Univerzita Palackého v Olomouci
Právnická fakulta

Kristýna Zábojníková

Mezinárodní závazky států v kybernetickém prostoru v kontextu lidských práv

Diplomová práce

Olomouc 2021

Prohlašuji, že jsem diplomovou práci na téma Mezinárodní závazky států v kybernetickém prostoru v kontextu lidských práv vypracovala samostatně a citovala jsem všechny použité zdroje.

V Olomouci dne 30. června 2021 ……..

Kristýna Zábojníková

Tímto bych ráda poděkovala vedoucímu diplomové práce JUDr. Pavlovi Burešovi, Ph.D., za jeho odborné vedení, vstřícnost a podnětné rady k vypracování této diplomové práce. Ráda bych také poděkovala svým rodičům za jejich veškerou podporu a pomoc.

Obsah

Seznam použitých zkratek

ESLP	Evropský soud pro lidská práva
EU	Evropská unie
GGE	Skupina vládních expertů
ICT	Informační a komunikační technologie
MPHSKP	Mezinárodní pakt o hospodářských, sociálních a kulturních právech
MPOPP	Mezinárodní pakt o občanských a politických právech
MSD	Mezinárodní soudní dvůr
NATO	Severoatlantická aliance
Návrh	Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování
OEWG	Otevřená pracovní skupina
OSN	Organizace spojených národů
RLP	Rada OSN pro lidská práva
UNESCO	Organizace OSN pro vzdělání, vědu a kulturu
VDLP	Všeobecná deklarace lidských práv

Úvod

Lidská práva je pojem, pod který spadají veškerá práva a svobody osob inherentně zakotvena v naší lidskosti. Jejich význam rozeznává a respektuje většina států a společností, i přes složitý historický vývoj. Největší rozkvět těchto práv a svobod začal právě po druhé světové válce, po době, kdy svět zažil jejich porušování v takové míře, že docházelo až k nejzávažnějším zločinům pro lidskosti. Mezinárodní společnost se následně zavázala, že k takovému extrémnímu porušování lidských práv již nesmí nikdy dojít, a proto v následující letech bylo přijato několik úmluv pokrývajících ochranu širokého spektra práv od občanských po ekonomické.

Tyto úmluvy však vznikaly v době, kdy komunikační a informační technologie nevyjímaje internet byly neznámým pojmem. Tyto technologie a další programy se řadí pod kyberprostor, který se tak dá považovat za další oblast, kterou státy, jednotlivci, soukromé společnosti, nevládní organizace a další subjekty využívají mimo jiné ke komunikaci, získávání informací, šíření názorů a dalšímu uplatňování svých práv. Stejně tak jako je jednoduché využívat tyto technologie za výše zmíněným účelem, je jednoduché i jejich zneužití za účelem např. nezákonného sbírání dat, sledování, omezování svobody slova a dalšího porušování lidských práv. Hranice mezi jejich pozitivním a negativním využitím je velmi tenká. Vynalezením internetu a rozvojem nových technologií tak vznikly nové možnosti a příležitosti ale zároveň i hrozby.

Hlavním cílem práce bylo zmapování mezinárodních lidskoprávních závazků států v kyberprostoru. Za tímto účelem byly vymezeny následující otázky. A to, zdali dochází k aplikaci mezinárodního práva v kyberprostoru, na což pak navazuje otázka dodržování mezinárodních závazků států v kyberprostoru. Zbývající otázkou je vztah lidských práv a kyberprostoru, a to jak po stránce právní, tak praktické z pohledu incidentů, které se v minulých letech udály.

Dotyčné otázky budou zodpovězeny postupným definováním nezbytných náležitostí a zároveň pomocí analytického postupu v následujících kapitolách diplomové práce. Na úvod práce bude nezbytné vysvětlit pojem kyberprostoru, jelikož se jedná o termín technický. Následovat bude stručný přehled mezinárodních lidskoprávních závazků států, jenž bude mapovat jak právně závazné instrumenty,

tak dokumenty s doporučujícím charakterem, a to z širšího hlediska než jen z pohledu Mezinárodního paktu o občanských a politických právech.

Tato úmluva totiž bude předmětem třetí kapitoly, ve smyslu analýzy její aplikovatelnosti v kyberprostoru. Konkrétně bude rozebrána jurisdikce a přičitatelnost chování státu v kyberprostoru. Následující čtvrtá kapitola se zaměří na tři konkrétní lidská práva, jež jsou novými technologiemi nejvíce dotčena, a to právo na soukromí, právo na svobodu projevu a názoru, a právo na svobodu shromažďování a sdružování. V rámci této kapitoly bude analyzován rozsah těchto práv v kyberprostoru a podrobně rozebrán dopad technologií na jejich vykonávání, včetně současné diskuze o vzniku nového práva na přístup k internetu. Poslední kapitola se pak bude věnovat problematickým otázkám v kyberprostoru, ve smyslu potřeby vzniku právně závazného dokumentu, či definování kyberprostoru jako mezinárodního prostoru. Právě pomocí posledních dvou kapitol bude formována odpověď na druhou výzkumnou otázku, zda státům plynou mezinárodní závazky pro kyberprostor.

Kyberprostor a lidská práva je obecně velmi mladé téma jak ve společnosti, tak v právu. Nebylo proto jednoduché nalézt mnoho zdrojů, ze kterých by se dalo vycházet. A to jak po akademické, právní či judikátní stránce. V současné době zatím neexistuje žádná mezinárodní smlouva, která by upravovala kyberprostor a lidská práva či kyberprostor obecně. V právně závazné rovině lze najít pouze výklad Výboru pro lidská práva, jenž svými dokumenty rozšiřuje vybrané články Mezinárodního paktu o občanských a politických právech. Poměrně širší spektrum dokumentů lze najít na nezávazné úrovni. V tomto případě se pak jedná o zprávy pracovních skupin pod 1. Výborem VS OSN nebo rezoluce jak Rady OSN pro lidská práva, tak Valného shromáždění OSN. K této skupině lze přiřadit také velké množství zpráv lidskoprávních expertů OSN.

Nadále pak bylo vycházeno převážně z elektronicky přístupných odborných článků různých expertů. Po akademické stránce byly využity převážně učebnice Mezinárodního práva veřejného. Kvůli nedostatku publikací specificky zaměřených na lidská práva a kyberprostor docházelo k aplikaci obecných publikací k veřejnému mezinárodnímu právu na tuto konkrétní oblast. Podobný princip se pak uplatnil i při využívání judikatury k jiné problematice. Široce byly využity rozsudky MSD. K ilustraci teoretických znalostí posloužily internetové stránky mapující události ve světě a zprávy neziskových organizací. Po právní stránce se hojně využil

Mezinárodní pakt o občanských a politických právech, a na národní úrovni, k porovnání, pak Listina základních práv a svobod. Převážná většina zdrojů pochází ze zahraničí, bohužel v české odborné literatuře se prozatím nenachází dostatečný počet publikací k této problematice.

1. Kybernetický prostor

1.1. Kyberprostor a technologie

Kyberprostor je abstraktní pojem, jedná se o nefyzickou doménu vytvořenou počítačovými systémy, jež poskytuje lidem prostor pro komunikaci, vyměňování si informací a sběr dat.[1] V rámci kyberprostoru můžeme narazit na pojem informační a komunikační technologie (*Information and Communication Technologies*, „ICT"), pod který se řadí *„počítače, počítačové sítě a systémy, distribuční a dodací pozemní či podmořské kabely, satelity, telefony a televize"*[2].

Kyberprostor pak poskytuje těmto technologiím místo pro jejich „*vytvoření, uložení, upravování, výměnu a využívání informací skrze závislé a propojené sítě pomocí informačních komunikačních technologií*"[3].

Důležité je také zmínit roli internetu. Často bývá zaměňován s pojmem kyberprostor, jedná se však pouze o jednu z globálních technologických platforem. Představuje síť propojující milion počítačů[4], která zahrnuje více funkcí a úkolů, které pak využívají různí aktéři, ať už ze soukromé či státní sféry.[5] Internet má i fyzickou dimenzi, a to díky propojení různých počítačových systémů a jejich přístupnosti a přenosu informací z jednoho na druhého standardními internetovými protokoly (*Internet Protocol*). Zároveň se jedná o velmi důležitou platformu, na které se v dnešní době realizují aktivity týkající se států i jednotlivců, ať už se jedná o ekonomické záležitosti, veřejnou bezpečnost, činnost občanské společnosti či záležitosti národní bezpečnosti.[6]

Tallinnský manuál, nezávazný dokument vypracovaný skupinou odborníků na kybernetické otázky, definuje kyberprostor jako *„prostředí tvořené fyzickými a nefyzickými komponenty, charakteristické užíváním počítačů a elektromagnetickým spektrem k ukládání, úpravě, a výměně dat pomocí počítačových sítí."*[7] Pro kontext a srovnání s mezinárodní úpravou se můžeme na definici kyberprostoru podívat

[1] TSAGOURIAS, Nicholas, BUCHAN, Russell. *Research handbook on international law and cyberspace*. Cheltenham, UK, Northampton, MA: Edward Elgar Publishing, 2017, s. 55.
[2] Zpráva UNIDIR z roku 2017, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, s. 7.
[3] Tamtéž.
[4] TSAGOURIAS: *Research handbook…,* s. 55.
[5] Zpráva UNIDIR z roku 2017: *The United Nations…,* s. 7.
[6] TSAGOURIAS: *Research handbook…,* s. 57.
[7] SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013, s. 258.

z národního hlediska. Český právní systém dle § 2 písmena a) zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, vymezuje kyberprostor jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“[8].

