kyberútoku už pravdepodobne nebude mať vplyv na kurz, cenu alebo výnos finančného nástroja v zmysle znenia MAR.

7.7. Časový aspekt

MAR hovorí o povinnosti bezodkladného uverejnenia *(„čo najskôr“). „Ide o primeraný časový úsek, v ktorom je emitent finančného nástroja schopný uverejniť vnútornú informáciu za daných okolností a pri svojom bežnom chode.“* [514] Za nezverejnenie zodpovedá priamo emitent. Domnievame sa, že emitent musí informovať o kyberútoku okamžite po tom, čo sa dozvedel o jeho technických znakoch, ktoré sú dostatočne zrozumiteľné pre uvážlivého investora a súčasne boli splnené všetky kritéria vnútornej informácie.

Uverejnenie informácie možno odložiť v prípade závažných dôvodov na strane emitenta. [515] Avšak musí byť splnená podmienka, že nesprístupnením informácie nebude verejnosť klamaná (pravdepodobne nebude zavádzaná) a emitent je schopný zabezpečiť dôvernosť týchto informácií. Zabezpečenie dôvernosti informácie o kyberútoku na strane emitenta je len zdanlivé riešenie. Ako bolo spomenuté vyššie, útočník, hoci v postavení zasvätenej osoby, je nekontrolovateľným elementom v šírení informácie, a preto túto povinnosť nemôže emitent takmer nikdy objektívne splniť.

[513] Čl. 34 GDPR.

[514] Ibid. ČNB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018, porovnaj nález ÚS ČR zo dňa 15. augusta 2005, sp. zn. IV. ÚS 314/05 a rozsudok NSS ČR zo dňa 2. apríla 2008, sp. zn. 3 As 2/2008 – 152.

[515] O odložení musí emitent informovať dozorný orgán, t.j. ČNB alebo NBS, a to vrátane uvedenia dôvodov pre odloženie a obsahu odkladanej informácie. Článok 17 ods. 3 MAR.

Domnievame sa, že odloženie informácie o zistenom kyberútoku je možné len v prípade, ak by došlo k zadržaniu všetkých útočníkov OČTK, súčasne by ešte nedošlo k rozšíreniu tejto informácie v relevantnom okruhu investorov a emitent bol o tejto skutočnosti riadne informovaný.

7.8. Praktické odporúčania pre hodnotenie rizík spojené s elektronickými dôkaznými prostriedkami o kyberútoku

Práve otázka presnosti informácie sa spája s tým, ako bude povinná osoba schopná vyhodnotiť kyberútok. Inšpiráciu tu je možné hľadať v obdobných postupoch ako pri elektronickom dokazovaní pred súdom. Povinná osoba bude mať vypracovaný vnútropodnikový plán o tom, ako naloží s IT incidentom a kto sú kľúčoví zamestnanci, ktorí budú schopní vyhodnotiť riziko a zakročiť. Fáza, v ktorej takýto tím zbiera informácie – zaisťuje digitálne stopy a vedie rozličné vnútorné vyšetrovanie so zamestnancami, pripomína prácu vyšetrovateľov. Rovnako fáza, kedy bezpečnostní experti posudzujú zaistené elektronické dôkazné prostriedky pripomína prácu súdnych znalcov. Nuž a vedenie spoločnosti sa v tejto metafore stavia do polohy súdu a rozhoduje o tom, ako vyhodnotí elektronické dôkazy, a kedy pôjde s pravdou von. Podobne ako pri elektronickom dokazovaní, každá osoba, ktorá je zapojená v takomto vnútornom šetrení, potrebuje poznať určité penzum ako vyhodnotí riziko predložených dôkazov na ďalší chod spoločnosti. Od nezvyčajného správania počítača až po antivírusové výstrahy, problémy sa musia eskalovať vopred naplánovaným kanálom k tímu, ktorý má správne znalosti a zručnosti pri odhaľovaní IT incidentov. Vo väčšej korporácii pôjde o reťaz postupov.

K praktickým odporúčaniam pre vnútropodnikové zbieranie dôkazov o kyberincidente je možné zaradiť nasledovné:

- Zriadenie *„horúcej linky,“* ktorá bude priamo napojená na expertný tím, v najlepšom prípade osobitnej skupiny určených zamestnancov z odvetvia IT bezpečnosti a rizikového manažmentu.
- V prípade vyhodnocovania získaných dôkazných prostriedkov sa odporúča konzultácia s právnikom, v anglo-amerických právnych systémoch sa dokonca celé hodnotenie presúva na spolupracujúcu advokátsku kanceláriu z dôvodu povinnosti mlčanlivosti advokáta a ochrany privilegovaného vzťahu klient – advokát (*client attorney privilige*).

- Ak členovia tímu v reťazi od nahlásenia incidentu až po zaistenie dôkazných prostriedkov, nie sú dostatočne oboznámení s potrebami expertného tímu a otázkami ako naložiť s podozrivými dátami, môže ich práca na riešení incidentov zmariť alebo znehodnotiť dôkaznú situáciu (napr. inštalácia nového softwaru alebo oprava napadnutej časti môže prepísať dáta, ktoré môžu byť neoceniteľné pre vyťaženie dôkazu o kyberútoku).
- Spoločnosti, ktoré využívajú IT subdodávateľov (napr. IT outsourcing v podobe poskytovateľov informačných a cloudových služieb), by sa mali ubezpečiť, že ich pracovníci technickej podpory sú oboznámení s okolnosťami, ktoré si vyžadujú zapojenie expertného tímu.
- Každý krok, od nahlásenia incidentu zamestnancom až po konečné rozhodnutie a oficiálne notifikácie, musí byť zdokumentovaný v elektronickej podobe. Je totiž časté, že vyšetrovania *post mortem* v sebe zahŕňa aj skúmanie krokov expertných tímov. Ak je taký tím schopný svoju prácu transparentne dokumentovať, jeho kroky budú ľahko oddeliteľné od tých, ktoré mohli viesť ku kyberútoku.
- Spoločnosť by mala mať vypracovaný rámec hodnotenia rizík kyberútokov, od čoho sa bude odvíjať aj jej hodnotenie zaistených dôkazných prostriedkov a ich rizík pre budúce konanie.[516]
- Spoločnosť by mala mať vypracovanú smernicu o riadení IT rizík (*IT Governance*) a bezpečnosti informačných systémov, záväznú pre každého zamestnanca.
- Spoločnosť by mala mať vypracovaný vzor zmluvného dodatku pre svojich dodávateľov informačných služieb, v ktorom sa dodávatelia zaväzujú ju informovať o IT incidentoch súvisiacich so spoločnosťou a jej dátami, a to podľa presne dohodnutého postupu a v konkrétnom čase.

[516] Príkladom môže byť smernica švajčiarskeho finančného regulátora o nakladaní s kyberútokmi a jej príloha troch stupňov rizík kyberútokov: FINMA Guidance 05/2020 - Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA. Annex 1: Determining the severity of a cyber attack. [Online]. [cit.1.9.2020]. Dostupné z: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf?la=en

7.9. Zhrnutie kapitoly

V čase pandemickej krízy COVID-19 sme svedkami prudkého nárastu kybernetických útokov alebo krádeži dát, ktoré vedú k trvalej ujme na reputácii, škode na majetku, strate ziskov alebo rovno ku bankrotu obchodných spoločností.[517] Tieto udalosti zvýšili citlivosť účastníkov kapitálového trhu a najmä regulátorov na akúkoľvek komunikovanú informáciu o informačnej bezpečnosti verejne obchodovateľnej alebo regulovanej spoločnosti. V predloženej kapitole sme sa pokúsili odpovedať na jednoduchú otázku v prípade kyberútoku, kedy a ako ísť s pravdou von.

Emitent v prípade vyšetrovania kyberútoku môže čerpať v mnohom z procesu elektronického dokazovania a hodnotenia rizík. V kapitole sme vysvetlili, prečo informácia o kyberútoku v niektorých prípadoch predstavuje vnútornú informáciu povinnej osoby. Zaoberali sme sa otázkami jej dostupnosti a presnosti, ktoré sú kritéria pre rozhodnutie povinnej osoby o jej zverejnení a notifikácii. Vysvetlili sme notifikačnú povinnosť a časový aspekt zverejnenia vnútornej informácie. Na základe vyššie uvedeného je možné dospieť k záveru, že emitent má povinnosť bezodkladne informovať o prebiehajúcom alebo dokonanom kyberútoku relevantnú verejnosť, ak sú splnené podmienky kladené na kvalitu vnútornej informácie. Takéto oznámenie by malo obsahovať jasne a jednoducho formulovaný opis povahy narušenia informačného systému emitenta a základné informácie o prijatých opatreniach.[518] Oznámenie musí byť dobre zdokumentované a podložené dôkazmi. Na záver sme ponúkli praktické odporúčania pre implementáciu procesu o vnútropodnikovom hodnotení dôkazných prostriedkov o kyberútoku.

[517] ESMA. Esma extends its operational-risk analysis. 13.4.2018. [Online]. [cit.1.9.2020]. Dostupné z: https://www.esma.europa.eu/press-news/esma-news/esma-extends-its-operational-risk-analysis

[518] Inšpiráciou tu môže byť použitie slovníka *Common Vulnerabilities and Exposures (CVE®)*. [Online]. [cit.1.9.2020]. Dostupné z: https://cve.mitre.org/about/

8. Zmenka ako elektronický dôkazný prostriedok

8.1. Hmotná forma ako dôkaz

Cenný papier je v obchodnej praxi definovaný ako *„listina alebo záznam v zákonom stanovenej evidencii, s ktorým je spojená existencia a právny osud určitého subjektívneho práva (právo stelesnené, inkorporované).“* [519] Pre cenný papier je charakteristická prítomnosť dvoch elementov: subjektívneho práva a fyzického nosiča, ktorý je s právom spojený. Pre potreby tejto kapitoly budeme analyzovať možnosti nahradenia papiera elektronickou formou, čo by mohlo uľahčiť dokazovanie v zmenkových sporoch a prinieslo takmer ideálny elektronický dôkazný prostriedok o zmenke a zmenkovom záväzku.

Ak sa obzrieme do histórie cenných papierov, išlo pôvodne o rôznorodé písomné prejavy vykonané na listine. Neskôr, v súlade s technickým pokrokom, došlo u niektorých typov cenných papierov k dematerializácii a nahradeniu jeho existencie evidenciou v registri cenných papierov (zaknihovaním). Avšak niektoré tradičné inštitúty, akým je napríklad zmenka alebo šek, ostali nedotknuté a zachovali si fyzickú podobu ako podmienku platnosti. Podstata obyčajného papiera spojeného so znakmi z atramentu, ktoré sú zrozumiteľné a kopírujú predvídané formulky záväzkov s vlastnoručnými podpismi výstavcov bola v obchodnej praxi tak rozšírená, že stala za zrodom jedného z najmocnejších ekonomických inštrumentov – prísľubu, že niekto niekomu zaplatí v blízkej budúcnosti v písanej podobe. Je zrejmé, že ústna forma pre rôznorodé zmluvy už nepostačovala, a to najmä v prípade komplikovanejších transakcií. Tie sa navyše stali predmetom mnohonásobných obchodov a oznamovanie o postúpení pohľadávky sa stalo nepraktické. Preto forma začala hrať významnú rolu za účelom preukázania toho, že k obchodu naozaj došlo. Hmotná forma predstavovala najvyššiu dôkaznú silu za použitia najjednoduchších nástrojov – pera a papiera (resp. akéhokoľvek technického prostriedku, ktorý vyjadrí a zachytí písmo v hmotnej podobe). Navyše, papier (alebo iný hmotný nosič) sa stal trvanlivým úložiskom pomyselných hodnôt, viery a nádejí, ktoré v ňom zúčastnení videli. Jeho trvanlivosť bola obmedzená kvalitou papiera a atramentu (alebo iného materiálu, napr. kože).

[519] HENDRYCH, Dušan. Právnický slovník. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009. Beckovy odborné slovníky. ISBN 978-80-7400-059-1. Str. 62.

Spoločná dohoda obchodníkov o tom, že kúsok hmotného sveta bude vyjadrovať nejakú hodnotu a bude niečo dokazovať (napr. zmenkovú obligácia) mala takmer magický rozmer. Namiesto „zlatých dukátov“ sa platilo alebo zaisťovalo popísaným papierom. Kúzlo sa však mohlo veľmi rýchlo stratiť, a to vplyvom rôznorodých skutočností. Počnúc neschopnosťou dokázať to, čo bolo na listine uvedené, až po nevôľu osôb na papieri zaviazaných. Postupom času sa s príchodom nových technológií forma dokazovania presúvala do elektronickej podoby. Elektronické bankové účty, zaknihované cenné papiere alebo elektronické platobné prostriedky sa stali nositeľmi hodnôt a inkorporovali v sebe práva komplexnejšie ako to vedeli hmotné veci, avšak tentokrát opäť za použitia dostupných, ale o to zložitejších nástrojov – počítačov. Otázkou je, prečo niektoré tradičné inštitúty ostali stranou? V nadväznosti na vyššie uvedené sa pokúsime odpovedať otázku, či zmenka v elektronickej podobe môže priniesť vyššiu dôkaznú spoľahlivosť v súčasnom právnom prostredí?

8.2. Dôkazná spoľahlivosť zmenkovej listiny

Aj keď zlatým vekom zmeniek bolo obdobie 1850 až 1940, listinné zmenky sú stále často používané v obchodnej praxi, a to najmä ako zaisťovacie mechanizmy.[520] Zmenka je cenný papier, na základe ktorého jedna strana (aj viacerí dlžníci) zaplatí druhej strane v určitom čase a mieste zmenkovú sumu. Ide o cenný papier vydaný podľa zákonom stanoveného spôsobu, ktorý obsahuje *„záväzky priame, nesporné, bezpodmienečné a abstraktné.“*[521] V zmysle § 514 NOZ je *„cenný papír listina, se kterou je právo spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést.“* Podstata listinného cenného papieru je v tom, že bez listiny (hmotného nosiča) nie je možné vykonať tam uvedené právo. Preto podľa súčasne platnej úpravy neprichádza vystavenie zmenky v elektronickej podobe alebo podpísanie zmenkového textu elektronickým podpisom do úvahy.

[520] Je vhodné spomenúť, že nápad vecí na české súdy v civilnej agende elektronického rozkazného konania po dvojročnom raste pomerne výrazne klesol (o viac ako 8%) v 2019. [online]. [cit.1.9.2020]. MS ČR: České soudnictví 2019: Výroční statistická zpráva. Str.38. Dostupné z: https://justice.cz/documents/12681/719244/Ceske_soudnictvi_2019_vyrocni_stat_zprava.pdf/28174b8b-c421-440b-9a17-1f48cfc50efc

[521] Ibid. HENDRYCH, Dušan. Právnický slovník. 3., Str. 993.