1.2. Kybernetická bezpečnost

Kybernetická bezpečnost je snaha zajištění bezpečnosti výše uvedených technologií ICT od neautorizovaných přístupů, nebo pokusů o přístup, a ohrožení tak důvěrnosti, integrity, a přístupnosti těchto technologií. Pod pojmem neautorizovaného přístupu je myšlena přítomnost cizího prvku, tedy úmyslné hrozby jako je například sabotáž či zničení, přičemž tento negativní dopad musí být vyloučen ze strany vnitřních chyb, či způsobením problémy počítačového systému. Do kybernetické bezpečnosti taky nespadají problémy spojené s obsahem komunikačních technologií.[9]

Pod zajišťování bezpečnosti ICT spadá i jejich vliv na lidská práva, která jsou vývojem a vlivem technologií silně ovlivněna.

„*Teoreticky lidská práva fungují nezávisle na jakékoliv technologii. Ve skutečnosti však technologie ovlivňují jak a jestli jedinci mají lidská práva zaručena.*“[10] Lidská práva jsou nejen provázána mezi sebou ale i mezi vývojem dané země, to se tím spíš týká vývoje technologií, který v dnešní době hraje významnou roli v rozvoji dané zemi.[11]

Internet, jako prostor pro realizaci v kyberprostoru, je jeden z nejvýznamnějších komunikačních pokroků vznikajících v době lidských práv. Význam internetu pro lidská práva je nejen v jeho načasování ale i v jeho funkčnosti a schopnostech jako takových.[12]

To můžeme vidět například u rozvojových zemí, kde v určitých částech není zavedený ani internet, díky kterému se lidé mohou lépe vzdělávat a posouvat se tak směrem k vyšší úrovni života, nehledě na to, že pomocí internetu a různých platforem získávají informace o aktuálním dění jak v jejich zemi, tak v zahraničí

[8] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
[9] Zpráva UNIDIR z roku 2017: *The United Nations*…, s. 7.
[10] TSAGOURIAS: *Research handbook*…, s. 95.
[11] Tamtéž.
[12] Tamtéž, s. 94.

a zároveň mohou i vyjadřovat své názory, čímž se od sociálních práv dostáváme k právům občanským.

Kromě významu pro občanskou společnost a úroveň lidských práv ve světě má vznik internetu dopad i na ochranu lidských práv, a lidskoprávní instituce a mechanismy. Kyberprostor je výzvou pro aplikaci principů mezinárodního práva důležitých pro lidská práva. Jedná se především o suverenitu, nevměšování se, a určování jurisdikce.[13] Nepopiratelný dopad kyberprostoru na lidská práva způsobil, že článek 19 MPOPP se vykládá i ve prospěch práva na informace a přístupu k internetu.[14]

[13] TSAGOURIAS: *Research handbook*…, s. 94.
[14] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 6. dubna 2018, A/HRC/38/35.

2. Stručný přehled mezinárodněprávních závazků států

2.1. Právně závazné instrumenty

2.1.1. Aplikace mezinárodního práva v kyberprostoru

Mezinárodní smlouvy a obyčeje upravují různé prostory[15] na planetě. Jelikož je však kyberprostor poměrně nová oblast nejen pro právo, ale i pro společnost, zůstává otázkou, jak k němu přistupovat z právního, společenského a politického hlediska.

Na mezinárodní úrovni mezi právně závazné prameny práva řadíme především mezinárodní smlouvy. Obsah těchto smluv je univerzálně rozeznávaný a přijatý ve společnosti.[16] Na mezinárodní úrovni nejsou žádné mezinárodní smlouvy, které by výlučně upravovaly kyberprostor a lidská práva. To nicméně není žádný problém, protože zde máme poměrně širokou mezinárodní úpravu lidských práv, jejichž aplikovatelnost se výkladem dá rozšířit, tak aby odpovídala aktuálním problémům.

V oblasti lidských práv se převážně jedná o dokumenty tzv. International Human Rights Bill, který obsahuje právně závazný Mezinárodní pakt o občanských a politických právech (*International Covenant on Political and Civil Rights*, „MPOPP“) a Mezinárodní pakt o hospodářských, sociálních a kulturních právech (*International Covenant on Economic, Social and Cultural Rights*, „MPHSKP“).

Obecná aplikace mezinárodního práva v kyberprostoru již v dnešní době politického konsenzu napříč státy dosáhla, avšak to, jakým způsobem a v jakém rozsahu se mezinárodní právo aplikuje, nadále zůstává předmětem složitých mezinárodních debat.[17] Přestože velké množství odborníků[18] už k tomu svá stanoviska vydalo.

---

[15] Různými prostory se myslí zemský povrch, zemské nitro a mimozemské prostory, dle DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. vydání. Praha: Leges, 2011. s. 291. Více v kapitole 5.2 této práce.

[16] SMITH, Rhona K.M. *Textbook on international human rights*. Oxford, New York, N.Y.: Oxford University Press, 2010, s. 44.

[17] Například během vyjednávání zprávy OEWG, blíže ITTELSON, Pavlina, RADUNOVIC, Vladimir. *What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis* [online]. Diplo, 19. března 2021 [cit. 23. května 2021]. Dostupné na <https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis>. Nebo při vyjednávání GGE skupiny k přijetí zprávy v roce 2017, blíže VÄLJATAGA, Ann. *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly* [online]. CCDCOE, [cit. 23. května 2021]. Dostupné na <https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>.

[18] Jedná se například o zprávy GGE z roku 2013 a 2015, blíže na *Developments in the field of information and telecommunications in the context of international security* [online]. UNODA, [cit. 22.

Politickou shodu států na aplikaci mezinárodního práva v kyberprostoru můžeme najít vyjádřenou mimo jiné v rezolucích Valného shromáždění OSN a Rady OSN pro lidská práva. Po odborné stránce pak existuje plno zpráv expertů zvláštních procedur OSN, které mapují dopad nových technologií na lidská práva, tomu se pak věnuje čtvrtá kapitola této práce. V právně závazné rovině můžeme vycházet z obecných komentářů Výboru pro lidská práva, které rozšiřují výklad MPOPP.

2.1.2. Praktické příklady dopadů nových technologií

To, že je potřeba klást důraz na dosažení konsenzu ohledně aplikace mezinárodního práva, a zvláště v jeho dodržování v kyberprostoru, potvrzují četné případy hackerských útoků, které zásadně zasahují do práv a svobod všech jednotlivců. Hackerské útoky mimo jiné mohou způsobit ztrátu dat či poškodit vnitřní servery a systémy počítačů napadených subjektů. Kromě toho, že se tyto útoky odehrávají v soukromé rovině, stále více k nim dochází i ve státní sféře, nezávislých médií nebo orgánech regionálních či mezinárodních organizací.

Jako příklad z nedávné doby slouží například útok na vnitřní systémy státních orgánů Spojených států amerických, kdy došlo k masivnímu úniku dat z několika nejen vládních orgánů.[19] Ačkoliv nedošlo k přímému ohrožení lidských práv a mohlo se jednat pouze o zásah do soukromí skrze získání interních dat, je jen otázkou času, kdy podobné útoky budou mít mnohem vážnější následky.

To můžeme vidět i na častých a opakujících se hackerských útocích na kritickou infrastrukturu, mezi něž patří i nemocnice. V poslední době se jedná například o kybernetický útok na nemocnici v německém Düsseldorfu. Tento útok se řadí mezi ty, které se nejvíce přiblížili k tragickému následku, ve smyslu ztráty na životě jedince.

Nemocnice byla v září 2020 napadena hackerským útokem, který ji znepřístupnil vnitřní systémy, což vedlo k dočasnému pozastavení její činnosti. Nemocnice musela po určitou dobu přesměrovávat akutní případy do jiných spádových zdravotnických zařízení. Tato změna se konkrétně dotkla pacientky, jež

---

května 2021]. Dostupné na <https://www.un.org/disarmament/ict-security/>. Nebo Tallinnský manuál, blíže SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013. 282 s. Nebo například zprávy zvláštních zpravodajů OSN, více v kapitole 4 této práce.