Používanie listín v právnom živote súvisí s potrebou dokázať určitú minulú právnu skutočnosť, resp. ide o garanciu dôkaznej spoľahlivosti.[522] V právnych vzťahoch vystupuje tento artefakt ako nositeľ dôkaznej informácie s určitou silou spoľahlivosti. Skúmanie dôkaznej spoľahlivosti v prípade zmenky je však nahradené abstraktným zmenkovým záväzkom a zákonom akceptovanou formou v podobe potvrdenia o dôveryhodnosti zdroja jej pôvodu, t.j. textu s vlastnoručným atramentovým podpisom na hmotnom predmete. Navyše, majiteľ zmenky má špeciálne postavenie v celej dôkaznej situácii. Predložením tohto artefaktu sa majiteľ osvedčuje a presvedčuje povinnú stranu o pravdivosti a vierohodnosti svojej zmenkovej listiny.

Môžeme sa pýtať, aké skutočnosti táto listina dokazuje? Typickým príkladom môže byť najpoužívanejšia vlastná zmenka, ktorá obsahuje nasledujúce údaje v listinnej podobe podľa § 75 ZSŠ:

> *Vlastní směnka obsahuje:*
> *1. označení, že jde o směnku, pojaté do vlastního textu listiny a vyjádřené v jazyku, ve kterém je tato listina sepsána;*
> *2. bezpodmínečný slib zaplatit určitou peněžitou sumu;*
> *3. údaj splatnosti;*
> *4. údaj místa, kde má být placeno;*
> *5. jméno toho, komu nebo na jehož řad má být placeno;*
> *6. datum a místo vystavení směnky;*
> *7. podpis výstavce.*

Každý z týchto údajov smeruje k identifikácii zmenkového dlžníka, veriteľa, peňažnej sumy a ďalších skutočností. Ako je zrejmé, ani v jednom prípade nejde o informáciu o kauze, resp. o tom, čo predchádzalo alebo čo zdôvodňovalo vystavenie zmenky. Zmenka nanajvýš prináša informáciu o zmenkovej sume a obligácii (zmluve o vystavení zmenky), ktorá môže existovať popri vlastnom (kauzálnom) vzťahu. Odráža sa tu abstraktná povaha zmenky v podobe platobného alebo zaisťovacieho inštitútu. Dôkazná sila je nahradená vyhlásením *pro futuro*, ktoré je zaznamenané na

[522] Právna skutočnosť je okolnosť, s ktorou právna norma spája vznik, zmenu alebo zánik právneho vzťahu, tj. subjektívnych práv a povinností. Možno ju všeobecne definovať ako skutočnosť, ktorá napr. na základe zákona pôsobí právne následky. Viď KNAPP, Viktor. Teorie práva. Praha : C. H. Beck, 1995. ISBN 80-7179-028-1. Str. 140. alebo BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. Teorie práva. 2., přeprac. vyd. Praha: ASPI, 2004. ISBN 80-7357-030-0. Str. 126.

hmotnom nosiči. Aj keď v niektorých prípadoch je možné v zmenkovom konaní skúmať kauzu vystavenia zmenky (námietky z vlastných vzťahov), samotná listina nám ju málo osvetlí.[523] No napriek tomu požíva pomerne silnú dôkaznú spoľahlivosť. Totiž ak pred súdom žalobca predloží v prvopise zmenku, o pravosti ktorej niet dôvodu pochybovať, a ďalšie listiny potrebné na uplatnenie práva, vydá súd na jeho návrh zmenkový platobný rozkaz.[524] V tomto kontexte je *„zmenka, o ktorej pravosti niet dôvodu pochybovať"* každá hmotná listina s presnými náležitosťami podľa ZSŠ. Je možné zhrnúť, že dôkazná spoľahlivosť v procese pri uplatnení takejto listiny je teda vopred určená zákonom. Tu sa naskytá otázka, prečo takúto dôkaznú silu nemôže požívať aj elektronická písomnosť, ktorá by mala všetky znaky platnej zmenky, resp. prečo zákonodarca s takouto alternatívou doposiaľ nepočítal?[525]

8.3. Elektronické zmenkovanie

Právna povaha zmenky je v súčasnosti určená tým, že ide v užšom zmysle slova o hmotnú vec podľa § 496 ods. 1 NOZ. Vystavenie zmenky je nutné vykonať na ovládateľnej časti vonkajšieho sveta, ktorá má povahu samostatného predmetu – napr. listiny. Navyše, NOZ považuje cenný papier za vec v právnom zmysle oproti bývalej úprave, kde išlo o inú majetkovú hodnotu.[526] Zmenka je tak dokonalý cenný papier – skriptúra. Aj keď eIDAS považuje kvalifikovaný elektronický podpis za rovnocenný s

[523] KOTÁSEK, Josef. Zákon směnečný a šekový: komentář. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-965-4. Str. 141.

[524] Podľa § 175 ods. 1 OSŘ: *„Předloží-li žalobce v prvopisu směnku nebo šek, o jejichž pravosti není důvodu pochybovat, a další listiny nutné k uplatnění práva, vydá na jeho návrh soud směnečný (šekový) platební rozkaz, v němž žalovanému uloží, aby do 15 dnů zaplatil požadovanou částku a náklady řízení nebo aby v téže lhůtě podal námitky, v nichž musí uvést vše, co proti platebnímu rozkazu namítá. Směnečný (šekový) platební rozkaz musí být doručen do vlastních rukou žalovaného, náhradní doručení je vyloučeno. Nelze-li návrhu na vydání platebního rozkazu vyhovět, nařídí soud jednání."*

[525] Je potrebné rozlišovať pojem písomnosť od pojmu listina. Písomnosť je prejav vôle písmom, t.j. bez ohľadu na formu (text, trvalosť, formálna určitosť) a listina je písomnosť zachytená na papierovom nosiči (papierový dokument, dokument v listinnej podobe). Podľa § 562 ods. 1 NOZ je *„písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby."*

[526] O povahe cenného papieru v bývalej civilnej úprave rozhodol NS ČR nasledovne: *„Akcie, stejně jako jiný cenný papír, není věcí ve smyslu ustanovení § 119 obč. zák.; lze ji charakterizovat jako specificko-majetkovou hodnotu, jejímž charakteristickým rysem je spojení práva s listinou (právo je v ní inkorporováno), která může být v zákonem stanovených případech nahrazena zápisem do zákonem stanovené evidence. Akcie pojmově má majetkovou hodnotu."* Usnesení NS ČR ze dne 9. 6. 2000, sp. zn. 21 Cdo 2587/99.

vlastnoručným podpisom,[527] zmenka vo svojej úplnosti je cenným papierom z hľadiska materiálneho, ale aj z dôvodov formálne právnych.[528] Avšak samotný zmenkový vzťah (zmenková obligácia - zmenka v širšom zmysle slova) predstavuje zmluvu so všetkými náležitosťami právnych konaní v zmysle § 545 an. NOZ. Pre určenie toho, aké práva a povinnosti budú zo zmenky plynúť, bude rozhodujúca jej forma, akú účastníci zmenkových vzťahov pre svoje vyhlásenia použili. Ako bolo uvedené, NOZ zaviedol definíciu cenného papiera, pričom sa inšpiroval švajčiarskou úpravou, keď v § 514 NOZ stanovil, že *„cenný papír je listina, se kterou je právo spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést.“*[529]Cenným papierom sú teda len hmotné listiny. Jeden z argumentov, prečo by takáto listina nemohla byť v elektronickej podobe je to, že z pohľadu platnej právnej úpravy zákon o elektronických úkonoch a autorizovanej konverzii dokumentov explicitne vylučuje konverziu zmeniek (ich prevod do elektronickej podoby).[530] Avšak to neznamená, že zmenka by nemohla byť vystavená elektronicky od počiatku, tak ako to je pri zaknihovaných akciách alebo elektronickej zmluve. Zaknihované cenné papiere pritom tvoria samostatnú kategóriu nehmotných vecí.

V anglo-americkej právnej literatúre zameranej na úvahy o elektronických zmenkách je možné nájsť viaceré názory zastávajúce možnosť zavedenia elektronickej

[527] Čl. 25 ods. 1 eIDAS: *„Právny účinok elektronického podpisu a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že má elektronickú formu alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy.“ a ods. 2: „Kvalifikovaný elektronický podpis má právny účinok rovnocenný s vlastnoručným podpisom.“ Avšak v zmysle čl. 2 ods. 3 v podstate eIDAS nemá vplyv na formu záväzku uznanú vnútroštátnym právom: „Toto nariadenie nemá vplyv na vnútroštátne právo ani právo Únie súvisiace s uzatváraním a platnosťou zmlúv alebo iných právnych či procesných záväzkov týkajúcich sa formy.“*

[528] KOVAŘÍK, Zdeněk. Zákon směnečný a šekový: komentář. 5., dopl. vyd. V Praze: C.H. Beck, 2011. Beckovy malé komentáře. ISBN 978-80-7400-385-1. Str. 2.

[529] § 965 A.*:“Wertpapier ist jede Urkunde, mit der ein Recht derart verknüpft ist, dass es ohne die Urkunde weder geltend gemacht noch auf andere übertragen werden kann.“*. Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (Stand am 1. Juli 2020). [online]. [cit.1.9.2020]. Dostupné z: https://www.admin.ch/opc/de/classified-compilation/19070042/index.html

[530] Viď § 24 ods. 4 písm. b) zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů.

zmenky do právnej praxe.[531] Zaujímavosťou je, že austrálska legislatívna pracovná skupina navrhovala novelizovať zákon o zmenkách (*Bills of Exchange Act 1909*) v nadväznosti na otázku dematerializácie zmeniek. Táto skupina riešila otázku obyčajného listinného podpisu voči elektronickému podpisu, kde táto rovnocennosť bola spochybnená vo svetle nárokov na formálnosť zmenky:[532]

„Aj keď je preukázateľné, že počítačový systém by mohol zabezpečiť individuálnu identifikáciu dostatočnú na to, aby vyhovoval súdnym rozhodnutiam ako je Moreton v Copeland, a síce, že podpis je „akákoľvek ochranná značka, ktorá ho identifikuje ako konanie strany", je pochybné, že identifikácia „dokumentu" takým spôsobom by sa považovala za podpis na účely zákona o zmenkách v jeho súčasnej podobe."

Asi najzásadnejšia otázka bola riešená z pohľadu práv držiteľa (majiteľa) listinnej zmenky a jeho práva disponovania s týmto predmetom, no najmä ako je možné túto skutočnosť naviazať na elektronickú formu. V prvom rade predstavuje zmenka obchodovateľný a prevoditeľný inštrument, ktorého povaha definovala jednoduchosť použitých nástrojov (bez nutnosti oznamovania zmeny veriteľov alebo zaviazaných dlžníkov):[533]

„Táto vlastnosť obchodovateľného nástroja, že je prevoditeľný tak, aby držiteľovi dal „zaručený titul" základnému záväzku, je dôvodom, prečo je obchodovateľný a nie iba prevoditeľný. […] Kvôli týmto obmedzeniam si obchodníci vyvinuli zmenku s atribútmi ľahkého prevodu medzi obchodnými stranami (t.j. jednoduchým prevodom

[531] GAMERTSFELDER. Leif. Electronic Bills of Exchange. Will the Current Law Recognise Them? University of New South Wales Law Journal 1998, Str. 566. [online]. [cit.1.9.2020]. Dostupné z: http://www.austlii.edu.au/au/journals/UNSWLJ/1998/50.html alebo PUIG, Gonzalo Villalta. Electronic Bills of Exchange and Promissory Notes in Australia. Murdoch University Electronic Journal of Law. 3/2000. [online]. [cit.1.9.2020]. Dostupné z: http://www.murdoch.edu.au/elaw/issues/v7n3/puig73b.html. TSAKATOURA, Anastasia. E-finance — bills of exchange, promissory notes, documentory credits, forfaiting. [online]. [cit.1.9.2020]. Dostupné z: http://www.inter-lawyer.com/lex-e-scripta/articles/e-finance1.htm alebo International Chamber of Commerce: The Legal Status of Electronic Bills of Lading. A report for the ICC Banking Commission. 2018. [online]. [cit. 1.9.2020]. Dostupné z: https://cdn.iccwbo.org/content/uploads/sites/3/2018/10/the-legal-status-of-e-bills-of-lading-oct2018.pdf (Viď zoznam článkov uverejnený na Iuridictum – Encyklopedie o právu: Směnka. [online]. [cit.1.9.2020]. Dostupné z: http://iuridictum.pecina.cz/w/Směnka).

[532] Commonwealth of Australia. National Competition Policy Review of the Bills of Exchange Act 1909. July 2003 [online]. [cit.1.9.2020]. Dostupné z: http://ncp.ncc.gov.au/docs/AG%20review%20of%20the%20Bills%20of%20Exchange%20Act%2C%20July%202003.pdf

[533] Ibid. Commonwealth of Australia. Str. 54.

alebo prevodom s indosamentom a bez predchádzajúceho oznámenia dlžníkom), spolu s prevodom vlastníckeho práva bez vád predchádzajúcich strán.“

V prípade elektronickej zmenky ide o ťažiskovú otázku prevodu a držby tohto inštrumentu. V zmenkových vzťahoch sa stáva, že držiteľ zmenky nemá žiaden vzťah k zmenkovo zaviazaným osobám, no napriek tomu predložením zmenky alebo jej vyplnením, indosovaním, sa stane oprávnenou osobou. Austrálska analýza tento problém riešila využitím obdobnej technológie, ako to je v prípade elektronického obchodovania:[534]

„S príchodom elektronických prostriedkov obchodovania sa môže stať, že prvý z týchto atribútov (t.j. prevod) už nie je vhodný, a že očakávania účastníkov trhu by lepšie uspokojilo posúdenie spôsobu prevodu obchodovateľných nástrojov s cieľom zohľadniť elektronické transakcie uskutočňované na trhu. Formálne požiadavky zákona o zmenkách a súvisiace pojmy „dodanie“ a „držba“ na druhej strane majú potenciál brániť rozvoju elektronických techník na prevod, obchodovanie a prevod vlastníctva zmenky a zmenky. Je to tak najmä vtedy, ak sa tieto prvky považujú za zásadné pre povahu zmeniek ako obchodovateľných nástrojov a pre prevod práv a povinností strán v nej obsiahnutých. Pokiaľ sa tieto prekážky nedajú prekonať, môžu brániť obchodovaniu zmeniek v elektronickej podobe.“

Kľúčovou časťou bolo, či faktické inštitúty ako fyzická držba zmenky, jej indosovanie, prezentovanie, protestovanie a iné faktické úkony, môžu byť implementované do takej elektronickej podoby, aby nenarušili súčasnú právnu úpravu a zároveň neznížili garanciu terajších práv regulovaných subjektov. Doposiaľ neboli elektronické zmenky v austrálskom právnom priestore zavedené, no výstupom analýzy bolo, že pre takýto proces je nutné začať novelou zmenkového zákona a zákona o korporáciách (*Corporation Act 2001*).[535]

[534] Ibid. Commonwealth of Australia. Str. 55.

[535] BATH, Robin Burnett and Vivienne. Law of international business in Australasia. Annandale, N.S.W: Federation Press, 2009. ISBN 9781862877245. Str. 216.

8.4. Úvahy *de lega ferenda*

Pohľad do zahraničných analýz načrtol možnosť úpravy inštitútu elektronickej zmenky. Na základe tejto inšpirácie je možné predložiť nasledovné odporúčania pre úvahu nad implementáciou elektronickej zmenky. Je za týmto účelom potrebné:

- definovať postavenie holografického listinného podpisu voči elektronickému podpisu,[536]
- prísne rozlišovať pojmy listinná (materializovaná) a elektronická (dematerializovaná) forma, kde obe môžu mať zachovanú písomnú podobu,[537]
- novelizovať ZZŠ, ktorý bude počítať s možnosťou vystavenia elektronickej formy zmenky a šeku za pomoci použitia zaručeného elektronického podpisu, časového razítka a registrácie tohto elektronického dokumentu za použitia vyspelých šifrovacích mechanizmov,[538]
- zaviesť inštitút centrálneho registra elektronických zmeniek a šekov, ktorý bude predstavovať autoritu pri verifikácii elektronických zmenkových listín a ich podpisov (centrálna evidencia zamedzí zneužitiu elektronických zmeniek, falšovaniu podpisov, vystavovaniu prebytočných duplikátov) alebo podporiť vývoj decentralizovanej technológie v podobe *private blockchain*, ktorá by mohla nahradiť centrálny register,
- upraviť niektoré hmotnoprávne inštitúty z pohľadu elektronických úkonov (faktické inštitúty ako fyzická držba zmenky, jej indosovanie, prezentovanie, protestovanie) tak, aby sa docielila rovnosť práv listinnej a elektronickej formy, a

---

[536] Podľa § 561 ods. 1 NOZ *„K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat.“ A podľa § 562 NOZ „Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.“* Taktiež viď KOUKAL, Pavel a Eva ZAHOŘOVÁ. Epravo.cz: Listinná a elektronická podoba písomného právního úkonu [online]. 2012 [cit.1.9.2020]. Dostupné z: http://www.epravo.cz/top/clanky/listinna-a-elektronicka-podoba-pisemneho-pravniho-ukonu-84178.html

[537] Avšak je potrebné vyhnúť sa nelogickým spojeniam typu *„elektronická listina“*. Viď POLČÁK, Radim. Elektronické právní jednání - změny, problémy a nové možnosti v zákoně č. 89/2012 SB. Bulletin Advokacie: www.cak.cz [online]. 2013. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-pravni-jednani-zmeny-problemy-a-nove-moznosti-v-zakone-c.-892012-sb

[538] Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů.

- novelizovať zákon o elektronických úkonoch a autorizovanej konverzii dokumentov a súvisiacu legislatívu, ktorá vylučuje zmenky alebo cenné papiere (napr. zákon o overovaní).[539]

Ďalej je možné uvažovať o výhodách a nevýhodách implementácie tejto technológie. Medzi zásadné pozitíva elektronickej zmenky bude patriť:

- vyššia dôkazná spoľahlivosť zmenky ako elektronického dôkazného prostriedku za použitia informačných technológií,
- vyššia pravdivosť a vierohodnosť v prípade sporov v zmenkových vzťahoch a obmedzenie falšovania, resp. pozmeňovania cenných papierov,
- vyššia obsahová správnosť vystavovania elektronickej zmenky oproti klasickej zmenke, a
- vyššia technologická bezpečnosť, či už na strane povinného alebo oprávneného.

Avšak každá nová technológia prináša určité riziká, resp. negatíva. Medzi tie najzásadnejšie patria:

- rôznorodé kyber-riziká spojené s prelomením šifrovania alebo zneužitím prihlasovacích údajov (kľúčov) pre elektronické podpisovanie, resp. registrovanie elektronických zmeniek,
- kauzálna nepreviazanosť s dematerializovaným vyhlásením zvyšuje riziko zneužitia elektronickej zmenky pri formálnej chybovosti informačného systému,
- časová obmedzenosť zmenky z dôvodu limitovanej platnosti elektronického podpisu a technológie šifrovania, a
- nutnosť centrálnej autority a medzinárodnej unifikácie zmenkového práva umožňujúceho elektronické zmenkovanie.

[539] Zákon č. 21/2006 Sb. o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování).

S poukazom na vyššie uvedené, je možné uvažovať o legislatívnych prácach smerujúcich k zavedeniu elektronickej zmenky do platnej právnej úpravy za dodržania určitých technologických podmienok. Tu však je potrebné zdôrazniť, že samotná technológia nezmení povahu zmenkových vzťahov, ale dodá novú kvalitu a formu jednotlivým právnym úkonom (konaniam), a to najmä v otázkach dokazovania.

8.5. Zhrnutie kapitoly

V kapitole boli predložené niektoré úvahy na tému súvisiacu s implementáciou elektronickej zmenky. Pokúsili sme sa zodpovedať otázku, či by zmenka v elektronickej podobe priniesla vyššiu dôkaznú spoľahlivosť v súčasnom právnom prostredí? Snahou bolo načrtnúť reálne fungovanie dematerializovaného cenného papieru – elektronickej zmenky, ktorý dlhé roky odoláva virtualizovaniu. Úvahy v tejto súvislosti smerovali k výhodám, ale aj nevýhodám elektronickej zmenky. Na príklade austrálskej právnej analýzy bola demonštrovaná možnosť zavedenia elektronickej zmenky do právnej praxe. Keďže zmenkový a šekový zákon patrí medzi naše najstaršie právne normy, je ťažké si predstaviť jeho bezproblémovú a nekonfliktnú novelizáciu. Najmä s prihliadnutím k terminológii, ktorú tento zákon doposiaľ používa. Ženevské konvencie na začiatku storočia ustálili mechanizmus fungovania zmeniek v európskom priestore a s určitým nadnesením je možné konštatovať, že zamrazili zmenkové právo na niekoľko ďalších desaťročí. Istotne ide o jednu z najkvalitnejších textácii právnych noriem, ktorá dokázala ustáť množstvo rokov bez novelizácie. Avšak to neznamená, že jej obsah by sa nemal prispôsobovať vývoju spoločenských potrieb. Anglo-americká tradícia zmenkového práva je v tomto smere flexibilnejšia a pokúša sa adaptovať novým moderným technológiám. Tu však paradoxne k slovu neprichádza sudcovské právo (precedensy), ale východiská sa hľadajú v parlamentnej legislatíve. Tieto aktivity môžu slúžiť ako inšpirácia pre kontinentálny právny systém poznačený silnou tradíciou zmenkového práva, ktorá sa zdá byť miestami prehnane konzervatívna a pripútaná na historické východiská pochádzajúce z dôb severotalianskych miest 12. storočia.

„Stroj neizoluje človeka od veľkých problémov, ale vrhá ho hlbšie do epicentra týchto udalostí.“ Antoine de Saint Exupéry

9. Záver

Môžeme konštatovať, že v súčasnosti existuje platný a právom akceptovateľný spôsob vykonania elektronického dôkazného prostriedku v občianskom ako aj trestnom konaní v ČR a SR. Návrhy na novú legislatívnu úpravu nie sú nevyhnutné. Limity sú však skôr dané personálnou a inštitucionálnou nepripravenosťou na elektronické dokazovanie. Elektronické dôkazné prostriedky sú síce technologicky náročné a často prinášajú nové otázky pre právnu prax, ale ako s nimi naložíme záleží len na našich vedomostiach o technológii a podstate tohto inštitútu. Pre niekoho sú novinkou a intelektuálnou výzvou v procesnom práve, pre iného len *„staronovým telegramom v morseovom kóde.“* Aplikácia existujúcich právnych noriem procesného práva pri vykonávaní elektronických dôkazných prostriedkov v sebe nesie určité riziká. Ak však pochopíme podstatu týchto rizík, minimalizujeme ich nepriaznivý účinok na naše rozhodovanie.

V tejto práci sme si dali za cieľ obhájiť platnosť a význam zásady voľného hodnotenia dôkazov získaných z elektronických dôkazných prostriedkov. Aby sme túto ťažiskovú zásadu dôkazného práva vo svetle nových technológií obhájili, v úvode práce sme si položili päť základných výskumných otázok. Na podklade tejto práce, ktorá predstavuje prierez cez rôzne odvetvia práva, môžeme zhrnúť nasledujúce odpovede:

1. **Môže virtualizácia slúžiť ako vhodné východisko pri riešení aktuálnych spoločenských problémov v otázkach elektronického dokazovania?**

Na túto otázku sme sa snažili odpovedať kladne v prvej kapitole. Predstavili sme koncept virtualizácie z filozofického, ale aj praktického hľadiska. Aby sme pochopili virtualizovanie elektronických dôkazných prostriedkov a procesu dokazovania, osvetlili sme prečo môže byť vizualizácia vítanou metódou riešenia spoločenského problému alebo konfliktu vo všeobecnosti. Pokúsili sme sa ozrejmiť, že virtualizácia je pohyb od aktuálneho k virtuálnemu, čo nastolilo viaceré axiologické otázky. Aj keď sa zdá, že technológia dolieha na zmenu fundamentu práva, demonštrovali sme na viacerých prípadoch, že tomu tak nie je. Virtualizácia ponúka radu zaujímavých

možností ako nastaviť niektoré nové procesy riešenia problémov vrátane elektronického dokazovania. Jedným z uvedených príkladov môže byť pozitívny dopad aspektov virtualizácie procesu autoritatívnej aplikácie práva v podobe systému riešenia on-line sporov.

2. Aké sú fundamenty a limity elektronického dôkazného prostriedku?

V druhej kapitole sme priniesli úvahu o podstate elektronického dôkazného prostriedku v občianskom sporovom konaní. Predložili sme základné definície a komparatívne úvahy s anglo-americkým právnym systémom. Pokúsili sme sa analyzovať najčastejšie limity elektronických dôkazných prostriedkov. Aby sme ich pochopili, opísali sme kybernetickú informačnú teóriu a jej vplyv na takýto prostriedok.

V predloženej práci sme dospeli k názoru, že správne určenie kategórie kvality elektronického dôkazného prostriedku je kľúčové. Hodnotili sme ju pomocou štyroch popisných párov. Potencionálna ubiquita a volatilita. Dôkazná spoľahlivosť a integrita. Pravdivosť a vierohodnosť. Platnosť a zákonnosť. Každá z týchto kvalít má určité špecifiká, ktoré zásadne ovplyvňujú nie len samotný dôkazný prostriedok, ale aj hodnotenie založené na vykonaní tohto prostriedku.

Kardinálnou otázkou bolo vysvetlenie úlohy zásady voľného hodnotenia dôkazov pri dokazovaní elektronickými dôkaznými prostriedkami. Pokúsili sme sa popísať všeobecnú teóriu tejto zásady a súvisiace rozhodnutia súdov. Zásadu sme však interpretovali aj z pohľadu teórie rizík. V našej práci vychádzame z toho, že rozhodovanie o elektronických dôkazných prostriedkoch môže byť videné aj ako rozhodovanie o rizikách, ktoré predstavuje použitie dôkazného prostriedku v elektronickej podobe. Dôkazný prostriedok totiž môže priniesť priaznivý alebo nepriaznivý účinok pre hľadanie práva. V prípade elektronických dôkazných prostriedkov pracuje súd s predmetom, ktorý musí byť interpretovaný odbornými technologickými vedomosťami. Bolo demonštrované, že súdy môžu pripisovať elektronickým dôkazným prostriedkom automaticky väčšiu váhu. Preto je namieste poznať aj ich riziká. Pokúsili sme sa predložiť rámec toho, ako identifikovať vnútorné a vonkajšie riziko elektronického dôkazného prostriedku v rámci zásady voľného hodnotenia dôkazov.

Ako nevyhnutnú súčasť úspešného elektronického dokazovania sme uviedli existenciu elektronického súdneho spisu. Pokúsili sme sa načrtnúť, že ťažiskom a Achillovou pätou je otázka konverzie elektronického dôkazného prostriedku do súdneho spisu.

Odpoveď na túto výskumnú otázku sme uzavreli exkurzom do anglo-americkej právnej doktríny *e-discovery,* ktorá v mnohom osvetľuje fundamentálne otázky elektronického dokazovania a je skvelou inšpiráciou o rôznych úvahách. Avšak dospeli sme k záveru, že ide o neprenositeľný a cudzí koncept pre kontinentálnu tradíciu procesného práva.

3. **Oslabuje kyberpriestor teritoriálnu výkonnú moc štátu voči jej virtualizovaným subjektom, a aký to má dopad na súdnu moc, resp. na elektronické dokazovanie?**

V tretej kapitole sme dospeli k záveru, že technológia kyberpriestoru oslabuje teritoriálnu výkonnú moc štátu voči virtualizovaným subjektom, čo má dopad aj na jej súdnu moc vrátane procesu elektronického dokazovania. Priblížili sme základy suverenity zo štátoprávneho hľadiska, jej formovanie v kyberpriestore a následný vplyv takejto informačnej suverenity na výkon súdnej moci. Pokúsili sme sa zodpovedať otázku vplyvu informačnej suverenity na dostupnosť elektronických dôkazných prostriedkov v kyberpriestore. V kapitole sme vysvetlili, prečo štát takéto oslabenie svojej informačnej suverenity kompenzuje buď snahou o oplotenie kyberpriestoru (napr. cenzúra internetu, regulácia definičných autorít) alebo snahou o pristúpenie k tzv. zdieľanej suverenite tak, ako to robí v prípade vonkajšej zvrchovanosti, kde prirodzene vyhľadáva spojencov a partnerov. Túto úvahu sme demonštrovali na otázkach ako je právo na sebaobranu alebo aplikácia práva v súdnom konaní, resp. pri dokazovaní v kyberpriestore. Svoje úvahy sme doplnili o pohľad na tradičné mechanizmy medzinárodnej spolupráce štátov vo veciach dokazovania v občianskom práve.

4. **Je možné uvažovať o rozhodovaní o dôkazoch sudcom-počítačom? Aké sú výhody a východiská?**

V súčasnosti ide o jednu z najčastejšie diskutovaných a možno najkontroverznejších otázok. Preto si štvrtá kapitola kladie za cieľ vyvolať právnu diskusiu o automatizovanom rozhodovaní a nesnaží sa podať vyčerpávajúci výklad.