[19] PAUL, Kari, BECKETT, Lois. *What we know – and still don't – about the worst-ever US government cyber-attack* [online]. The Guardian, 19. prosince 2020 [cit. 22. února 2021]. Dostupné na <https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government>.

byla v danou chvíli převážena sanitkou, která byla přesměrována do jiné nemocnice.[20] Pacientka následně zemřela. V návaznosti na tento vývoj docházelo ke spekulacím, zda mezi těmito dvěma skutečnostmi existuje příčinná souvislost či nikoliv. Hrozilo, že při prokázání kauzality, se bude jednat o první případ, kdy by v důsledku kybernetického útoku, došlo ke ztrátě na životě civilní osoby. Vyšetřování však nakonec neprokázalo příčinnou souvislost mezi těmito dvěma událostmi.[21]

2.2. Prameny doporučujícího charakteru

V oblasti lidských můžeme vycházet ze Všeobecné deklarace lidských práv („VDLP“). Jedná se však o pouhé doporučení, které slouží spíše jako morální a politický závazek států, přestože její některá ustanovení by se z pohledu mezinárodního práva daly vykládat jako principy či dokonce jako pravidla obyčejové povahy.[22] Význam VDLP leží spíše než v její právní závaznosti v základu pro vytvoření dalších dvou už zmíněných mezinárodních úmluv. MPOPP a MPHSKP jsou již ze své povahy právně závazné a státy, jež jsou jejich členy, jsou povinny dodržovat jejich obsah.

Otázkou kyberprostoru a mezinárodního práva na mezinárodní úrovni se státy začaly zabývat v roce 1998, kdy Rusko předložilo 1. Výboru VS OSN rezoluci A/RES/53/70, následně schválenou konsenzem. Na základě této iniciativy se zmíněná problematika zařadila do agendy OSN. Později pak, na základě rezoluce A/RES/58/32, vznikla v roce 2004 skupina vládních expertů (*Groups of Governmental Experts*, „GGE“), jejíž agendou bylo monitorovat a studovat hrozby informačních a komunikačních technologií v kontextu mezinárodní bezpečnosti, a navrhovat, jak k těmto hrozbám přistupovat.[23]

Zásadní jsou zprávy GGE vydané a přijaté konsenzem v roce 2013 a 2015. Zpráva z roku 2013 jako první stanovila, že mezinárodní právo a normy z něj vyplývající se v kyberprostoru aplikují, a jsou nezbytné k udržení míru, stability

[20] TIDY, Joe. *Police launch homicide inquiry after German hospital hack* [online]. BBC, 18. září 2020 [cit. 22. února 2021]. Dostupné na <https://www.bbc.com/news/technology-54204356>.
[21] O'NEILL, Patrick Howell. *Ransomware did not kill a German hospital patient* [online]. MIT Technology Review, 12. prosince 2020 [cit. 22. února 2021]. Dostupné na <https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/>.
[22] SMITH, Rhona K.M. *Textbook on international human rights*. Oxford, New York, N.Y.: Oxford University Press, 2010, s. 37.
[23] *Developments in the field of information and telecommunications in the context of international security* [online]. UNODA, [cit. 22. února 2021]. Dostupné na <https://www.un.org/disarmament/ict-security/>.

a k prosazování otevřeného, bezpečného, pokojného a dostupného prostředí informačních a komunikačních technologií. Dále zpráva zmiňuje, že chování států v kyberprostoru nebo aktivity na území spadající pod jejich jurisdikci se musí řídit principy mezinárodního práva včetně principu suverenity. Zároveň veškeré podniknuté kroky pro udržení bezpečnosti v kyberprostoru musí být v souladu s lidskými právy a základními svobodami stanovenými ve Všeobecné deklaraci lidských práv a v Chartě OSN.[24]

Následující zpráva vydaná v roce 2015 navazuje na závěry předchozí skupiny a klade důraz na dodržování lidskoprávních smluv včetně respektování rezolucí Rady OSN pro lidská práva („RLP“) při zajišťování bezpečnosti v kyberprostoru. Zvláště pak zmiňuje rezoluce týkající se práva na soukromí a práva na svobodu projevu. Významný posun oproti zprávě z roku 2013 je pak ve stanovení doporučení v otázce aplikace mezinárodního práva, jeho norem, a principů v kyberprostoru. Ze zprávy vyplývá, že státy mají jurisdikci nad ICT umístěnými na svých územích, a při jejich využívání musí brát ohled nejen na své mezinárodní závazky[25] ale také na „*suverenitu států, pokojné řešení mezinárodních sporů…, zdržení se užití síly vůči územní integritě nebo politické nezávislosti států…, respektování lidských práv a základních svobod, a nevměšování se do vnitřních záležitostí jiných států.“*[26]

Kromě vzniklé GGE pod záštitou 1. Výboru VS OSN vznikla také v roce 2018 otevřená pracovní skupina (*Open-ended Working Group*, „OEWG“), která řeší úplně stejnou agendu jako GGE. Rozdíl mezi těmito skupinami je v účasti států na procesu, v OEWG jsou zapojeny všechny státy na rozdíl od GGE. První zpráva této skupiny vyjde teprve během roku 2021.

Problém u rezolucí Rady OSN pro lidská práva, kterých k tomuto tématu v posledních letech přibývá čím dál tím více, spočívá v tom, že se jedná o právně nezávazná doporučení, která mají většinou pouze politický význam.[27] Na druhou stranu díky jejich politické závaznosti je státy respektují a podřizují se tak vytvořenému nátlaku k podniknutí kroků v souladu s jejich obsahem.[28] Rezoluce jsou vnímány také jako morální odraz společnosti.

---

[24] Zpráva skupiny vládních expertů ze dne 24. června 2013, A/68/98, odst. 16-25.
[25] Zpráva skupiny vládních expertů ze dne 22. července 2015, A/70/174, odst. 24-29.
[26] Tamtéž, odst. 26.
[27] ONDŘEJ, Jan, MRÁZEK Josef, KUNZ Oto. *Základy mezinárodního práva veřejného*. Praha: C.H. Beck, 2018. s. 31.
[28] DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. vydání. Praha: Leges, 2011. s. 220.

Rezoluce RLP pokrývají široké množství lidských práv v kontextu kyberprostoru a digitálního světa. Převážně se zaměřují na ochranu občanských a politických práv jako je právo na svobodu projevu a názoru (A/HRC/RES/44/12), právo na pokojné shromažďování a sdružování (A/HRC/RES/44/20) nebo právo na soukromí (A/HRC/RES/42/15).

Právo na soukromí jako jediné z těchto výše zmíněných práv je také předmětem samostatných rezolucí ve 3. Výboru VS OSN, což naznačuje zájem všech států OSN na ochraně tohoto práva. Je nutno podotknout, že všechny rezoluce byly přijaty konsenzem, tudíž na jejich obsahu panuje mezi státy shoda, což je pro budoucí vynucování či dodržování z politického hlediska výhodou.

3. Mezinárodní pakt o občanských a politických právech

Jak je zmíněno výše, státy jsou povinny dodržovat své mezinárodní závazky. Jedny z těchto závazků vyplývají i z Mezinárodního paktu o občanských a politických právech. Smlouva vstoupila v platnost v roce 1976 a k dnešnímu datu čítá 173 smluvních stran. Můžeme tedy říct, že ochranu práv a svobod v ní obsaženou se zavázaly dodržovat téměř všechny státy světa.

MPOPP je smlouva, která zajišťuje ochranu práv jednotlivců *„každý stát, který je smluvní stranou Paktu, se zavazuje respektovat práva uznaná v tomto Paktu a zajistit tato práva všem jednotlivcům na svém území a podléhajícím jeho jurisdikci, bez jakéhokoli rozlišování podle rasy, barvy, pohlaví, náboženství, politického nebo jiného smýšlení, národnostního nebo sociálního původu, majetku, rodu nebo jiného postavení.“*[29]

Těžší je to ovšem s oblastí kyberprostoru a dodržování těchto povinností v její rovině. Otázka, zda se lidská práva aplikují i online už je sice dávno překonaná, přesto ale stále nemáme žádný dokument, který by byl právně závazný a zavazoval by tak státy k dodržování mezinárodních závazků i v této oblasti.

Na rozdíl od absence právně závazných dokumentů, lze na mezinárodním poli nalézt poměrně velké množství politických stanovisek a dokumentů, které jasně stanovují, že lidská práva platí jak online tak offline. Jedná se například o rezoluci Rady OSN pro lidská práva z roku 2018 (A/HRC/RES/38/7), která v prvním odstavci *„potvrzuje, že právům, která lidi mají offline, musí být zajištěna stejná ochrana i v online prostředí“*[30].

Aplikaci lidských práv v online prostředí potvrdily i státy NATO v rámci Summitu ve Varšavě v roce 2016.[31] I skupina států G7 na Summitu v Deauville v roce 2011 se shodla na tom, že při zavádění internetu musí být brány v potaz také lidskoprávní závazky států, které jsou páteří demokratické společnosti a nárokem všech lidí.[32] Přestože na těchto názorech panuje mezi státy shoda, nelze je bohužel považovat za prameny práva pro jejich nezávazný charakter.

[29] Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2, čl. 2
[30] Rezoluce Rady OSN pro lidská práva ze dne 17. července 2018, A/HRC/RES/38/7
[31] *Warsaw Summit Communiqué* [online]. NATO, 9. července 2016 [cit. 22. března 2021]. Dostupné na <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.
[32] *G*8 Declaration – Renewed Commitment For Freedom And Democracy [online]. NATO [cit. 22. března 2021]. Dostupné na

3.1. Podmínky dodržování MPOPP v kyberprostoru

Proto, abychom se mohli začít bavit o ochraně lidských práv v kyberprostoru a o dodržování předmětné smlouvy, je potřeba abychom si vymezili základní podmínky pro její aplikaci. Jako první požadavek, a jeden z nejjednodušších je, aby daný stát byl smluvní stranou smlouvy. To nám nicméně stanoví již výše zmíněný čl. 2 MPOPP. Vzhledem k tomu, že většina států světa je smluvní stranou smlouvy, není v tomto směru potřeba hlubší analýzy.