Dospeli sme k záveru, že počítač môže dopĺňať a podporovať rozhodovaciu činnosť sudcu, najmä v otázke zaistenia elektronických dôkazných prostriedkov, avšak nemôže prevziať jeho samostatnú právomoc a kompetenciu. Domnievame sa, že stále stojíme pred mnohými technologickými obmedzeniami, ktorých zvládnutie je len otázkou času. Avšak možné nahradenie sudcu počítačom vyvoláva právne, technické, ale aj filozofické otázky. V kapitole sme sa pri riešení tejto otázky snažili porovnať dva koncepty, ako by rozmýšľal sudca-človek a sudca-počítač. Domnievame sa, že na problém sudca-počítač je možné nazerať z pohľadu praktického využitia existujúcej technológie. Tu je možné uviesť nenahraditeľnú výhodu počítača pri podpore rozhodovania, najmä v otázkach zaistenia a hodnotenia počítačových dát.

5. Ako nakladať so špecifickými druhmi elektronického dôkazného prostriedku?

Túto otázku sme zodpovedali v osobitnej časti venovanej štyrom druhom elektronických dôkazných prostriedkov.

Opísali sme, ako by mohol vyzerať proces dokazovania profilom sociálnej siete, webstránkou a IP adresou. Išlo prevažne o otázky zaistenia, forenznej analýzy, vykonania a hodnotenia dôkazu podľa trestného poriadku v ČR. Predložili sme analýzu judikatúry o identifikácií IP adresy. Dospeli sme k záveru, že záznam o IP adrese „páchateľa“ má okrem iného závisieť aj od ostatných priamych alebo nepriamych dôkazoch, v čom nadväzujeme na dôležitosť zásady voľného hodnotenia dôkazov.

Rovnako sme ponúkli pohľad na zaistenie elektronického dôkazného prostriedku v zmysle aktuálnej rekodifikácie trestného poriadku. Tu sme sa zamerali na komparatívnu analýzu českej a slovenskej právnej úpravy. Dospeli sme k záveru, že v prípade zaistenia počítačových údajov priamo z dátového nosiča, majú OČTK zákonnú možnosť selektovať a citlivo vyberať tie údaje, ktoré sú pre trestné konanie naozaj dôležité. Rovnako sme odporučili, aby technická forma realizácie zaistenia počítačových údajov bola popísaná vo verejne dostupnom odporúčaní - smernici alebo vnútornom predpise policajného zboru.

V osobitnej časti sme ďalej analyzovali vnútornú informáciu súkromnej spoločnosti o kyberútoku. Tá je za istých okolností podobná elektronickému dôkaznému prostriedku. Na príklade kyberútokov voči regulovaným subjektom sme

vysvetlili, akým spôsobom a aké elektronické dôkazné prostriedky o vnútornej informácii sa majú zaistiť, hodnotiť a vysvetliť. Predložili sme odpoveď na to, kedy a za akých podmienok kyberútok splní definíciu vnútornej informácie. Dospeli sme k záveru, že emitent má povinnosť bezodkladne informovať o prebiehajúcom alebo dokonanom kyberútoku relevantnú verejnosť, ak sú splnené podmienky kladené na kvalitu vnútornej informácie. Takéto oznámenie by malo obsahovať jasne a jednoducho formulovaný opis povahy narušenia informačného systému emitenta a základné informácie o prijatých opatreniach. Na záver sme ponúkli praktické odporúčania pre implementáciu procesu o vnútropodnikovom hodnotení elektronických dôkazných prostriedkov o kyberútoku.

Do poslednej kapitoly sme zaradili starodávny inštitút zmenky, ktorý z nepochopiteľných príčin stále odoláva elektronickému kontrahovaniu a súčasnej technológií *blockchainu.* Na komparatívnej analýze sme demonštrovali, že možnosť zavedenia elektronickej zmenky do právnej praxe by priniesla vyššiu dôkaznú spoľahlivosť tohto inštitútu oproti súčasnému stavu. Kapitolu sme uzavreli úvahou o výhodách a nevýhodách implementácie tejto technológie.

Zoznam použitej literatúry

A. Odborné publikácie a články

[1.] ABELOVSKÝ, Tomáš. Elektronický dôkazný prostriedok vo svetle práva duševného vlastníctva. 1. vydání. Brno: Spisy Právnické Fakulty MU, 2014. 1033 s. ISBN 978-80-210-7211-4

[2.] ABELOVSKÝ, Tomáš. Kyberútok ako vnútorná informácia alebo kedy s pravdou von. Revue pro právo a technologie. [Online]. 2017, č. 15 [cit.1.9.2020]. Dostupné z: https://journals.muni.cz/revue/article/view/6307

[3.] ABELOVSKÝ, Tomáš. Počítač ako sudca. Revue pro právo a technológie, Masarykova univerzita, 2016, roč. 7, č. 14, ISSN 1804-5383

[4.] ABELOVSKÝ, Tomáš. Virtualizácia ako metóda riešenia spoločenských problémov, Právny obzor, 2015, roč. 98. č. 2

[5.] ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. Revue pro právo a technologie, Masarykova univerzita, 2015, roč. 6, č. 11, ISSN 1804-5383

[6.] ALEXY, R.: Pojem a platnosť práva, Bratislava: Kaligram, 2009, ISBN 978-80- 8101-062-0

[7.] ALLEN, R. Artificial intelligence and the evidentiary process: The challenges of formalism and computation. Artificial Inteligence and Law 9: 99-114, 2001. Kluwer Academic Publisher. Printed in Netherlands

[8.] AMPÉRE, A. Essai sur la philosophie des sciences ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines. Bachelier, Libraire-éditeur. Paris, 1834. In: [online]. [cit.1.9.2020]. Dostupné z: http://gallica.bnf.fr/ark:/12148/bpt6k110453h

[9.] ARAIZA, Alberto, G. Electronic Discovery in the Cloud, Duke Law and Technology Review, č. 8. 2011 [online]. [cit.1.9.2020]. Dostupné z: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1222&context=dltr

[10.] ARASZKIEWICZ, M. Towards Systematic Research on Statutory Interpretation in AI and Law. Frontiers in Artificial Intelligence and Applications. Ebook. Volume 259: Legal Knowledge and Information Systems. [online]. [cit. 1.9.2020]. Dostupné z: http://ebooks.iospress.nl/publication/35595.

[11.] ARCURI, Brogi a GANDOLFI. The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? [Online]. [cit.1.9.2020]. Dostupné z: http://www.efmaefm.org/0EFMAMEETINGS/EFMA%20ANNUAL%20MEETINGS/2014-Rome/papers/EFMA2014_0408_fullpaper.pdf

[12.] ASIMOV, I. Nahé slunce. Praha: Ivo Železný, 1994

[13.] BARTOŠEK, Milan. 1981. Encyklopedie římského práva. Praha: Panorama. Pyramida (Panorama)

[14.] BARTOŠKOVÁ, Tereza. Doménové spory před Rozhodčím soudem při Hospodářské komoře České republiky a Agrární komoře České republiky, Odborný seminář: Doménová jména a právo - novinky z České republiky i zahraničí. CZ.NIC, z. s. p. o. [online]. [cit.1.9.2020] Dostupné z: http://www.nic.cz/seminar/

[15.] BATH, Robin Burnett and Vivienne. Law of international business in Australasia. Annandale, N.S.W: Federation Press, 2009. ISBN 9781862877245

[16.] BEISNER, John H. Discovering a better way: the need for effective civil litigation reform. Duke Law Journal, vol. 60, no. 3, 2010

[17.] BENTO, V.M. Globalization of Discovery: The Law and Practice under 28 U.S.C. § 1782. Kluwer Law International B.V., 21 Nov 2019. E-book. Chapter 1 Foundational Concepts of International Discovery. [online]. [cit.1.9.2020]. Dostupné z:

https://books.google.ch/books?id=YmfIDwAAQBAJ&printsec=frontcover&dq=inauthor:%22Lucas+V.M.+Bento%22&hl=en&sa=X&ved=0ahUKEwiw19CL6OznAhXhGDQIHYpxB1sQ6AEIKDAA

[18.] BITGLASS. "Where's your data?" experiment. [Online]. [cit.1.9.2020]. Dostupné z: http://pages.bitglass.com/rs/bitglass/images/BR-Bitglass_____Wheres_Your_Data.pdf

[19.] BOBEK, M. – MOLEK, P. – ŠIMÍČEK, V. Komunistické právo v Československu: kapitoly z dějin bezpráví. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2009

[20.] BOCKWEG, Gary. Electronic case files in the federal courts: A preliminray examiation of goals, issues and road ahead. [online]. [cit.1.9.2020]. Dostupné z: http://www.kentlaw.edu/faculty/rstaudt/classes/oldclasses/internetlaw/casebook/Electronic%20Case%20Files%20in%20the%20Federal%20Courts%20Executive%20Summary%20in%20pdf%20format.pdf

[21.] BOGUSZAK, Jiří, Jiří ČAPEK a Aleš GERLOCH. Teorie práva. Vyd. 1. Praha: Eurolex Bohemia, 2001. ISBN 80-86432-13-0

[22.] BOHÁČ, R. Legislativní proces: (teorie a praxe). Praha: Tiskárna Ministerstva vnitra, 2011

[23.] BOHM, R. M. Miscarriages of Criminal Justice: An Introduction. Journal of Contemporary Criminal Justice. 2005, vol. 21, issue 3

[24.] BORDALO, P. GENNAIOLI, N. and SHLEIFER, A. Salience theory of judicial decisions, Journal of Legal Studies, Vol. 44, No. S1, 2015, [online]. [cit.1.9.2020]. Dostupné z: https://scholar.harvard.edu/shleifer/publications/salience-theory-judicial-decisions

[25.] BORCH, Karl. The Theory of Risk. Journal of the Royal Statistical Society. Series B. vol. 29, no. 3, 1967

[26.] BRTKO, Róbert. Dôkazy a dokazovanie v rímskom občianskom procese. Akadémia PZ v Bratislave. [online]. [cit.1.9.2020]. Dostupné z: https://www.akademiapz.sk/sites/default/files/OVVP/004%20BRTKO_cl_Dokazy_APZ.pdf

[27.] BRTNÍK, Stanislav. Materiální a formální pravda v současném soudním procesu. Bulletin advokacie. 2010, č. 10

[28.] BUCKINGHAM, Will. Kniha filozofie. Vyd. 1. Praha: Knižní klub, 2013. Universum (Knižní klub). ISBN 978-80-242-3912-5

[29.] CALAPRICE, A., ed. The New Quotable Einstein, Princeton University Press; 2000

[30.] CALO, Ryan. Bad laws would hurt good drones. In: CNN.COM: Special to CNN [online]. [cit.1.9.2020]. Dostupné z: http://edition.cnn.com/2013/03/05/opinion/calo-drones/

[31.] CALO, Ryan. The drone as privacy catalyst, Stanford Law Review, Vol. 64, 2011

[32.] CARR, J. Inside cyber warfare. Sebastopol, Calif.: 2010. O'Reilly Media, Inc. ISBN 05-968-0215-3

[33.] CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the Internet. 3rd ed. Amsterdam: Elsevier, 2011. ISBN 978-0-12-374268-1

[34.] CAVAGNETTO, Stefano; GAHIR, Bruce. Multiple personalities and the proteus effect in collaborative virtual environments. A. Wittgensteinian viewpoint. Masaryk University Journal of Law and Technology. Brno: Masaryk University. Faculty of Law, 2011, roč. 5, č. 2

[35.] CUMMINS, Robert R. Basics of legal document preparation. Delmar Publishers Inc. 1997. ISBN: 0-8273-6799-6

[36.] CURTIS, S. Explained: how tech companies plan to stop paedophiles sharing child pornography. The Telegraph. 11 Dec 2014. [online]. [cit.1.9.2020]. Dostupné z: http://www.telegraph.co.uk/technology/news/11288028/Explained-how-tech-companies-plan-to-stop-paedophiles-sharing-child-pornography.html

[37.] ČAPEK, K., R.U.R.: Rossum's Universal Robots: kolektivní drama o vstupní komedii a třech dějstvích [online]. Praha: Štorch-Marien, 1920 (Spisy bratří Čapků; sv. 10). Dostupné z: http://web2.mlp.cz/koweb/00/03/34/75/81/rur.pdf

[38.] DAMAŠKA, Mirjan. “A Continental Lawyer in an American Law School: Trials and Tribulations of Adjustment.” University of Pennsylvania Law Review, zv. 116, č. 8, 1968

[39.] DAMAŠKA, Mirjan. Free Proof and Its Detractors. The American Journal of Comparative Law, Vol. 43, No. 3 (Summer, 1995)

[40.] DELEUZE, Giles; GUATTARI,Félix. Anti-Oedipus: capitalism and schizophrenia. University of Minnesota. Humanities Press Inc. 2000. ISBN 0-8166-1225-0

[41.] DELEUZE, Gilles; GUATTARI, Felix. A thousand plateaus: capitalism and schizophrenia. London: Athlone Press, 1988. ISBN 0485120585

[42.] DESET, Miloš. V prípade Kuciakovej úkladnej vraždy je Threema zákonný dôkaz. Denník N. 23. januára 2020. [online]. [cit.1.9.2020]. Dostupné z: https://dennikn.sk/1728346/v-pripade-kuciakovej-ukladnej-vrazdy-je-threema-zakonny-dokaz/

[43.] DETMOLD, M. J. The Unity of law and Morality: A Refutation of Legal Posivism. London: Routledge & Kegan Paul, 1984

[44.] DIAZ, F. Using Technology to Prevent the Distribution of Child Pornography. Berkeley Technology Law Journal. November 10, 2015. [online]. [cit.1.9.2020]. Dostupné z:http://btlj.org/2015/11/using-technology-to-prevent-the-distribution-of-child-pornography/

[45.] DORR, O. Use of Force, Prohibition of, Max Planck Encyclopedia of Public International Law [MPEPIL]. [online]. [cit.1.9.2020]. Dostupné z: Dostupné z: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e427?rskey=4C8VMG&result=1&prd=EPIL

[46.] DOXIADES. Logicomix. 1st U.S. ed. New York: Bloomsbury, 2009. ISBN 1-59691-452-1

[47.] DRÁPAL, BUREŠ a kol. Občanský soudní řád I, II. Komentář. 1. vydání. Praha: C. H. Beck, 2009, ISBN 978-80-7400-107-9

[48.] DWORKIN, R. Taking rights seriously. Cambridge: Harvard University Press, xv

[49.] EHRENTRAUT, Judy. Mark Poster’s “Postmodern Virtualities” and Pierre Levy’s “Becoming Virtual”. In: Simulation Space: Cyberspace, Critical Theory, Gaming [online]. 2013 [cit.1.9.2020]. Dostupné z: http://thesimulationspace.wordpress.com/2013/07/05/mark-posters-postmodern-virtualities-and-pierre-levys-becoming-virtual/

[50.] EPSTEIN, L., LANDES, W., POSNER, R. A Realistic Theory of Judicial Behavior. In The Behavior of Federal Judges. 2013. Cambridge, Massachusetts; London, England: Harvard University Press

[51.] FINDEJS, Stanislav. K otázce elektronického spisu. Právní Prostor. Publikované 14.05.2018. [online]. [cit.1.9.2020]. Dostupné z: https://www.pravniprostor.cz/nazory/glosa-stanislava-findejse/k-otazce-elektronickeho-spisu

[52.] GAMERTSFELDER. Leif. Electronic Bills of Exchange. Will the Current Law Recognise Them? University of New South Wales Law Journal 1998. [online]. [cit.1.9.2020]. Dostupné z: http://www.austlii.edu.au/au/journals/UNSWLJ/1998/50.html

[53.] GARRETT, B. L., Monahan, J. Judging Risk. California Law Review. 2020. Roč. 108. č.2 [online]. [cit.1.9.2020]. Dostupné z: https://lawcat.berkeley.edu/record/1161691

[54.] GAZDA, Viktor. Míra důkazu a úloha pravděpodobnosti v důkazním právu. Právní rozhledy. 2019, č. 3

[55.] GRABINER, J. Partisans and critics of a new science: the case of artificial intelligence and some historical parallels. History and philosophy of modern mathematics, Minnesota Stud. Philos. Sci., XI, Univ. Minnesota Press, Minneapolis, MN, 1988

[56.] GRAYLING.Antohny. Wittgenstein: průvodce pro každého. 1. vyd. v českém jazyce. Praha: Dokořán, 2007. ISBN 9788073630775

[57.] GRYGAR, Jiří. Ustanovení § 127a o. s. ř. a jeho další legislativní směřování. Bulletin-advokacie.cz. 24.04.2018. [online]. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/ustanoveni-127a-o.-s.-r.-a-jeho-dalsi-legislativni-smerovani?browser=mobi

[58.] GŘIVNA, Tomáš. Virtual crimes. Masaryk University Journal of Law and Technology. Brno: Masaryk University. Faculty of Law, 2008, roč. 2, č. 1

[59.] HÁBL, Jan. I když se nikdo nedívá: Fundamentální otázky etického vychovatelství. Pavel Mervart 2015

[60.] HALAS, Norbert, K uchovaniu a vydaniu počítačových údajov z obsahu mobilných telefónov v trestnom konaní. Justičná revue. 72. 2020. č.6-7.

[61.] HANUŠ, Libor. Ústavněprávní vady důkazního procesu z pohledu judikatury Ústavního soudu. Právní rozhledy. 2006, č. 18

[62.] HANYCH, Monika, PIVODA, Marek. Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown. Revue pro právo a technologie. 2017, č. 16

[63.] HAO, Karen. AI is sending people to jail—and getting it wrong. MIT Technology Review. Január 2019. [online]. [cit.1.9.2020]. Dostupné z: https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

[64.] HARAŠTA, Jakub, MÍŠEK, Jakub. IP adresy v kybernetické bezpečnosti*. Revue pro právo a technologie. 2015, č. 12.

[65.] HASÍKOVÁ, J. Počítačový údaj - zdroj dokazovania. Bulletin slovenskej advokácie. 1-2/2013. Bratislava.

[66.] HAVELKOVÁ, Renata, JIRÁSKO, Vojtěch. Využití metody pachové identifikace v trestním řízení. Trestněprávní revue. 2019, č. 9

[67.] HECHMAN, M. How Google handles child pornography in Gmail, search. PC World. Aug 5, 2014. [online]. [cit.1.9.2020]. Dostupné z: http://www.pcworld.com/article/2461400/how-google-handles-child-pornography-in-gmail-search.html

[68.] HENDRYCH, Dušan. Právnický slovník. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009. Beckovy odborné slovníky. ISBN 978-80-7400-059-1

[69.] HILSKÝ, Martin. Slovník citátů z Díla Williama Shakespeara. Vyd. 1. Praha: Academia. ISBN 978-80-200-2193-9

[70.] HOLLÄNDER, Pavel. Filosofie práva. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, ISBN 80-868-9896-2

[71.] HONG, N. a Sidel, R., Hackers Breach Law Firms, Including Cravath and Weil Gotshal. The Wall Street Journal. [Online]. [cit.1.9.2020]. Dostupné z: http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

[72.] HUTCHENS, J. How to Pass the Turing Test by Cheating. University of Western Australia. 1997 [online]. [cit.1.9.2020]. Dostupné z: http://www.csee.umbc.edu/courses/471/papers/hutchens.pdf

[73.] JELÍNEK, Jiří, a kolektiv. Trestní právo procesní. 3. vyd. Praha: Leges, 2013. ISBN 978-80-87576-44-1

[74.] KAAG, John a Sarah KREPS. Morálne riziká dronov: Preklad ŠKODA, Rastislav. In: Zošity humanistov [online]. 2012. vyd. [cit.1.9.2020]. Dostupné z: http://www.zosity-humanistov.sk/2012/08/moralne-rizika-dronov/

[75.] KANDOVÁ, Katarína. Pojem pravdy (nejen) v trestním řízení a některé související instituty. Právník, Praha: AV ČR, Ústav státu a práva, 2017, roč. 156, č. 10, s. 842-857. ISSN 0231-6625

[76.] KARIE, Nickson. KEBANDE, Victor. VENTER, H. Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy. 2019. [Online]. [cit.1.9.2020]. Dostupné z: https://www.researchgate.net/publication/332220947_Diverging_deep_learning_cognitive_computing_techniques_into_cyber_forensics

[77.] KELSEN, H. Všeobecná teorie norem. Preklad Milan Kubín. Masarykova univerzita, Brno. 2000

[78.] KESSELOVÁ, Katarína. Cezhraničný prístup k elektronickým dôkazom v trestných veciach. Visí vo vzduchu európsky Cloud act? Revue pro právo a technologie. č.19. 2019

[79.] KNAPP, Viktor. Teorie práva. 1. vyd. Praha, 1995. Právnické učebnice (C.H. Beck). ISBN 3406401775

[80.] KOLOUCH, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. [online]. [cit.1.9.2020]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/zajistovaci_ukony-rtf.pdf

[81.] KORBEL, František, KOVÁŘ, Dalibor, POTOČŇÁK, Štefan, AMLER, Pavel. Elektronická identita při elektronickém (hmotně)právním jednání. Právní rozhledy. 2019, č. 18

[82.] KOTÁSEK, Josef. Ochrana vnitřních informací. Brno: Tribun EU, 2008. 255 s. ISBN 978-80-7399-355-9

[83.] KOTÁSEK, Josef. Zákon směnečný a šekový: komentář. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-965-4

[84.] KOUKAL, Pavel a Eva ZAHOŘOVÁ. Epravo.cz: Listinná a elektronická podoba písomního právního úkonu [online]. 2012 [cit.1.9.2020]. Dostupné z: http://www.epravo.cz/top/clanky/listinna-a-elektronicka-podoba-pisemneho-pravniho-ukonu-84178.html

[85.] KOVAŘÍK, Zdeněk. Zákon směnečný a šekový: komentář. 5., dopl. vyd. V Praze: C.H. Beck, 2011. Beckovy malé komentáře. ISBN 978-80-7400-385-1

[86.] KRABEC, Tomáš. Limity použití § 127a OSŘ z pohledu soudního znalce. Právní rozhledy. 2015, č. 15-16

[87.] KRIŠTÚFEK, M. Základy práva duševného vlastníctva – autorské právo, jemu príbuzné právo a s ním súvisiace práva. In. Ochrana duševného vlastníctva. Zborník. Bratislava: Vydavateľské oddelenie Právnickej fakulty Univerzity Komenského, 2001

[88.] KŘÍSTEK, Lukáš. Jak má vypadat znalecký posudek. Soudce. 2017, č. 2

[89.] KUBIČKA, Remig, KUBIČKA, Oliver. Počítačové údaje v trestnom konaní. In: Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov. Bratislava. 2018. Akadémia PZ v Bratislave. ISBN 978-80-8054-774-5. [online]. [cit.1.9.2020]. Dostupné z: https://www.akademiapz.sk/sites/default/files/KIM/ZBORNÍK%2021.3.2018%20WEB_0.PDF

[90.] KÜHN, Zdeněk, Michal BOBEK a Radim POLČÁK. Judikatura a právní argumentace: teoretické a praktické aspekty práce s judikaturou. Vyd. 1. Praha: Auditorium, 2006. ISBN 80-903786-0-9

[91.] KÜHN, Zdeněk. Iura novit curia: aplikace starého principu v nových podmínkách. Právní rozhledy. 2004, č. 8

[92.] KULMS, R. Competition law enforcement under informational asymmetry. China-EU Law Journal 5, 2017. [online]. [cit.1.9.2020]. Dostupné z: https://link.springer.com/content/pdf/10.1007/s12689-016-0073-8.pdf

[93.] KURILOVSKÁ, L., KORDÍK, M. Zaistenie vecí a majetku. Právny obzor, 103, 2020, č. 1

[94.] KVOCHKO, Elena. PANT, Rajiv. Why Data Breaches Don't Hurt Stock Prices. Harvard Business Review.[Online]. [cit.1.9.2020]. Dostupné z: https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

[95.] KYCKELHAHN T., COHE T.C. Bureau of Justice Statistics Special Report. Civil Rights Complaints in U.S. District Courts, 1990-2000. [online]. [cit. 1.9.2020]. Dostupné z: https://www.bjs.gov/content/pub/pdf/crcusdc06.pdf

[96.] KYNCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. In: Revue pro právo a technologie. Brno: Masarykova univerzita, č.3, 2011. ISSN 1805-2797

[97.] KYSELOVSKÁ, Tereza. Procesní a kolizní problematika práv k duševnímu vlastnictví se zaměřením na judikaturu Soudního dvora EU. Revue pro právo a technologie. 2013, č. 8

[98.] LEE, Timothy. The inside story of Aaron Swartz's campaign to liberate court filings. ARS Technica. [online]. [cit. 1.9.2020]. Dostupné z: http://arstechnica.com/tech-policy/2013/02/the-inside-story-of-aaron-swartzs-campaign-to-liberate-court-filings/2/

[99.] LEMLEY, M. Place and Cyberspace. California Law Review. no. 2. vol. 91. California Law Review. 2003

[100.] LESSIG, Lawrence. Code: version 2.0. New York: Member of the Perseus Books Group, 2006. ISBN 04-650-3914-6

[101.] LÉVY, Pierre. Becoming virtual: reality in the Digital Age. New York, c1998. ISBN 0306457881

[102.] LI, Victor. Zubulake 10 Years After: Landmark case created an industry–and still stirs debate. ABA Journal, vol. 100, no. 9, 2014

[103.] LOUTOCKÝ, Pavel. Ochrana spotřebitele při uzavírání smluv na internetu a možnost řešení vzniklých sporů online. In: POLČÁK, Radim et al. Právo informačních technologií. 2018. Praha: Wolters Kluwer

[104.] LOWRANCE, W.William. The Nature of Risk. In: Schwing R.C., Albers W.A. (eds) Societal Risk Assessment. General Motors Research Laboratories. 1980. Springer, Boston, MA

[105.] LUKEŠ, Ján. Elektronický spis v agendě elektronického platebního rozkazu. Systém CEPR po roce provozu. [online]. [cit. 1.9.2020]. Dostupné z: http://www.isss.cz/archiv/2013/download/prezentace/msp_lukes.pdf

[106.] LUPAČ Petr, Alena CHROBÁKOVÁ a Jan SLÁDEK, 2014. Internet v České republice 2014. Praha: Filozofická fakulta Univerzity Karlovy v Praze. [online]. [cit.1.9.2020]. Dostupné z: https://www.academia.edu/12609849/The_Internet_in_the_Czech_Republic_2014

[107.] MACUR, J. Dokazovaní a procesní odpovědnost v občanském soudním řízení. Spisy Právnické fakulty University J.E.Purkyně v Brně; svazek 56, Brno. 1984

[108.] MACUR, Josef. Důkazní břemeno v civilním soudním řízení. Brno: Masarykova univerzita, 1995

[109.] MACUR, Josef. Postmodernizmus a zjišťování skutkového stavu v civilním řízení. Brno: Masarykova univerzita, 2001

[110.] MACUR, Josef. Povinnost pravdivosti a její legislativní úprava v civilním soudním řádu. Právní rozhledy. 1999, č. 4

[111.] MACUR, Josef. Vyšetřovací důkaz v civilním soudním řízení. Právní rozhledy. 2000, č. 2

[112.] MAČÁK, K. Kyberútok: ilegalita jednotiek a núl. SME.sk. zo dňa 5. jún 2012. [online]. [cit.1.9.2020]. Dostupné z: http://komentare.sme.sk/c/6405738/kyberutok-ilegalita-jednotiek-a-nul.html

[113.] MADLEŇÁK, Ján. Threema, USB, mobily. Aké dôkazy súd nepripustil v prípade vraždy novinára Kuciaka. Týždeň. [online]. 2019 [cit.1.9.2020]. Dostupné z: https://www.tyzden.sk/politika/61159/threema-usb-mobily-ake-dokazy-sud-nepripustil-v-pripade-vrazdy-novinara-kuciaka/

[114.] MAREK, T.: Autonomie vůle a soukromí na Facebooku. Právní rozhledy, Nakladatelství C. H. Beck 2015. č. 6/2015

[115.] MAŘÁDEK, David. Soukromě pořízený zvukový a zvukově obrazový záznam jako důkazní prostředek a důkaz v civilním soudním řízení. Právní rozhledy. 2015, č. 20

[116.] MASON, Stephen. Electronic evidence. 2nd ed. London: LexisNexis, 2010. ISBN 978-140-5749-121

[117.] MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6.