Tím, že se stát stane smluvní stranou se automaticky zaváže k zajištění práv uvedených ve smlouvě všem jednotlivcům na jeho území a taktéž i těm, kteří se nachází mimo jeho území ale současně spadají pod jeho jurisdikci.[33]

Právě otázka jurisdikce a s tím související přičitatelnost chování jiných subjektů státům se jeví jako problematická v kontextu kyberprostoru. Nejasnost vymezení kyberprostoru a jeho zjevná abstraktnost, spolu s rychlým vývojem v této oblasti, ztěžuje určení právního rámce.

3.2. Jurisdikce

Jurisdikce je úzce spjata se suverenitou. Suverenita jako taková je však spojena s územím daného státu a představuje nezávislost státní moci jak uvnitř, tak navenek, a jurisdikce je jedním z prostředků, jak ji uplatňovat. Jedná se tedy o její podmnožinu.[34]

Přesná definice jurisdikce se v různých českých učebnicích mezinárodního práva veřejného[35] lehce rozchází, jisté však je, že jurisdikce narozdíl od suverenity, představuje užší definici nezávislého výkonu státní moci.[36]

Pro srovnání se můžeme na definici jurisdikce podívat i pohledem zahraničního autora, který vidí jurisdikci jako zásadní a ústřední prvek státní suverenity, poněvadž se jedná o výkon moci, který může změnit, založit či ukončit právní vztahy a závazky. Výkon moci se provádí prostřednictvím zákonodárných, výkonných či soudních opatření.

<https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf>.

[33] *International human rights law* [online]. Dostupné na <https://cyberlaw.ccdcoe.org/wiki/International_human_rights_law>.

[34] ONDŘEJ, Jan, MRÁZEK Josef, KUNZ Oto. *Základy mezinárodního práva veřejného*. Praha: C.H. Beck, 2018. s. 88.

[35] Srovnání DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou. 2. vydání*. Praha: Leges, 2011. 448 s.; ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. Praha: C.H. Beck, 2018. 549 s.; ONDŘEJ, Jan, MRÁZEK Josef, KUNZ Oto. *Základy mezinárodního práva veřejného*. Praha: C.H. Beck, 2018. 271 s.

[36] ONDŘEJ: *Základy mezinárodního…,* s. 88.

Přestože je jurisdikce primárně spojována s územím státu, může být založena i na jiných důvodech, jako je například státní příslušnost, to se však netýká jejího vynucování, jež je omezeno územím státu.[37]

Jurisdikci dělíme podle jejího způsobu výkonu na teritoriální, personální či univerzální. Každý z uvedených druhů má svá specifická kritéria, za kterých je možná jeho aplikace. Jurisdikce spjatá s aplikací MPOPP je převážně dvojího druhu teritoriální a personální.

3.2.1. Teritoriální jurisdikce

Územní jurisdikce je provázena principem teritoriality, na jehož základě může stát nejen vykonávat jurisdikci nad činy spáchanými na jeho území ale i uplatňovat svou suverénní moc.[38] Typické pro teritoriální neboli územní jurisdikci je její propojení s územní suverenitou státu, která se vyjadřuje hranicemi daného státu.

Ochrana práv a svobod stanovených v MPOPP musí být zajištěna všem jednotlivcům na jejich území. Obecný komentář č. 31, odst. 10 Výboru pro lidská práva to dále upřesňuje a stanovuje, že *„…všem jednotlivcům se myslí nejen občanům státu ale i dalším osobám bez ohledu na národnost nebo státní příslušnost, čímž se myslí žadatelé o azyl, uprchlíci, migrační pracovníci a další osoby, které se nachází na území státu nebo spadají pod jeho výkon moci…“*[39].

3.2.2. Extrateritoriální jurisdikce

Extrateritoriální jurisdikce se dělí na personální a územní. Jedná se o výkon státní moci mimo hranice státu, který se váže na dodržování závazků státu vyplývajících z mezinárodních smluv. Tato jurisdikce je relevantní zejména v případě mezinárodních lidskoprávních smluv, jež se v zásadě aplikují extrateritoriálně.

V případě personální jurisdikce se jedná o výkon státní moci nad jednotlivci nacházejícími se převážně mimo území daného státu. Personální jurisdikce působí samozřejmě i na území příslušného státu, avšak v danou chvíli je upozaděna před jurisdikcí teritoriální.

Pro vznik je potřeba, aby mezi státem a jednotlivcem byl dostatečně úzký vztah, častým příkladem je, že konkrétní subjekt je občanem daného státu.[40] Mezi

[37] SHAW, Malcolm N. *International Law*. UK: Cambridge University Press, 2008. s. 645–646.
[38] RYNGAERT, Cedric. *Jurisdiction in International Law*. Oxford: New York, N.Y.: Oxford University Press, 2008. str. 42.
[39] Obecný komentář Výboru pro lidská práva ze dne 29. března 2004, CCPR/C/21/Rev.1/Add. 1326.
[40] RYNGAERT: *Jurisdiction in…,* s. 88.

dostatečně úzký vztah se ale také dále řadí například pracovněprávní vztah, příbuzenský vztah mezi rodiči a dětmi nebo provozování podnikatelské činnosti.[41]

V reálném případě to znamená, že i když se občan příslušného státu bude nacházet v zahraničí, tak ten stát jehož je občanem mu nesmí například zakázat vyjadřovat se v online prostředí k vnitřním či zahraničním záležitostem státu, protože by mu jinak omezil svobodu projevu, na kterou má dle mezinárodního práva právo.

Kromě personální jurisdikce, která se řadí mezi jeden z extrateritoriálních druhů, nesmíme zapomínat na území, která se nenachází v rozmezí hranic státu, ale stát na nich přesto vykonává svoji moc. V podstatě se jedná o stejný princip jako u personální jurisdikce, s tím rozdílem, že v tomto případě se jedná o území a ne o osoby.

Rozšířený výklad aplikace této smlouvy na daná extrateritoriální území můžeme znovu vyvodit z již zmíněného komentáře Výboru pro lidská práva z roku 2004 „*to znamená, že smluvní stát musí respektovat a zajišťovat práva stanovená ve smlouvě komukoli v rámci jurisdikce smluvního státu, i když se nenachází na jeho území.*“[42]

I v rámci extrateritoriální jurisdikce, týkající se území státu, nesmíme zapomínat na aplikaci MPOPP na všechny jednotlivce nacházející se na tomto území. To znamená, že pod výkon moci státu spadají všichni jednotlivci bez rozdílu, jak je definované Výborem pro lidská práva.[43]

Poslední oblastí, kterou jsme zatím nepokryli a která se také týká jurisdikce státu, je aktivita prováděná mimo jeho území. Dalo by se říci, že právě uznání dodržování lidských práv v souvislosti s těmito aktivitami je nejvíce kontroverzní. Pokud by došlo k jeho potvrzení na základě právně závazného instrumentu, znamenalo by to pro státy větší kontrolu a omezení jejich aktivit.

Okrajově tento teoretický přístup převedl do praxe Mezinárodní soudní dvůr („MSD“), jenž navázal na výklad Výboru pro lidská práva poradním posudkem č. 131 ze dne 9. července 2004. Ačkoliv se posudek týkal právních dopadů výstavby zdi na okupovaném palestinském území (*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*), soudní dvůr v něm stanovil pro výklad MPOPP důležité pravidlo. Ve čl. 111 potvrzuje, že kromě výše uvedených situací se

[41] Tamtéž.
[42] Obecný komentář Výboru OSN pro lidská práva ze dne 29. března 2004, CCPR/C/21/Rev.1/Add. 1326.
[43] Tamtéž.

„… aplikace MPOPP vztahuje i na aktivity státu prováděné mimo jeho vlastní území v rámci výkonu jeho státní moci“[44]*.*

I když se jedná pouze o poradní posudek, který sám o sobě není právně závazný, díky významnosti soudu má přesto vysokou politickou a morální váhu a je často využíván jako základ pro diplomatická jednání. Jeho účelem, mimo jiné, je také rozšiřování a konkretizování výkladu mezinárodního práva.

3.3. Přičitatelnost chování státu

S koncepcí jurisdikce státu a určení odpovědnosti za porušení mezinárodněprávních závazků plynoucích nejen z MPOPP je velmi úzce spojen i institut přičitatelného chování státu (*attribution*). A právě ten se jeví jako jeden z nejvíce problematických v praktické rovině.

Velký počet států se distancuje od aplikovatelnosti přičitatelnosti v kyberprostoru, protože jejím potvrzením by mohlo dojít k omezení aktivit států v kyberprostoru, a tudíž k ukončení některých jejich praktik, která můžou zasahovat do lidských práv. Příklady takových zásahů jsou uvedeny ve čtvrté kapitole.