[118.] MAYS, W. Can Machines Think?. Philosophy. 1952, vol. 27, issue 101[online]. [cit.1.9.2020]. Dostupné z: http://www.journals.cambridge.org/abstract_S003181910002266X

[119.] MCMAHON, P. Rediscovering the Equitable Origins of Discovery: The 'Blending' of Law and Equity Prior to Fusion. in J. Goldberg, H. Smith, & P. Turner (Eds.), Equity and Law: Fusion and Fission. Cambridge: Cambridge University Press. 2019

[120.] MIHÓK, Alexander. Príkaz na zaistenie a oznámenie údajov o uskutočnenej prevádzke a vybrané problémy aplikačnej praxe. Justičná Revue. 71. 2019. č.12.
[121.] MINÁRIK, Š. Trestný poriadok, stručný komentár. Druhé, prepracované a doplnené vydanie. Iura Edition, Bratislava. 2010
[122.] MOOR, J. An analysis of the turing test. Philosophical Studies. 1976, vol. 30, issue 4
[123.] MORÁVEK, Jakub. Kdy lze jako důkazní prostředek připustit záznam z kamerového systému. Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 2011. č. 13. ISSN 1210-6410
[124.] MUSIL, J., KRATOCHVÍL, V., ŠÁMAL, P. a kol. Kurs trestního práva. Trestní právo procesní, 2003
[125.] National Arbitration Forum: Domain Names Disputes. [online]. [cit. 1.9.2020]. Dostupné z: http://domains.adrforum.com/decision.aspx
[126.] NESSON, Charles. The evidence or the event? on judicial proof and the acceptability of verdicts, Logic, Probab. Presumptions Leg. Reason., vol. 98, no. 7. 2013
[127.] NONNEMANN, František. IP adresa jako osobní údaj. Právní rozhledy. 2017, č. 3
[128.] NOVOCKÝ, J. Zaistenie majetku a vecí v trestnom konaní – aplikačné problémy, Justičná akadémia 2013. [online]. [cit.1.9.2020]. Dostupné z: https://www.ja-sr.sk/files/Zaistenie_majetku_a_veci_v_trestnom_konani_aplikacne_problemy.pdf
[129.] OLŠOVSKÝ, Jiří. Slovník filozofických pojmů současnosti. 3., rozš. a aktualiz. vyd., v nakl. Grada 1. Praha: Grada, 2011
[130.] PAUL, Monica. Sony hack sends stock down 10% in past week. .[Online]. [cit.1.9.2020]. Dostupné z: http://money.cnn.com/2014/12/15/investing/sony-stock-hack/
[131.] PAULOV, Ján. Entropia a modelovanie. ORGANON F, 9(1). Filozofický ústav Slovenskej akadémie vied, 2002
[132.] PAVLÍČEK, Václav. a kol., Ústavní právo a státověda, I.díl, Linde Praha, a.s. 1998
[133.] PECH, Lukáš. Vyhledávání důkazů advokátem v trestním řízení. ePravo.cz [online]. [cit.1.9.2020]. Dostupné z: http://www.epravo.cz/top/clanky/vyhledavani-dukazu-advokatem-v-trestnim-rizeni-55563.html
[134.] PEKELIS, V. Malá encyklopédia kybernetiky. Bratislava: Mladé Letá, 1981
[135.] PHILLIP, Phillip. Online 'authenticity' and how Facebook's 'real name' policy hurts Native Americans. In: The Washington Post [online]. [cit.1.9.2020]. Dostupné z: https://www.washingtonpost.com/news/morning-mix/wp/2015/02/10/online-authenticity-and-how-facebooks-real-name-policy-hurts-native-americans/
[136.] PICHA, Marek. 100 myšlenkových experimentů ve filozofii. Vyd. 1. Praha: Dybbuk, 2013. ISBN 978-80-7438-096-9
[137.] PIROŠ, Peter. Princíp ochrany a neporušiteľnosti štátnych hraníc. e-Polis.cz. 2014. [online]. [cit.1.9.2020]. Dostupné z: http://www.e-polis.cz/clanek/princip-ochrany-a-neporusitelnosti-statnych-hranic.html
[138.] PLATO., G. GRUBE a C. REEVE. Republic. Indianapolis: Hackett Pub. Co., xx, 300 p. ISBN 08-722-0136-8
[139.] POLČÁK, Radim. Dokazovaní elektronickými dokumentami. In: Dokazovanie v civilnom a trestnom konaní. Pezinok: Justičná akadémia Slovenskej republiky, 2012. ISBN 978-809-7020-743
[140.] POLČÁK, Radim. Elektronické právní jednání - změny, problémy a nové možnosti v zákoně č. 89/2012 SB. Bulletin Advokacie: www.cak.cz [online]. 2013. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-pravni-jednani-zmeny-problemy-a-nove-moznosti-v-zakone-c.-892012-sb
[141.] POLČÁK, Radim. Internet a proměny práva. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3
[142.] POLČÁK, Radim. Pět tichých minut za Viktorem Knappem. Právník, Praha: AV ČR, Ústav státu a práva, 2013, roč. 152, č. 12. ISSN 0231-6625

[143.] POLČÁK, Radim. PÚRY, František, HARAŠTA, JAKUB a kolektiv. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015, Spisy Právnické fakulty MU č. 542 (řada teoretická, Edice Scientia). ISBN 978-80-210-8073-7MUNI/A/1296/2014

[144.] POLČÁK, Radim. SVANTESSON, Dan. Chapter 6. A possible method for solving sovereignty clashes. In: Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. Edward Elgar Publishing, 2017 – (eBook 1/19)

[145.] POLČÁK. Právo a evropská informační společnost. vyd. Brno: Masarykova univerzita, 2009. Spisy Právnické fakulty Masarykovy univerzity v Brně, sv. 344. ISBN 9788021048850

[146.] POSTER, Mark. Postmodern Virtualities. In: Personal web page: UCI History Department Faculty [online]. 1995 [cit.1.9.2020]. Dostupné z: http://www.csun.edu/~snk1966/Pomovirt.htm

[147.] PUIG, Gonzalo Villalta. Electronic Bills of Exchange and Promissory Notes in Australia. Murdoch University Electronic Journal of Law. 3/2000. [online]. [cit.1.9.2020]. Dostupné z: http://www.murdoch.edu.au/elaw/issues/v7n3/puig73b.html.

[148.] PULKRÁBEK, Zdeněk. O dokazování negativních skutečností v civilním soudním řízení (a o některých zásadách zjišťování skutkového stavu vůbec). Právní rozhledy. 2013, č. 17

[149.] PULKRÁBEK, Zdeněk. Znovu a trochu jinak o dokazování negativních skutečností. Právní rozhledy. 2018, č. 1

[150.] RADBRUCH, G. O napětí mezi účely práva. Vyd. 1. Překlad Libor Hanuš. Praha: Wolters Kluwer Česká republika, 2012

[151.] RACHLINSKI, Jeffrey J. Gains, Losses, and the Psychology of Litigation. 1996. Cornell Law Faculty Publications. Paper 795. [online]. [cit.1.9.2020]. Dostupné z: http://scholarship.law.cornell.edu/facpub/795

[152.] RAMPÁŠEK, M. Uchovanie a vydanie počítačových údajov v trestnom konaní. Bulletin slovenskej advokácie. ISSN 1335-1079. Roč. 19, č. 5. 2013

[153.] REILING, Dory. Technology for Justice, Leiden University Press, 2009. [cit. 1.9.2020]. Dostupné z: https://openaccess.leidenuniv.nl/bitstream/handle/1887/21365/file174577.pdf?sequence=1

[154.] REPÍK, B. Procesní důsledky porušení předpisů o dokazování v trestním řízení, Bulletin advokacie, 1982

[155.] SAINT-EXUPÉRY, Antoine. Malý princ. Gardenia Publishers, Bratislava, 2000

[156.] SARTOR, G. Doing justice to rights and values: teleological reasoning and proportionality. Artificial Intelligence and Law. June 2010, Volume 18, Issue 2 [online]. [cit.1.9.2020]. Dostupné z: http://link.springer.com/article/10.1007/s10506-010-9095-7

[157.] SEAL, Mark. An Exclusive Look at Sony's Hacking Saga. Vanity Fair. Retrieved February 4, 2015.[Online]. [cit.1.9.2020]. Dostupné z: http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

[158.] SCHEPPELE, Kim Lane. „It's Just Not Right": The Ethics of Insider Trading. Law and Contemporary Problems, Vol. 56, No. 3, Modern Equity, Summer, 1993

[159.] SCHIELDS, Rob. The Role of the Virtual in Knowledge-Based Economies, Organizations, and Localities. In: SEED Journal Semiotics, Evolution, Energy, and Developmen [online]. 2020 [cit.1.9.2020]. Dostupné z: http://see.library.utoronto.ca/SEED/Vol2-4/shields.html

[160.] SCHWARTZ, John. An Effort to Upgrade a Court Archive System to Free and Easy. New York Times. [online]. [cit.1.9.2020]. Dostupné z: http://www.nytimes.com/2009/02/13/us/13records.html?pagewanted=all&_r=0

[161.] SIMMA, B. NATO, the UN and the Use of Force: Legal Aspects, European Journal of International Law, roč. 10, č. 1, 2003

[162.] SINGEL, Ryan. FBI Investigated Coder for Liberating Paywalled Court Records. WIRED. [online]. [cit.1.9.2020]. Dostupné z: http://www.wired.com/2009/10/swartz-fbi/

[163.] SMEJKAL, Vladimír. Elektronické důkazy – současnost či budoucnost českého soudnictví? Bulletin-advokace.cz. [online]. [cit.1.9.2020]. Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-dukazy-soucasnost-ci-budoucnost-ceskeho-soudnictvi

[164.] SMULLYAN, Raymond. Šachové záhady Sherlocka Holmese, aneb, Padesát úloh šachové dedukce, které vám nedají spát. 1. vyd. Praha: Mladá fronta, 2005. ISBN 80-204-1233-6

[165.] SOBEK, Tomáš. Nemorální morálka. In: Jiné právo [online]. [cit.1.9.2020]. Dostupné z: http://jinepravo.blogspot.sk/2010/07/tomas-sobek-nemoralni-moralka.html

[166.] SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. Bulletin advokacie. 2019, č. 9, s. 15-19

[167.] STUPKA, Václav. eJustice. Revue pro právo a technologie. 2011, č. 2

[168.] SUSSKIND, Richard E. The end of lawyers?: rethinking the nature of legal services. New York: Oxford University Press, 2008. ISBN 978-0-19-954172-0

[169.] SUSSKIND, Richard. Transforming the law: essays on technology, justice, and the legal marketplace. 1. publ. New York: Oxford University Press, 2001

[170.] SVANTESSON, Dan. A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft. AJIL Unbound. 2015. Vol 109

[171.] SVOBODA, Karel, Dokazovaní, Praha: ASPI – Wolters Kluwer, 2009

[172.] SVOBODA, Karel, SMOLÍK, Petr, LEVÝ, Jiří, ŠÍNOVÁ, Renáta. Občanský soudní řád. 2. vydání. Praha: Nakladatelství C. H. Beck, 2017

[173.] ŠÁMAL, P. a kol.: Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013

[174.] ŠÁMAL, Pavel. Provádění dokazování v hlavním líčení a úprava absolutní a relativní neúčinnosti důkazů ve věcném záměru trestního řádu. Trestněprávní revue. 2008, č. 12

[175.] ŠAMKO, P. Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestom konaní. Zo súdnej praxe. 2017, č. 6

[176.] ŠAVELKA, J., ASHELEY, K., Extracting Case Law Sentences for Argumentation about the Meaning of Statutory Terms. In Proceedings of the 3rd Workshop on Argument Mining. ACL, 2016 [online]. [cit.1.9.2020]. Dostupné z: http://www.aclweb.org/anthology/W/W16/W16-28.pdf#page=62

[177.] ŠKOP, Martin, 2013. --právo, jazyk a příběh. Praha: Auditorium. ISBN 978-80-87284-37-7

[178.] ŠKOP, Martin. Základní metodologie dokazovaní v právu. In: Dokazovanie v civilnom a trestnom konaní. Pezinok: Justičná akadémia Slovenskej republiky, 2012. ISBN 978-809-7020-743

[179.] ŠOVAR, Ján. Soudní dvůr Evropské unie k insider tradingu: Jak moc nepřesná informace je ještě přesná?.[Online]. [cit.1.9.2020]. Dostupné z: https://www.patria.cz/pravo/2949748/soudni-dvur-evropske-unie-k-insider-tradingu-jak-moc-nepresna-informace-je-jeste-presna.html

[180.] TELEC, Ivo. Šíření děl a výkonů v telekomunikačních sítích, zvláště v Internetu, In: Právní rozhledy: časopis pro všechna právní odvětví. Praha: C. H. Beck. 1997. č.4. ISSN 1210-6410

[181.] TLAPÁK NAVRÁTILOVÁ, Jana, GALOVCOVÁ, Ingrid. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?. Bulletin advokacie. 2019, č. 11

[182.] TOMOSZEK, Maxim. Jaké zásady pro znalecké dokazování vyplývají z práva na spravedlivý proces? Časopis pro právní vědu a praxi. 2020, č. 1

[183.] TSAKATOURA, Anastasia. E-finance — bills of exchange, promissory notes, documentory credits, forfaiting. [online]. [cit.1.9.2020]. Dostupné z: http://www.inter-lawyer.com/lex-e-scripta/articles/e-finance1.htm

[184.] TURING, A. Computing machinery and intelligence. Mind, 1950. 59 [online]. [cit.1.9.2020]. Dostupné z: http://www.loebner.net/Prizef/TuringArticle.html

[185.] TVERSKY, Amos. KAHNEMAN, Daniel. Judgment under Uncertainty: Heuristics and Biases. Science, vol. 185, no. 4157, 1974

[186.] TVRDÝ, F. Turingův test. TOGGA, spol. s r.o., Praha, 2014

[187.] UHLÍŘ, A. Soudní znalci ničí lidské životy: aneb o neschopnosti Ministerstva spravedlnosti ČR vyřešit letitý problém. Britské listy. [online]. [cit.1.9.2020]. Dostupné z: http://blisty.cz/art/57881.html

[188.] UŠIAK, J.: Premeny suverenity európskych štátov v kontexte vybraných teórií medzinárodných vzťahov. In.: Současná Evropa, roč. 14, 2009, č. 2., ISSN 1804-1280

[189.] VALČEK, Adam. Aj kľúčová znalkyňa hovorí o antedatovaní zmeniek. Sme.sk. Petit Press, a.s. 10.2.2020. [online]. [cit.1.9.2020]. Dostupné z: https://domov.sme.sk/c/22322855/aj-klucova-znalkyna-hovori-o-antedatovani-zmeniek.html

[190.] VANTUCH, Pavel. Kdy může obhajoba důkaz vyhledat, kdy předložit a kdy jen navrhnout jeho provedení? Bulletin advokacie. 2013, č. 7-8

[191.] VUČKA, Jan. Test proporcionality při zajišťování důkazů. Trestněprávní revue. 2010, č. 9

[192.] VUČKA, Ján. Znalecký posudek - dobrý sluha, ale zlý pán. Jiné Právo. [online]. [cit.1.9.2020]. Dostupné z: https://jinepravo.blogspot.com/2011/09/znalecky-posudek-dobry-sluha-ale-zly.html

[193.] WEINBERGER, O., ZICH, O. Logika. Praha 1965

[194.] WEINBERGER, Otto. Základy právní logiky. Brno: MU, 1993. ISBN 80-210-0827-X

[195.] WIENER, N. Cybernetics: or Control and Communication in the Animal and the Machine. 2.edition. Quid Pro Books, 2013

[196.] WIENER, Norbert. With a new introduction by Steve J. HEIMS. The human use of human beings: cybernetics and society. London: Free Association, 1989. ISBN 18-534-3075-7

[197.] WILLIAMS, P. The brain is just a computer made of meat. Science, Technology and Society. STAS Topic 3, [online]. [cit.1.9.2020]. Dostupné z: http://www.technoid.net/uni/ai.doc

[198.] WINTEROVÁ, Alena a kol. Civilní právo procesní. 6. aktualiz. vyd. Praha. Linde. 2008

[199.] WITTGENSTEIN, Ludwig. Tractatus logico-philosophicus. Kalligram, Bratislava, 2003

[200.] ZÁHORA, Jozef a kol. Dokazovanie v trestnom konaní. 1.vydanie. Praha: Leges, 2013

[201.] ZIMA, Petr. Limity použití § 127a OSŘ. Právní rozhledy. 2015, č. 10

[202.] ZOUBKOVÁ, Ivana a Jana FIRSTOVÁ. Kriminologie: aktuální problémy. Vyd. 1. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-395-6

B. Rozhodnutia súdov

[1.] District Court of Maryland. Lorraine et al. v. Markel American Insurance Company [online]. 2007 [cit.1.9.2020]. Dostupné z: https://www.govinfo.gov/app/details/USCOURTS-mdd-1_06-cv-01893

[2.] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González. Judgment of the Court (Grand Chamber) of 13 May 2014, No. C-131/12. Case-law of the Court of Justice [online]. 6. June 2013. [online]. [cit.1.9.2020]. Dostupné z:http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[3.] Najvyšší súd USA: Prípad Brady v. Maryland, 373 U.S. 83 (1963) [online]. [cit. 1.9.2020]. Dostupné z: https://scholar.google.com/scholar_case?case=9550433126269674519

[4.] Nález ÚS ČR ze dne 1. 11. 2001, sp. zn. III. ÚS 190/01

[5.] Nález ÚS ČR ze dne 1. 3. 2007, sp. zn. Pl. ÚS 8/06

[6.] Nález ÚS ČR ze dne 10. 8. 2017, sp. zn. I. ÚS 615/17

[7.] Nález ÚS ČR ze dne 13. 11. 2018, sp. zn. I. ÚS 1491/17-2

[8.] Nález ÚS ČR ze dne 13. 8. 2002, sp. zn. Pl. ÚS 3/02

[9.] Nález ÚS ČR ze dne 15. 1. 2009, sp. zn. IV. ÚS 1554/08

[10.] Nález ÚS ČR ze dne 15. 2. 2016, sp. zn. I. ÚS 368/15

[11.] Nález ÚS ČR ze dne 20. 8. 2013, sp. zn. I. ÚS 1428/13

[12.] Nález ÚS ČR ze dne 20. 8. 2014, sp. zn. I. ÚS 173/13

[13.] Nález ÚS ČR ze dne 22. 9. 2015, sp. zn. I. ÚS 1944/15

[14.] Nález ÚS ČR ze dne 25. 11. 2010, sp. zn. II. ÚS 889/10

[15.] Nález ÚS ČR ze dne 27. 2. 2018, sp. zn. II. ÚS 2299/17

[16.] Nález ÚS ČR ze dne 27. 9. 2006, sp. zn. Pl. ÚS 51/06

[17.] Nález ÚS ČR ze dne 29. 4. 2009, sp. zn. I. ÚS 3094/08

[18.] Nález ÚS ČR ze dne 3. 9. 2009, sp. zn. III. ÚS 346/09

[19.] Nález ÚS ČR ze dne 9. 12. 2014, sp. zn. II. ÚS 1774/14

[20.] Nález ÚS ČR zo dňa 15. augusta 2005, sp. zn. IV. ÚS 314/05

[21.] Nález ÚS SR zo dňa 25. augusta 2010, sp. zn. III. ÚS 68/2010

[22.] Rozhodnutí NS ČR ze dne 17.12.2013, sp. zn. 23 Cdo 3895/2011

[23.] Rozhodnutí NS ČSSR ze dne 8. 7. 1980, sp. zn. Tzv 17/80. [R 33/1981 tr.]

[24.] Rozhodnutí NSS ČR ze dne 19. 9. 2011, č. j. 15 Kse 4/2011-62

[25.] Rozhodnutí ÚS ČR ze dne 30.10.2014 sp.zn. III.ÚS 3844/13

[26.] Rozhodnutie ESĽP zo dňa 16.10.2007, spis. zn. 74336/01 vo veci Wieser a Bicos Beteiligungen GmbH proti Rakúsku [online]. [cit.1.9.2020]. Dostupné z: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-82711

[27.] Rozhodnutie SDEÚ vo veci Data Protection Commissioner v Facebook Ireland and Maximillian Schrems zo dňa 16.7.2020, C-311/18

[28.] Rozhodnutie SDEÚ zo dňa 08/04/2014 - Digital Rights Ireland a Seitlinger a další, Vec C-293/12 a Vec C-594/12

[29.] Rozhodnutie ÚS ČR zo dňa 14.12.2011, sp. zn. IV. ÚS 3225/09

[30.] Rozhodnutie ÚS SR zo dňa 25.8.2010, sp. zn. III. ÚS 68/2010-62

[31.] Rozhodnutie ÚS SR zo dňa 29. apríla 2015, sp. zn. PL. ÚS 10/2014

[32.] Rozhodnutie ÚS SR zo dňa 29.4.2015, sp. zn. PL. ÚS 10/2014

[33.] Rozsudek NS ČR ze dne 10. 1. 2013, sp. zn. 30 Cdo 2591/2011-I

[34.] Rozsudek NS ČR ze dne 10. 6. 2008, sp. zn. 28 Cdo 1813/2008

[35.] Rozsudek NS ČR ze dne 11. 5. 2005, sp. zn. 30 Cdo 64/2004
[36.] Rozsudek NS ČR ze dne 15. 10. 2019, sp. zn. 25 Cdo 1778/2019
[37.] Rozsudek NS ČR ze dne 20. 3. 2008, sp. zn. 21 Cdo 3075/2006
[38.] Rozsudek NS ČR ze dne 22. 1. 2014, sp. zn. 26 Cdo 3928/2013
[39.] Rozsudek NS ČR ze dne 24. 4. 2013, sp. zn. 30 Cdo 718/2013
[40.] Rozsudek NS ČR ze dne 24. 9. 2014, sp. zn. 30 Cdo 1982/2012
[41.] Rozsudek NS ČR ze dne 26. 4. 2016, sp. zn. 23 Cdo 3415/2014
[42.] Rozsudek NS ČR ze dne 26. 7. 2017, sp. zn. 22 Cdo 1479/2017
[43.] Rozsudek NS ČR ze dne 27. 3. 2008, sp. zn. 29 Odo 1538/2006 (Rc 28/2009 civ.)
[44.] Rozsudek NS ČR ze dne 27. 5. 2015, sp. zn. 30 Cdo 5216/2014
[45.] Rozsudek NS ČR ze dne 4. 9. 2018, sp. zn. 22 Cdo 2711/2018
[46.] Rozsudek NSS ČR ze dne 2.4.2008, sp. zn. 3 As 2/2008 – 152
[47.] Rozsudek NSS ČR ze dne 26. 6. 2003, č. j. 22 Ca 427/2002-35
[48.] Rozsudek NSS ČR ze dne 4. 2. 2009, č. j. 1 As 90/2008-189
[49.] Rozsudek NSS ČR ze dne 6. 3. 2019, č. j. 2 As 153/2018-31
[50.] Rozsudok NS SR zo dňa 26.11.2014, sp. zn. 2To/9/2014
[51.] Rozsudok SDEÚ zo dňa 11.3.2015, sp. zn. C‑628/13 vo veci Jean-Bernard Lafonta proti Autorité des marchés financiers
[52.] Rozsudok SDEÚ zo dňa 29. 1. 2008, sp. zn C-275/06 vo veci Produtores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU
[53.] Rzsudek SDEU z 19. 10. 2016, C-582/14, Breyer v. Německo.
[54.] Societe Nationale Industrielle Aerospatiale and Societe de Construction d'Avions de Tourisme, Petitioners v. United States District Court for the Southern District of Iowa 107 S.Ct 2542. [online]. [cit.1.9.2020]. Dostupné z: https://www.law.cornell.edu/supremecourt/text/482/522
[55.] Stanovisko generálního advokáta - Wahl - 11 září 2014. - CA Consumer Finance proti Ingrid Bakkaus a další - Věc C-449/13
[56.] Usnesení NS ČR ze dne 22. 3. 2012, sp. zn. 6 Tdo 89/2012
[57.] Usnesení NS ČR ze dne 22. 5. 2019, sp. zn. 26 Cdo 1230/2019
[58.] Usnesení NS ČR ze dne 22. 7. 2014, sp. zn. 4 Tdo 815/2014-37
[59.] Usnesení NS ČR ze dne 25. 6. 2014, sp. zn. 3 Tcu 33/2014-26
[60.] Usnesení NS ČR ze dne 27. 1. 2010, sp. zn. 5 Tdo 31/2010
[61.] Usnesení NS ČR ze dne 4. 6. 2008, sp. zn. 28 Cdo 1938/2008
[62.] Usnesení NS ČR ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011
[63.] Usnesení NS ČR ze dne 9. 6. 2000, sp. zn. 21 Cdo 2587/99
[64.] Usnesení ÚS ČR ze dne 12. 9. 2017, sp. zn. III. ÚS 2977/16
[65.] Usnesení ÚS ČR ze dne 14. 12. 2011, sp. zn. IV. ÚS 3225/09
[66.] Usnesení ÚS ČR ze dne 19. 9. 2013, sp. zn. III. ÚS 1077/13
[67.] Uznesenie ÚS SR zo dňa 17.1.2012, sp. zn. III. ÚS 24/2012-53

C. Legislatíva a medzinárodné zmluvy

[1.] 18 U.S. Code Chapter 119 - Wire and electronic communications interception and interception of oral communications. [online]. [cit.1.9.2020]. Dostupné z: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

[2.] BGer 4A_9/2018, 31. Oktober 2018. [online]. [cit.1.9.2020]. Dostupné z: https://www.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F31-10-2018-4A_9-2018&lang=de&type=show_document&zoom=YES&

[3.] Budapeštiansky dohovor o počítačovej kriminalite z 23. novembra 2001. Oznámenie Ministerstva zahraničných vecí SR publ. pod č. 137/2008 Z.z.

[4.] Cal. Civ. Code 1798.82 and 1798.29. [Online]. [cit.1.9.2020]. Dostupné z: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

[5.] Commonwealth of Australia. National Competition Policy Review of the Bills of Exchange Act 1909. July 2003 [online]. [cit.1.9.2020]. Dostupné z: http://ncp.ncc.gov.au/docs/AG%20review%20of%20the%20Bills%20of%20Exchange%20Act%2C%20July%202003.pdf

[6.] Division of Corporation Finance, Securities and Exchange Commission, CF Disclosure Guidance. 2011. [Online]. [cit.1.9.2020]. Dostupné z: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[7.] Dôvodová správa k návrhu nariadenia o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [Online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A52018PC0225

[8.] Draft Convention on Jurisdiction with Respect to Crime. 1935. American Journal of International Law, 29(S1). [online]. [cit.1.9.2020]. Dostupné z: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/draft-convention-on-jurisdiction-with-respect-to-crime/30D6EC4FC2D1E0377E93B7623992A189

[9.] Důvodová zpráva Návrhu zákona o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv [online]. [cit.1.9.2020]. Dostupné z: https://apps.odok.cz/kpl-detail?pid=KORN999FKLW5. Ekonomický deník. [online]. [cit.1.9.2020]. https://ekonomickydenik.cz/esbirka-a-elegislativa-nejdrive-v-roce-2021

[10.] ESAs: Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT). [Online]. [cit.1.9.2020]. Dostupné z: https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

[11.] European Comission. Public consultation on improving cross-border access to electronic evidence in criminal matters. [online]. [cit.1.9.2020]. Dostupné z: https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en

[12.] European Commission: Explanatory note to an authorisation to conduct an inspection in execution of a Commission decision under Article 20(4) of Council Regulation No 1/2003 [online]. [cit.1.9.2020]. Dostupné z: https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf

[13.] Európska rada: Rada Európskej komisie. Nariadenie o cezhraničnom prístupe k elektronickým dôkazom: Rada sa dohodla na pozícii. [online]. [cit.1.9.2020]. Dostupné z: https://www.consilium.europa.eu/sk/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[14.] Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings: Explanatory Memorandum. 1335th meeting of the European Committee on Legal Co-operation (CDCJ), 30 January 2019. Council of Europe. [online]. [cit.1.9.2020]. Dostupné z: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e

[15.] H.R.4943 - CLOUD Act. [online]. [cit.1.9.2020]. Dostupné z: https://www.congress.gov/bill/115th-congress/house-bill/4943

[16.] HCCH Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/docs/ec1fc148-c2b1-49dc-ba2f-65f45cb2b2d3.pdf

[17.] Charta Organizace spojených národů a Statut Mezinárodního soudního dvora, Informační centrum OSN, Praha, 2002. [online]. [cit.1.9.2020]. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/03/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf

[18.] International Chamber of Commerce: The Legal Status of Electronic Bills of Lading. A report for the ICC Banking Commission. 2018. [online]. [cit.1.9.2020]. Dostupné z: https://cdn.iccwbo.org/content/uploads/sites/3/2018/10/the-legal-status-of-e-bills-of-lading-oct2018.pdf (Viď zoznam článkov uverejnený na Iuridictum – Encyklopedie o právu: Směnka. [online]. [cit.1.9.2020]. Dostupné z: http://iuridictum.pecina.cz/w/Směnka).

[19.] Justičná spolupráca v občianskych veciach. Informačné listy o Európskej únii. [online]. [cit.1.9.2020]. Dostupné z: https://www.europarl.europa.eu/factsheets/sk/sheet/154/justicna-spolupraca-v-obcianskych-veciach

[20.] Ministerstvo spravedlnosti ČR: Komise pro nový trestní řád. Věcný záměr trestního řádu - hlavní principy navrhované rekodifikace trestního práva procesního [online]. [cit.1.9.2020]. Dostupné z: http://www.ceska-justice.cz/wp-content/uploads/2014/04/hlavn%C3%AD_principy_1.pdf

[21.] Ministerstvo spravedlnosti ČR: Komise pro nový trestní řád. Východiska a principy nového trestního řádu [online]. [cit.1.9.2020]. Dostupné z: http://portal.justice.cz/Justice2/soubor.aspx?id=112883

[22.] Ministerstvo spravodlivosti SR. Dôvodová správa, Všeobecná časť, Podľa Plánu legislatívnych úloh vlády SR na rok 2003 sa predkladá do legislatívneho procesu návrh nového Trestného poriadku. Epi.sk. Elektronické právne informácie. [online]. [cit.1.9.2020]. Dostupné z: http://www.epi.sk/dovodova-sprava/Dovodova-sprava-k-zakonu-c-301-2005-Z-z.aspx

[23.] Ministerstvo spravodlivosti SR. Elektronický súdny spis. [online]. [cit. 2020-09-01]. Dostupné z: http://www.justice.gov.sk/Stranky/Nase-sluzby/Nase-projekty/Elektronicky%20sudny%20spis/Elektronicky-sudny-spis.aspx

[24.] Ministerstvo spravodlivosti SR. Riadne predbežné stanovisko k návrhu nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. LP/2018/566. [online]. [cit.1.9.2020]. Dostupné z: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2018/566/

[25.] Ministerstvo spravodlivosti SR. Správa o základných otázkach justície. [online]. [cit. 2020-09-01]. Dostupné z: http://www.nrsr.sk/web/Dynamic/Download.aspx?DocID=374610

[26.] MS ČR: České soudnictví 2019: Výroční statistická zpráva. Dostupné z: https://justice.cz/documents/12681/719244/Ceske_soudnictvi_2019_vyrocni_stat_zprava.pdf/28174b8b-c421-440b-9a17-1f48cfc50efc

[27.] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (GDPR)

[28.] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 596/2014 z 16. apríla 2014 o zneužívaní trhu (MAR) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES

[29.] Nariadenie Európskeho parlamentu a rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

[30.] Nariadenie Rady (ES) č. 1206/2001 z 28. mája 2001 o spolupráci medzi súdmi členských štátov pri vykonávaní dôkazov v občianskych a obchodných veciach.