Přičitatelné chování státu je jednou z podmínek odpovědnosti za mezinárodně protiprávní chování státu, která je částečně kodifikovaná v Návrhu článků o odpovědnosti státu za mezinárodně protiprávní chování (*Responsibility of States for Internationally Wrongful Acts*, „Návrh“) přijatým Komisí OSN pro mezinárodní právo v roce 2001.[45]

Obecné podmínky stanovení přičitatelnosti nám plynou z výše zmíněného Návrhu ve čl. 2: „*O mezinárodně protiprávní chování státu se jedná, jestliže chování spočívající v jednání nebo opomenutí: a) je státu podle mezinárodního práva přičitatelné, a b) představuje porušení mezinárodního závazku státu.*“[46]

Definici jednání nebo opomenutí není potřeba více rozvíjet pro účely této práce, stejně tak jako porušení mezinárodního závazku státu. Předmětné je ustanovení písmena a), které uvádí, že pokud je určité jednání či opomenutí státu jemu přičitatelné, tak se bude jednat, za předpokladu splnění ostatních podmínek, o protiprávní chování. Právě určení přičitatelnosti je stěžejní a je jí věnována celá druhá kapitola části první Návrhu.

---

[44] Poradní posudek Mezinárodního soudního dvora ze dne 9. července 2004, *Právní dopady výstavby zdi na okupovaném palestinském území*, čl. 131.
[45] DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. vydání. Praha: Leges, 2011. s. 326.
[46] Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování z roku 2001, čl. 2

3.3.1. Články 4–7 Návrhu

Podle článku 4 až 7 je stát odpovědný za chování státních orgánů, osob a entit, kteří vykonávají moc státu. Pod tuto definici se řadí orgány jakéhokoliv státního orgánu ať už při vykonávání legislativní, výkonné, soudní či jiné funkce. Dále se mu přičítá chování osob nebo entit, které vykonávají prvky státní moci, ale nejsou orgány státu dle předchozí definice. Chování orgánů jiného státu, které byly dány k dispozici jinému státu, se také přičítá k odpovědnosti státu, jemuž byl dán k dispozici. Za chování státu se taky považuje překročení pravomocí určitého státního orgánu nebo jeho jednání v rozporu se služebními příkazy.[47]

V tomto případě není potřeba další analýzy, jelikož se jedná o tzv. státní orgány de iure, a proto je jejich chování v kyberprostoru jasně přičitatelné státu.

3.3.2. Články 8–11 Návrhu

V následujících článcích, tj. čl. 8 až 11 Návrhu, je upravena poněkud kontroverznější přičitatelnost státu, jelikož se týká nestátních aktérů a vyjmenovává případy za jakých okolností je za jejich chování stát odpovědný. Jedná se o chování státních orgánů de facto, tudíž osob nebo skupiny osob v případě, že je jejich chování řízené nebo kontrolované tímto státem či pokud určitá situace vyžaduje výkon státní moci, který však není státními orgány poskytnut z důvodu opomenutí či jejich nepřítomnosti. Dále se státu přičítá také chování povstaleckých či jiných hnutí, pokud se stanou novou vládou státu a v neposlední řadě je stát odpovědný za chování, které sám uzná a přijme za své.[48]

Stát zpravidla není odpovědný za chování nestátních aktérů, nicméně pokud dojde k naplnění k některých z výše uvedených prvků, tak se toto chování může státu přičítat.

3.3.3. Článek 8 Návrhu

V kontextu kyberprostoru je nejčastěji zmiňovaný článek 8 Návrhu, který zní: „*Chování osoby nebo skupiny se považuje za chování státu podle mezinárodního práva, pokud osoba nebo skupina osob ve skutečnosti jednají podle pokynů tohoto státu, nebo je jejich chování tímto státem řízeno nebo kontrolováno.“*[49]

Z článku vyplývají tři situace, kdy je chování nestátního aktéra připisováno státu. Buďto určitá osoba nebo skupina osob jednají podle pokynů státu, nebo je

[47] Tamtéž, čl. 4–7
[48] Tamtéž, čl. 8–11
[49] FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 1, Dokumenty.* Praha: Leges, 2015, s. 298.

jejich chování řízeno, či kontrolováno daným státem. V minulosti byly tyto tři prvky zaměňovány, používány jako synonyma nebo považovány za kumulativní podmínky. To se však postupným vývojem výkladu práva změnilo, a v dnešní době jsou vnímány alternativně.[50]

3.3.4. Chování podle pokynů státu

První prvek, jednání podle pokynů státu, značí, že se stát rozhodne zapojit do určité situace a vydá pokyny nestátnímu aktéru, aby tak za něj konal. Důležité v tomto kontextu je, aby ten aktér, který za stát jedná, nevykonával státní moc, potom by totiž tohle chování spadalo pod články v první části druhé kapitoly Návrhu.[51]

Další podmínkou, která musí být naplněna, aby bylo dané chování možné přičíst státu, je *„potřeba faktické podřízenosti nestátního subjektu ve chvíli, kdy se stát rozhodne pro vykonání zamýšleného aktu*“[52]. Jako je například přijetí pokynů státu a jejich následné vykonání. Nicméně zde může nastat problém vágnosti daných pokynů, na což reaguje Mezinárodní soudní dvůr v rozsudku *Bosny a Hercegoviny v. Srbska a Černé Hory*, ve věci Bosenské genocidy, kde říká, že *„…pokyny státu musí být vydány za účelem dosažení požadovaného cíle konkrétní operace…“.*[53] Pokud by se jednalo pouze o obecné instrukce bez bližší specifikace, pak by následně vykonané chování nebylo dostatečně odůvodněné pro přičitatelnost státu. Nedostatečné je také sdílení stejného zájmu bez podniknutí dalších kroků, jako jsou například již uvedené pokyny.[54]

Dále je také potřeba, aby bylo možné zpětně prověřit, že daný akt je výsledkem pokynů, které vedou k původnímu zadavateli, v tomto případě konkrétnímu státu či jeho orgánu. Neznamená to, že musí být detailně vysvětlen každý krok, který by měl být podniknutý, ale určitý stupeň určitosti zde musí zůstat zachován. Mačák v článku uvádí, že tato konkretizace může koneckonců hrát i ve prospěch státu, ve smyslu vyhnutí se připsání chování, k němuž stát nevydal žádné pokyny, v případě širokého výkladu daných instrukcí. Nehledě na vágnost daných instrukcí, vždy musí být prokázána vůle státu k povolení spáchání takového aktu

---

[50] International Law Commission. *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001, s. 48. (čl. 8 Návrhu).
[51] MAČÁK, Kubo. Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict & Security Law,* 2016, roč. 21, s. 414.
[52] Tamtéž, s. 415.
[53] Rozsudek Mezinárodního soudního dvora z 26. února 2007, *Bosna a Hercegovina v. Srbsko a Černá Hora*, odst. 400.
[54] MAČÁK: *Decoding Article 8*…, s. 415.

chování. V případě excesu při postupování dle pokynů státu, nebude stát odpovědný za takové chování subjektu. Může se jednat například o odchýlení se od hlavního účelu zadaných instrukcí státem, kdy stát umožní přístup soukromé společnosti do jeho sítí za určitým účelem, a tato společnost by toho zneužila a napadla skrze tyto sítě jiný stát. [55]

Mačák dále uvádí příklad takového chování soukromého subjektu, které by státu bylo přičitatelné. Pokud by stát zadal konkrétní instrukce IT oddělení soukromé univerzity, aby provedla kybernetický útok na určitý cíl, bylo by toto jednání přičitatelné danému státu.[56]

3.3.5. Chování řízené státem

Druhým prvkem přičitatelnosti ve článku 8 Návrhu, je řízení státem. Pro jeho definici můžeme využít rozhodnutí Mezinárodního soudního dvoru ve věci Bosenské genocidy, který definuje řízení v případě kdy stát *„…poskytnul směr na jehož základě byl protiprávní akt proveden…“.*[57] Mačák v článku cituje slova advokáta Alaina Pelleta, jenž v této kauze vystupoval a který definoval pojem řízení jako „*méně přesný pojem než pokyny*“.[58]

Poskytnutí směru může znamenat pokračující fázi pokynů nebo vztah mezi státem a nestátním subjektem v tom smyslu, že i náznak nebo narážka na tento vztah může založit odpovědnost státu, jak například vysvětluje James Crawford.[59] Záhy ale dodává, že pochybuje, že samotný náznak nebo narážka na vztah mezi těmito aktéry by z pohledu států byl dostačující důkaz pro přičitatelnost. Klíčovým prvkem tedy bude skutečný vzájemný vztah. Jedná se například o situace, kdy stát fyzicky nevydá konkrétní pokyny k vykonání určitého chování, ale vzhledem k nerovnému vztahu daných subjektů, ve smyslu nadřízenosti státu a podřízenosti jednice či skupiny osob, a řízení chování tohoto soukromého subjektu státem, se bude dané chování a následný akt přičítat státu, jenž toto řízení vykonává.[60]

V praxi můžeme vidět aplikaci tohoto prvku přičitatelnosti například na známém případu napadení červem Stuxnet. Ačkoliv nedošlo k potvrzení

[55] Tamtéž, s. 416–417.
[56] Tamtéž, s. 415.
[57] Rozsudek Mezinárodního soudního dvora z 26. února 2007, *Bosna a Hercegovina v. Srbsko a Černá Hora*, odst. 406.
[58] MAČÁK: *Decoding Article 8*…, s. 417.
[59] MAČÁK: *Decoding Article 8*…, s. 413.
[60] Tamtéž, s. 418.

odpovědnosti konkrétního státu, lze zde vidět jak se článek 8 aplikuje na skutečné případy.