[31.] Návrh nariadenia a smernice Komisie EÚ na vytvorenie právneho rámca, ktorý by policajným a súdnym orgánom uľahčil a urýchlil zabezpečovanie a získavanie prístupu k elektronickým dôkazom v cezhraničných prípadoch zo dňa 17.4.2018. Procedurálna zložka č. 2018/0107(COD) a 2018/0108(COD) [online]. [cit.1.9.2020]. Dostupné z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0107(COD)&l=en a https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0108(COD)&l=en

[32.] Návrh nariadenia Európskeho parlamentu a Rady o európskom príkaze na predloženie a uchovanie elektronických dôkazov v trestných veciach. [online]. [cit.1.9.2020]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/sk/pdf

[33.] Návrh smernice, ktorou sa stanovujú harmonizované pravidlá určovania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní. [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52018PC0226

[34.] Outline of the Convention. HCCH. [online]. [cit.1.9.2020]. Dostupné z: https://www.hcch.net/en/instruments/conventions/specialised-sections/evidence

[35.] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM/2018/226 final - 2018/0107 (COD). [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN

[36.] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM/2018/225 final - 2018/0108 (COD). [online]. [cit.1.9.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN

[37.] Rekodifikace trestního práva procesního. Pracovní verze paragrafového znění, které je aktuální ke dni 1. 1. 2020. [online]. [cit.1.9.2020]. Dostupné z: https://tpp.justice.cz

[38.] Řád Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky, [online]. [cit. 21.7.2020]. Dostupné z: https://www.soud.cz/rady/rad-rozhodciho-soudu-01-07-2012

[39.] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č.104/2013 Sb. medzinárodných smluv ČR. [online]. [cit.1.9.2020]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=26438

[40.] Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (Stand am 1. Juli 2020). [online]. [cit.1.9.2020]. Dostupné z: https://www.admin.ch/opc/de/classified-compilation/19070042/index.html

[41.] Smernica Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach. [online]. [cit.1.9.2020]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0041&qid=1430677259904&from=EN

[42.] Sněmovní tisk 74. Vl.n.z.o změně zák.v souv.s přij. z. o znalcích a soud.tlum. - EU [online]. [cit.1.9.2020]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?o=8&t=74&snzp=1

[43.] Stanovisko NSZ č. 1/2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek

[online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf

[44.] The US Federal Rules of Civil Procedure (eff. Dec. 1, 2019). [online]. [cit.1.9.2020]. Dostupné z: https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure

[45.] Ústavní zákon č. 1/1993 Sb., Ústava České republiky

[46.] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod

[47.] Věcný záměr civilního řádu soudního. Dostupné z: https://crs.justice.cz

[48.] Vyhláška č. 129/1976 Sb. ministra zahraničních věcí o Úmluvě o provádění důkazů v cizině ve věcech občanských a obchodních v znení sdělení č. 68/2014 Sb. m. s. Ministerstva zahraničních věcí, kterým se vyhlašuje oprava českého překladu Úmluvy o provádění důkazů v cizině ve věcech občanských nebo obchodních, vyhlášené pod č. 129/1976 Sb.

[49.] Vyhláška č. 37/1992 Sb., ministerstva spravedlnosti České republiky o jednacím řádu pro okresní a krajské soudy

[50.] Vyhláška č. 543/2005 Z. Ministerstva spravodlivosti Slovenskej republiky o spravovacom a kancelárskom poriadku pre okresne súdy, krajské súdy, Špeciálny súd a vojenské súdy

[51.] Výkladové stanovisko č. 1/2018 k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu. [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_719-2017.pdf

[52.] Výkladové stanovisko NSZ č. 9/2001 k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků. [online]. [cit.1.9.2020]. Dostupné z: https://verejnazaloba.cz/wp-content/uploads/2020/03/stanovisko-9-2001.pdf

[53.] Vykonávacie nariadenie Komisie (EÚ) 2016/347 z 10. marca 2016, ktorým sa stanovujú vykonávacie technické predpisy, pokiaľ ide o presný formát zoznamov osôb, ktoré majú dôverné informácie, a pre aktualizáciu zoznamov osôb, ktoré majú dôverné informácie, v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 596/2014

[54.] Zákon č. 141/1961 Sb., o trestním řízení soudním (Trestní řád)

[55.] Zákon č. 160/2015 Z.z., Civilný sporový poriadok

[56.] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

[57.] Zákon č. 191/1950 Sb., Zákon směnečný a šekovýZákon č. 99/1963 Sb., Občanský soudní řád

[58.] Zákon č. 21/2006 Sb. o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování)

[59.] Zákon č. 254/2019 Sb. o znalcích, znaleckých kancelářích a znaleckých ústavech

[60.] Zákon č. 255/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o znalcích, znaleckých kancelářích a znaleckých ústavech a zákona o soudních tlumočnících a soudních překladatelích

[61.] Zákon č. 256/2004 Sb. o podnikání na kapitálovém trhu

[62.] Zákon č. 280/2009 Sb., Daňový řád

[63.] Zákon č. 300/2005 Z. z., Trestný zákon

[64.] Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů

[65.] Zákon č. 301/2005 Z.z., Trestný poriadok

[66.] Zákon č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok)

[67.] Zákon č. 351/2011 Z. z., o elektronických komunikáciách

[68.] Zákon č. 36/1967 Sb. o znalcích a tlumočnících

[69.] Zákon č. 382/2004 Z.z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov
[70.] Zákon č. 40/2009 Sb., Trestní zákoník
[71.] Zákon č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov
[72.] Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů
[73.] Zákon č. 500/2004 Sb., Správní řád
[74.] Zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov
[75.] Zákon č. 89/2012 Sb., Občanský zákoník
[76.] Zákon č. 99/1963 Sb., Občanský soudní řád
[77.] Zákon č. 99/1963 Z.z., Občiansky súdny poriadok (zrušený)
[78.] Zmluva o fungovaní Európskej únie

D. Ostatné pramene

[1.] CLEMENT, J. Global social networks ranked by number of users 2020. In: STATISTA.com. Most popular social networks worldwide as of July 2020, ranked by number of active users (in millions). [online]. [cit.1.9.2020]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[1.] Conclusions and Recommendations of the 2009 Special Commission on the practical operation of the Hague Apostille, Service, Taking of Evidence and Access to Justice Conventions. HCCH. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/upload/wop/jac_concl_e.pdf

[2.] COVID-19 and the global approach to further court proceedings, hearings. Norton Rose Fulbright. [online]. [cit.1.9.2020]. Dostupné z: https://www.nortonrosefulbright.com/de-de/wissen/publications/bbfeb594/covid-19-and-the-global-approach-to-further-court-proceedings-hearings

[3.] Česká pošta. PostServis. Co je to hybridní pošta? [online]. [cit. 21.7.2020]. Dostupné z: http://www.ceskaposta.cz/sluzby/tisk-a-kompletace-zasilek/postservis#1

[4.] DLA Passes Third Day Without Email After Malware Attack. Law360, New York. June 29, 2017. [Online]. [cit.1.9.2020]. Dostupné z: https://www.law360.com/articles/939824/dla-passes-third-day-without-email-after-malware-attack

[5.] Do spisů Ústavního soudu přistupuje elektronicky přes internet 222 advokátů. Česká justice. Media Network s.r.o. [online]. [cit.1.9.2020]. Dostupné z: https://www.ceska-justice.cz/2019/03/do-spisu-ustavniho-soudu-pristupuje-elektronicky-pres-internet-222-advokatu/

[6.] First Turing Test success marks milestone in computing history. In: Phys.org. [online]. [cit.1.9.2020]. Dostupné z: http://phys.org/news/2014-06-turing-success-milestone-history.html

[7.] Facebook.com, Help Center: What names are allowed on Facebook?. In: [online]. [cit.1.9.2020]. Dostupné z: https://www.facebook.com/help/112146705538576

[8.] Guide to Good Practice on the Use of Video-Link under the Evidence Convention. The Hague Conference on Private International Law – HCCH Permanent Bureau. 2020. [online]. [cit.1.9.2020]. Dostupné z: https://assets.hcch.net/docs/569cfb46-9bb2-45e0-b240-ec02645ac20d.pdf

[9.] ICANN Lookup: About WHOIS. 2019. Internet Corporation for Assigned Names and Numbers. [online]. [cit. 1.9.2020]. Dostupné z: https://whois.icann.org/en/about-whois

[10.] ICANN: List of Approved Dispute Resolution Service Providers. [online]. [cit. 21.7.2020]. Dostupné z: https://www.icann.org/resources/pages/providers-6d-2012-02-25-en

[11.] NB: Soubor odpovědí na dotazy související s regulací ochrany proti zneužívání trhu a transparentností, 28. 11. 2018. [Online]. [cit.1.9.2020]. Dostupné z: https://www.cnb.cz/cs/casto-kladene-dotazy/Soubor-odpovedi-na-dotazy-souvisejici-s-regulaci-ochrany-proti-zneuzivani-trhu-a-transparentnosti-28.-11.-2018/

[12.] PACER: Public Access to Court Electronic Records [online]. [cit. 1.9.2020]. Dostupné z: https://www.pacer.gov/psc/hfaq.html

[13.] Právo ozbrojeného konfliktu a jeho uplatňovanie vo vojenských operáciách. In: Ozbrojené sily Slovenskej republiky: Konferenční príspevok [online]. 2010 [cit.1.9.2020]. Dostupné z: www.mil.sk/data/att/11772_subor.ppt

[14.] PWC Česká Republika, s.r.o. Forenzní služby: eDiscovery [online]. [cit.1.9.2020]. Dostupné z: http://www.pwc.com/cz/cs/forenzni-sluzby/assets/pwc-vyhledavaci-technologie.pdf

[15.] RECAP US Federal Court Documents. Dostupné z: https://archive.org/details/usfederalcourts

[16.] Request for user information. Legal process. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/legalprocess/

[17.] Rozhodčí centrum pro spory o domény .CZ: Rozhodčí soud při HK ČR a AK ČR. [online]. [cit. 21.7.2020]. Dostupné z: http://domeny.soud.cz/adr/decisions/index.php

[18.] Swiss Re Corporate Solutions joins forces with IBM to offer cyber risk protection. [Online]. [cit.1.9.2020]. Dostupné z: http://www.swissre.com/corporate_solutions/Swiss_Re_Corporate_Solutions_joins_forces_with_IBM_to_offer_cyber_risk_protection.html

[19.] Štandardy ISO. Viď ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. [online]. [cit.1.9.2020]. Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=44381

[20.] Transparency report. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2020. [online]. [cit.1.9.2020]. Dostupné z: http://en.wikipedia.org/wiki/Transparency_report

[21.] Viď napríklad Sociální sítě nejsou jen Facebook. Podívejte se i na ty české. iDnes.cz. MAFRA, a. s. [online]. [cit.1.9.2020]. Dostupné z: https://www.idnes.cz/technet/internet/socialni-site-nejsou-jen-facebook-podivejte-se-i-na-ty-ceske.A091017_234210_tec_reportaze_vse

[22.] Videokonferencia ako súčasť európskej e-spravodlivosti: základy videokonferencie v cezhraničných konaniach. 2009. [online]. [cit.1.9.2020]. Dostupné z: https://e-justice.europa.eu/fileDownload.do?id=f26030b3-ae25-4d08-825f-05152d7bb772

[23.] Vzorové podanie na ÚS SR vo veci plošného sledovania občanov. In: European Information Society Institute. [online]. [cit.1.9.2020]. Dostupné z: https://www.eisionline.org/images/finish%20-%20podanie%20na%20ussr.pdf

[24.] What lies behind the JPMorgan Chase cyber-attack. The Economist. [Online]. [cit.1.9.2020]. Dostupné z: http://www.economist.com/news/business-and-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itself-what-lies-behind

[25.] Informácie o transparentnosti. Žiadosti od vládnych orgánov a súdov. Google Inc. [online]. [cit.1.9.2020]. Dostupné z: https://transparencyreport.google.com/user-data/overview?hl=en

[26.] Jak na internet. CZ.NIC, z.s.p.o. Doména, IP adresa, DNS [online]. [cit.1.9.2020]. Dostupné z: http://www.jaknainternet.cz/page/1261/domena,-ip-adresa,-dns/

[27.] Common Vulnerabilities and Exposures (CVE®). [Online]. [cit.1.9.2020]. Dostupné z: https://cve.mitre.org/about/

[28.] ESMA. Esma extends its operational-risk analysis. 13.4.2018. [Online]. [cit.1.9.2020]. Dostupné z: https://www.esma.europa.eu/press-news/esma-news/esma-extends-its-operational-risk-analysis

[29.] FINMA Guidance 05/2020 - Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA. Annex 1: Determining the severity of a cyber attack. [Online]. [cit.1.9.2020]. Dostupné z: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf?la=en

[30.] CZ.NIC, z. s. p. o. Domain Report 2020 [online]. [cit.1.9.2020]. Dostupné z: https://stats.nic.cz

[31.] Facebook Developers. [online]. [cit.1.9.2020]. Dostupné z: https://developers.facebook.com

[32.] Google Transparency Report. [online]. [cit.1.9.2020]. Dostupné z: https://policies.google.com/terms/information-requests

[33.] Goverment requests report. Facebook Inc. [online]. [cit.1.9.2020]. Dostupné z: https://transparency.facebook.com/government-data-requests/jul-dec-2019

[34.] IBM Watson. Ibm.com.[online]. [cit.1.9.2020]. Dostupné z: https://www.ibm.com/watson

[35.] Our Transparency Report. LinkedIn Inc. [online]. [cit.1.9.2020]. Dostupné https://about.linkedin.com/transparency/government-requests-report#government-requests-2019-2017

[36.] US Army Commercial Targets Video Gamers. In: YouTube [online]. [cit.1.9.2020]. Dostupné z: http://www.youtube.com/watch?v=HU1y1G6uzAI

[37.] WIPO: Alternative dispute resolution. [online]. [cit.1.9.2020]. Dostupné z: http://www.wipo.int/amc/en/domains/search/index.html