Stuxnet je název velmi propracovaného počítačového červa (*computer worm*), který využívá neznámých zranitelností systému Windows k infikaci počítačů a svému následnému šíření. Jeho účelem není pouze infikovat počítače, ale způsobit opravdové fyzické škody, které mají dopad v reálném světě. Převážně se zaměřuje na odstředivky neboli centrifugy, které pohání jaderné reaktory a používají se k výrobě obohaceného uranu.[61]

Poprvé byl objevený až v roce 2010, i když vznikl přibližně už o pět let dříve. Jeho objev se váže na známou kauzu pojmenovanou právě po jeho názvu. Účelem Stuxnetu pravděpodobně bylo zpomalení až zastavení vývoje jaderného vývoje v Íránu. Stuxnet se přes své unikátní naprogramování dostal pomocí fyzického USB zařízení do počítačů a způsoboval mnohem častější poškozování centrifugy[62], než by za normálního chodu bylo běžné. Toto poškozování vyústilo až ke stovkám až tisícům zlikvidovaných centrifug pro obohacování uranu, což Írán zasáhlo nejen po finanční stránce.[63]

Červa v počítačích íránské jaderné základny v Natanzu objevili techničtí specialisté v Bělorusku v roce 2010, při provádění kontroly z důvodu neustálého restartování počítačů. Po důkladnějším prozkoumání zjistili, že Stuxnet byl navržen tak, aby zároveň podával zprávy, že je všechno v pořádku, a mezitím operoval dál. Předpokládá se, že v počítačích působil rok až dva před jeho objevením. Po důsledném vyšetřování nebylo pochyb, že se jednalo o červa navrženého speciálně pro íránský jaderný program.[64]

V současnosti převažuje neoficiální tvrzení, že za tímto útokem údajně stojí USA spolu s Izraelem. Dokazují to dlouhodobé snahy o zastavení jaderného vývoje

---

[61] FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. CSO, 22. srpna 2017 [cit. 15. května 2021]. Dostupné na <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>.

[62] Centrifuga neboli odstředivka je rotační zařízení určené především k oddělování různě těžkých frakcí kapalin a plynů nebo k oddělování kapalin nebo plynů od pevných látek. V jaderném průmyslu se využívá pro obohacování uranu separací izotopu uranu-235.

[63] ERBEN, Lukáš. *Příchod hackerů: příběh Stuxnetu* [online]. root.cz, 29. dubna 2014 [cit. 10. května 2021]. Dostupné na <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>.

[64] KUSHNER, David. *The Real Story of Stuxnet* [online]. ieee spectrum, 26. února 2013 [cit. 15. května 2021]. Dostupné na <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

v Íránu i potřeba vysoké kooperativy a plánování včetně velkého množství expertů pro vytvoření takového viru.[65]

Právě dlouhodobé plánování projektu takového záběru zapadá spíše do definice „pokračování pokynů“ a zároveň je natolik oddělené od přímé kontroly státem, že nelze podřadit ani pod pojem „pokyny“ či „kontrola“. Pravděpodobně bychom tuto akci identifikovali jako chování řízené státem.[66]

3.3.6. Chování kontrolované státem

Poslední pojem zahrnutý ve článku 8, dle kterého je možné připsat určité chování státu, je založen na kontrole. Tudíž, že stát musí vykonávat kontrolu nad daným chováním nestátního subjektu.

Tento pojem je lehce zaměnitelný s kontrolou nad orgánem státu v případě, že stát bude vykonávat zvláště velký stupeň kontroly, jak je stanoveno v rozsudku MSD ve věci Bosenské genocidy.[67] Samotná povinnost státu vykonávat kontrolu na svém území neznamená bez dalšího, že je stát zodpovědný za jakékoliv protiprávní chování. Otázkou tedy bude, jak stanovit hranici mezi oběma typy kontrol. Tato problematika má pak reálný dopad na právní posouzení věci, ve smyslu, zda situaci posuzovat dle čl. 8 nebo čl. 4 Návrhu.[68] V potaz musíme vzít to, že v rámci přičitatelnosti je právní posouzení dle čl. 4 jistější pro zajištění odpovědnosti státu než dle čl. 8 Návrhu. Hranice mezi oběma články se určí podle stupně vykonávané kontroly, v případě *„převážně velké“*[69] kontroly ve smyslu *„úplné závislosti“*[70] na státu se bude postupovat dle čl. 4 Návrhu.

Mačák ve svém článku uvádí jako příklad takové kontroly situaci, kdy státem vytvořená skupina skládající se ze zaměstnanců jak státní správy, tak soukromých společností vykonává aktivity na žádost státu za účelem odvracení kybernetických útoků. V takovémto případě by stát automaticky odpovídal za chování této skupiny, která de facto substituuje orgán státu.[71]

---

[65] NAKASHIMA, Ellen. *Stuxnet was work of U.S. and Israeli experts officials say* [online]. The Washington Post, 2. června 2012 [cit. 27. května 2021]. Dostupné na <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.
[66] MAČÁK: *Decoding Article 8*…, s. 419.
[67] Rozsudek Mezinárodního soudního dvora z 26. února 2007, *Bosna a Hercegovina v. Srbsko a Černá Hora*, odst. 393.
[68] MAČÁK: *Decoding Article 8*…, s. 420.
[69] Rozsudek MSD: *Bosna a Hercegovina v. Srbsko a Černá Hora*, odst. 393.
[70] Tamtéž.
[71] MAČÁK: *Decoding Article 8*…, s. 420.

Při určování stupně kontroly se v mezinárodním právu v průběhu minulých let formulovaly dva přístupy, efektivní kontrola a celková kontrola. Test efektivní kontroly byl prvně rozeznán MSD. V rozsudku ve věci Vojenských a para-vojenských aktivit v Nikaragui a proti ní (*Nikaragua v. USA)* z roku 1986 Soud poprvé vyložil pojmy řízení, pokyny a kontrola, zmiňované ve čl. 8 Návrhu. Tento výklad později podpořila i jeho další judikatura, a to přesněji již zmiňovaný rozsudek *Bosna a Hercegovina v. Srbsko a Černá Hora* z roku 2007. MSD dospěl k závěru, že je třeba kontrolu vykládat ve smyslu kontroly efektivní, což znamená vykonávat kontrolu nad každou operací, kterou došlo k porušení mezinárodního práva.[72] *„Musí se jednat o víc než jen pouhou podporu nestátního subjektu, a to ať už ve smyslu financování, organizování, trénování, zásobování nebo vybavování.“*[73] Pod určení kontroly jako efektivní spadá například zapojování státu ve smyslu vybrání velitele, organizace, trénování a vybavování, plánování operací, vybírání cílů a poskytnutí operativní pomoci určitému nestátnímu subjektu.[74] Rozsudek zmiňuje, že veškeré výše uvedené zapojení státu samo o sobě nezakládá přičitatelnost bez dalšího. Je nezbytné prokázat, že stát řídil či vynucoval chování odporující lidskoprávním závazkům. A to z toho důvodu, že nestátní subjekt by takové chování mohl klidně podnikat i bez vědomí státu.[75]

V kyberprostoru nastává s tímto přístupem dokonce mnohem větší problém než ve fyzickém světě. Uvedené prvky efektivní kontroly jsou totiž docela přísně nastavené, a tudíž získání důkazů pro jejich prokázání bývá extrémně složité.[76] Příklad můžeme vidět na nedávném kybernetickém útoku nejen na Spojené státy americké. Na konci roku 2020 došlo k odhalení kyber-útoku na společnost SolarWinds a její systémy, na kterých fungují i státní orgány USA. I přes získané důkazy a podobnou taktiku, jako u předchozích útoků, bude přičtení takového útoku velmi složité.[77]

---

[72] FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 2, Praktikum.* Praha: Leges, 2017, s. 129.
[73] MAČÁK: *Decoding Article 8*…, s. 421.
[74] Rozsudek Mezinárodního soudního dvora z 27. června 1986, *Nikaragua v. USA*, odst. 112.
[75] Tamtéž, odst. 115.
[76] MAČÁK: *Decoding Article 8*…, s. 421.
[77] TIDY, Joe. *SolarWinds hack: Russian denial 'unconvincing'* [online]. BBC, 18. května 2021 [cit. 5. června 2021]. Dostupné na <https://www.bbc.com/news/technology-57156197>.

Širší náhled, a tudíž benevolentnější přístup k definici kontroly, nabídl Mezinárodní trestní tribunál pro bývalou Jugoslávii v rozhodnutí ve věci *Tadić*[78]. K výrazu kontrola přistupuje jako ke kontrole celkové, kdy k přičitatelnosti státu stačí např. materiální či finanční podpora.[79] V kyberprostoru se může jednat například o situaci, kdy stát vyvine malware, který poskytne nestátnímu subjektu např. skupině hackerů a následně se částečně podílí i na koordinaci a výběru cíle. V tomto případě by se jednalo o kontrolu celkovou, i když by to nenaplnilo prvky efektivní kontroly.[80]

Dalším argumentem na zvážení změny aplikace testu kontroly v kyberprostoru je skutečnost, že v době přijetí rozsudku *Nikaragua v. USA* v roce 1986, dokonce ještě ani neexistovala internetová sít WWW. Tudíž soud ani nemohl vzít v potaz tuto další vrstvu pro uplatňování mezinárodního práva. Otázkou tedy zůstává, zda se na tento rozsudek, byť ve své době aktuální, nedívat očima současné doby a nepřehodnotit jeho aplikaci v tomto kontextu.[81]

Pro doplnění dvou výše uvedených přístupů vnímání kontroly jako takové, se nabízí i rozsudek ESLP ve věci *Loizidou v. Turecko* z roku 1995. Soud v rozsudku přiznal přičitatelnost chování státu na základě celkové efektivní kontroly. Smluvní stát je povinen dodržovat lidskoprávní závazky plynoucí z Evropské úmluvy o ochraně lidských práv i v případě, pokud v důsledku legálních či nelegálních vojenských akcí vykonává efektivní kontrolu nad územím mimo hranice svého státu. Tato kontrola může být vykonávána přímo, pomocí ozbrojených sil nebo pomocí podřízených místních sil.[82]

Zmíněný rozsudek ESLP se jeví jako tzv. střední cesta mezi kontrolou efektivní a celkovou. Jeho přínos je však otázkou, stírá sice značné rozdíly mezi zbylými dvěma přístupy, ale zároveň není rozveden více do hloubky.

3.3.7. Přičitatelnost chování státu v kyberprostoru

Celkově se dají identifikovat tři hlavní problémy spojené s kyberprostorem a přičitatelností. Zaprvé se jedná o velmi anonymní prostředí, kde je problém dohledat skutečného pachatele, zadruhé je možné vyvinout útok který postihne široké množství počítačů a obětí, a za třetí rychlost se kterou určitý útok může být

[78] Rozsudek Mezinárodního trestního tribunálu pro bývalou Jugoslávii z 15. července 1999, *The Prosecutor v.Tadić*.
[79] FAIX: *Rukověť ke studiu…,* s. 129.
[80] MAČÁK: *Decoding Article 8*…, s. 422.
[81] Tamtéž, s. 425.
[82] Rozsudek Evropského soudu pro lidská práva ze dne 23. března 1995, *Loizidou v. Turecko*, 15318/89, odst. 62

vyvinut je v přirovnání s fyzickým útokem neporovnatelná. Při kybernetickém útoku je pak důležité zjistit nejen odkud útok vychází, ale hlavně kdo za ním stojí.[83]

Z výše uvedených skutečností vyplývá, že v kontextu čl. 8 Návrhu se na přičitatelnost přednostně aplikuje kontrola efektivní. Nicméně důležité taky je, posuzovat každou situaci zvlášť v kontextu v jakém se nachází. Tento přístup potvrzuje i mezinárodní judikatura a doktrína.[84] Čl. 55 Návrhu, jenž zní *„Tyto články se nepoužijí tam a v takovém rozsahu, kde podmínky pro existenci mezinárodně protiprávního chování nebo obsah nebo provádění mezinárodní odpovědnosti státu jsou upraveny zvláštními pravidly mezinárodního práva.“*[85] rozeznává existenci speciálních režimů mezinárodních prostorů s jejich vlastními pravidly pro přičitatelnost. To nicméně, dle Mačáka, prozatím právo neuznává v kombinaci s kyberprostorem. Stále ale platí, že se klasická pravidla přičitatelnosti vztahují i na kybernetické útoky.[86]

[83] TSAGOURIAS, Nicholas. Cyber attacks, self-defence and the problem of Attribution. *Journal of Conflict & Security Law,* 2012, roč. 17, s. 233.
[84] Tamtéž, s. 238.
[85] Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování z roku 2001, čl. 55
[86] MAČÁK: *Decoding Article 8*…, s. 425.

4. Vybrané články MPOPP

4.1. Čl. 17 MPOPP: Právo na soukromí

„1. Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst. 2. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“[87]

Právo na soukromí je jedno ze základních práv člověka, které je kodifikováno i v Listině základních práv a svobod, kde článek 7 odst. 1 jasně stanoví, že: *„Nedotknutelnost osoby a jejího soukromí je zaručena.“*[88]

Předmětné právo lze najít také ve Všeobecné deklaraci lidských práv a svobod ve čl. 12: *„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“*[89]

4.1.1. Regulace na půdě OSN

Ve stanovisku Úřadu vysoké komisařky OSN pro lidská práva představeném na Odborném workshopu k právu na soukromí v digitálním věku, konaném v roce 2018, se uvádí: *„Nejen, že se jedná o základní právo rozeznané mezinárodním právem, ale zároveň se jedná i o univerzální právo, na které by každý měl mít nárok kdekoliv z toho vyplývá, že by kdekoliv na světě mělo být každým respektováno. Každým se myslí jak státy, tak nestátní aktéři, bez ohledu na etnicitu, národnost, gender, náboženství, filozofické či politické názory nebo osobní stav jedince. Univerzálnost tohoto práva vychází ze základních principů při stanovování rámce lidských práv po druhé světové válce.“*[90]

Přestože panuje konsenzus, že právo na soukromí existuje a je potřeba ho ochraňovat, jeho poněkud vágní definice zanechává spoustu otázek o jeho konkrétních implikací. Není zřejmé, jaké nároky z něj přesně plynou, či jak ho uplatňovat v různých situacích. Tato nepříliš jasná definice má svoje výhody i nevýhody, jak bylo zmíněno během workshopu. Je zřejmé, že pokud bychom se vydali cestou jasného vymezení pojmu právo na soukromí mohli bychom se dopustit

[87] Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2, čl. 17
[88] Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod, čl. 7
[89] Všeobecná deklarace lidských práv ze dne 10. prosince 1948, čl. 12
[90] Zpráva zvláštního zpravodaje k právu na soukromí ze dne 28. února 2018, A/HRC/37/62, příloha, odst. 1.

až přílišného zúžení jeho ochrany což by při neustálém vývoji technologií a změny situací mělo spíše negativní dopad.[91] *„Neustále se vyvíjející technologie kladou důležité výzvy pro ochranu soukromí: tyto technologie mohou odhalit nejintimnější chování, přání, preference a smýšlení jednotlivce způsoby, které předtím nebyly možné. Chytré telefony, kreditní karty a internet jsou tři dobré příklady technologií, které sebou přináší významné výzvy pro ochranu soukromí.“*[92] Postupem času a neustálým objevováním nových hrozeb se také mění naše vnímání zásahu do soukromí a jeho úzkým vymezením bychom omezovali jeho aplikaci.[93]

Nejen Úřad komisařky vydal zprávu k dopadu nových technologií, tématu se věnoval i zvláštní zpravodaj OSN k právu na soukromí ve své zprávě z roku 2018 (A/HRC/39/29) a zaměřil se na soukromí v digitálním věku a jeho vymezení rozsahu. Ochrana soukromí je velmi široký pojem, který se vztahuje nejen na informace obsažené v samotném vláknu komunikace ale zároveň i na metadata[94], která když jsou sesbíraná a analyzovaná mohou poskytnout vhled do různých aspektů života jedince. Ať už se jedná o chování, sociální vazby, osobní preference nebo identitu. Zmíněné aspekty jedince nelze vyčíst z pouhého obsahu komunikace, je k nim právě zapotřebí přístup k metadatům, z toho plyne jejich přidaná, a za určitých okolností nebezpečná hodnota.[95]

Zpráva dále upřesňuje, že „*ochrana práva na soukromí se nevztahuje pouze na soukromé odlehlé prostory jako je domov jedince, ale myslí se tím i veřejné prostory a informace jež jsou veřejně přístupné.“*[96] Vychází tak ze závěrů Komise OSN pro lidská práva[97].

Jako fiktivní příklad výše uvedených závěrů se jeví například situace, kdy „*vláda státu monitoruje veřejné prostory, například trhy, nádraží, a tím pozoruje chování a pohyb jedinců. Podobně to také platí v případě, kdy jsou osobní informace sdílené na sociálních sítích sbírány a analyzovány. Obsah veřejně sdílených informací pojímá stejné ochrany.“*[98]

---

[91] Zpráva zvláštního zpravodaje: *A/HRC/37/62*, odst. 2.
[92] Tamtéž, odst. 5.
[93] Tamtéž, odst. 2.
[94] Metadata popisují jiná data. Poskytují informace o obsahu určité položky. Například metadata obrázku popisují jeho velikost, barvu, kdy byl vytvořen a další informace. Více na: *Metadata* [online]. Tech Terms, [cit. 10. května 2021]. Dostupné na <https://techterms.com/definition/metadata>.
[95] Zpráva Úřadu vysoké komisařky OSN pro lidská práva ze dne 30. června 2014, A/HRC/27/37, odst. 19.
[96] Zpráva Úřadu vysoké komisařky OSN pro lidská práva ze dne 3. srpna 2018, A/HRC/39/29, odst. 6.
[97] Dokument Výboru pro lidská práva ze dne 17. listopadu 2016, CCPR/C/COL/CO/7, odst. 32.
[98] Zpráva Úřadu vysoké komisařky OSN: *A/HRC/39/29*, odst. 6.

Stejně jako Výbor pro lidská práva, který v obecném komentáři č. 31 stanoví, že se MPOPP aplikuje i extrateritoriálně, zmiňuje to i zvláštní zpravodaj OSN ve své zprávě k právu na soukromí. *„členský stát musí respektovat a zajistit práva stanovená v MPOPP každému v rámci jeho výkonu státní moci, i když se nenachází na jeho území.“*[99] Lidská práva včetně ochrany práva na soukromí se aplikují i na využívání moderních technologií mimo území státu. Jedná se například o technologie k přímému odposlechu či nepřímému využívání digitální komunikační infrastruktury. Stejná pravidla se uplatní i ve vztahu ke třetím stranám, jako jsou soukromé společnosti, v případě, že nad nimi stát vykonává jurisdikci. Ochrana dat, kterými tyto třetí strany disponují musí být zajištěna na základě MPOPP.[100]

Kromě zpráv úřadu vysoké komisařky nebo zvláštních zpravodajů, kteří potvrdili závazek států dodržovat své lidskoprávní závazky i v online prostředí, a to převážně při využívání technologií k získávání dat o soukromém životě jednotlivců, se k těmto závazkům zavázaly i státy pomocí rezolucí OSN, které převážně vycházejí z těchto zpráv. Nejsou sice právně závazné, jak je zmíněno v první kapitole této práce, nicméně se jedná o důležitý politický krok směrem k budoucímu vynutitelnému právnímu instrumentu, jak dále zmiňuji v kapitole pět.

Mimo jiné se jedná o rezoluci Rady OSN pro lidská práva Právo na soukromí v digitálním věku (A/HRC/RES/42/15), kde v odstavci 4 potvrdili, že *„stejná práva, která mají lidé offline musí být ochráněny také online, včetně práva na soukromí.“*[101]. Jasně a zřetelně přiznali, že právo na soukromí spadá mezi ochranu práv, jež lidé užívají online cestou. Soukromí v online prostoru, jako jediné lidské právo, je řešeno i na půdě Valného shromáždění OSN, a to přesněji v rezoluci A/C.3/75/L.40 Právo na soukromí v digitálním věku. Rezoluce v odst. 5 vyzývá státy aby „*podporovaly otevřené, bezpečné, stabilní, přístupné a mírové prostředí informačních a komunikačních technologií založené na dodržování mezinárodního práva, včetně závazků zakotvených v Chartě OSN a v lidskoprávních instrumentech“*.[102] Tato rezoluce byla schválena konsenzem, což znamená, že s ní souhlasily všechny státy OSN. Jedná se tedy o skvělý základ pro budoucí utváření vynutitelných lidskoprávních závazků států v kyberprostoru.

[99] Tamtéž, odst. 9.
[100] Zpráva Úřadu vysoké komisařky OSN pro lidská práva ze dne 30. června 2014, A/HRC/27/37, odst. 34.
[101] Rezoluce Rady OSN pro lidská práva ze dne 7. října 2019, A/HRC/RES/42/15
[102] Rezoluce Valného shromáždění OSN ze dne 30. října 2020, A/C.3/75/L.40, odst. 5

4.1.2. Dohled státu

V souvislosti s ochranou práva na soukromí je ještě důležité zmínit i dohled státu. Toto téma bylo mimo jiné několikrát zdůrazněné whistblowery, jako je například Edward Snowden. Bývalý zaměstnanec americké CIA zveřejnil v roce 2013 záznamy rozsáhlého sledování internetové i telefonní komunikace osob americkými tajnými službami.[103] Tato medializovaná kauza rozvířila debatu o tom, jak státy sbírají a uchovávají informace o osobách, a zda je to v souladu s právem, či zda je vůbec takové uchovávání informací určitým způsobem regulováno.

Sledování aktivit osob a právu na soukromí se věnuje mimo jiné i zvláštní zpravodaj OSN k právu na soukromí. Ve zprávě z roku 2017[104] cituje judikát Evropského soudu pro lidská práva („ESLP“) z roku 2016[105], který připomíná státům EU povinnost respektovat lidskoprávní závazky. V rozsudku říká, že *„taková právní úprava je zásahem do základních práv zakotvených v článcích 7 a 8[106] Listiny, který se jeví jako rozsáhlý a musí být považován za zvlášť závažný. Okolnost, že k uchovávání údajů dochází bez vyrozumění uživatelů služeb elektronických komunikací, může v dotčených osobách vyvolávat dojem, že jejich soukromí je pod neustálým dohledem.*“[107]. Mimo jiné pak rozsudek zmiňuje i možné negativní dopady na svobodu projevu při nezákonném uchovávání těchto dat.[108]

Nutno zmínit, že ESLP se také vyjádřil k přijímání legislativy na národní úrovni, jenž může omezovat právo na soukromí „*dále, i když účinnost boje proti závažné trestné činnosti, zejména proti organizované trestné činnosti a terorismu, může ve značném rozsahu záviset na využívání moderních vyšetřovacích postupů, nemůže takový cíl obecného zájmu, jakkoli se jedná o cíl základní, však sám o sobě odůvodnit, že vnitrostátní právní úprava, která stanoví plošné a nerozlišující*

---

[103] *Edward Snowden: Leaks that exposed US spy programme* [online]. BBC, 17. ledna 2014 [cit. 22. května 2021]. Dostupné na <https://www.bbc.com/news/world-us-canada-23123964>.
[104] Zpráva zvláštního zpravodaje k právu na soukromí ze dne 6. září 2017, A/HRC/34/60.
[105] Rozsudek ESLP ze dne 21. prosince 2016, *Tele2 Sverige a Secretary of State for the Home Department v. Post- och telestyrelsen a další,* spojené věci C-203/15 a C-698/15
[106] Článek 7 *„Každý člověk má právo na respektování svého soukromého a rodinného života, obydlí a korespondence či jiných druhů komunikace.“*; článek 8 *„1. Každý člověk má právo na ochranu údajů osobního charakteru, které se ho týkají. 2. S těmito údaji musí být nakládáno čestně, pouze k přesně danému účelu a na základě souhlasu dotyčné osoby či na základě jiného legitimního opodstatnění uvedeného v zákoně. Každý člověk má právo na přístup k údajům sebraným o jeho osobě a na jejich zpřesnění. 3. Respektování těchto pravidel podléhá kontrole nezávislé moci.“*
[107] Rozsudek ESLP: *Tele2 Sverige a Secretary…,* odst. 100.
[108] Zpráva zvláštního zpravodaje *A/HRC/34/60*, odst. 16.

uchovávání veškerých provozních a lokalizačních údajů, je považována za nezbytnou pro účely uvedeného boje.“[109].

Zatímco zastánci práva na soukromí považují tento rozsudek za přelomový, jiní odborníci považují rozsudek za radikální ve smyslu přílišného omezení uchovávání dat, což může mít negativní dopad a způsobit obtíže při vymáhání práva.[110]

Zpráva zmiňuje ještě jeden rozsudek ESLP, a to *Zakharov v. Rusko* z roku 2015, který stanoví povinnost zakotvit na národní úrovni přiměřené a účinné záruky proti zneužití nahrávání komunikace při tajném sledování.[111]

4.2. Čl. 19 MPOPP: právo na svobodu projevu a názoru

„1. Každý má právo zastávat svůj názor bez překážky. 2. Každý má právo na svobodu projevu; toto právo zahrnuje svobodu vyhledávat, přijímat a rozšiřovat informace a myšlenky všeho druhu, bez ohledu na hranice, ať ústně, písemně nebo tiskem, prostřednictvím umění nebo jakýmikoli jinými prostředky podle vlastní volby. 3. Užívání práv uvedených v odstavci 2 tohoto článku s sebou nese zvláštní povinnosti a odpovědnost. Může proto podléhat určitým omezením, avšak tato omezení budou pouze taková, jaká stanoví zákon a jež jsou nutná: a) k respektování práv nebo pověsti jiných; b) k ochraně národní bezpečnosti nebo veřejného pořádku nebo veřejného zdraví nebo morálky.“[112]

Právo na svobodu projevu je však kodifikováno i v České republice, a to v Listině základních práv a svobod ve čl. 17 odst. 1 a 2: *„(1) Svoboda projevu a právo na informace jsou zaručeny. (2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.“*[113]. Obě úpravy stejně jako právo na soukromí vychází ze Všeobecné deklarace lidských práv, toto konkrétní právo je pak upraveno v čl. 19: „*Každý má právo na svobodu přesvědčení a projevu; toto právo nepřipouští, aby někdo trpěl újmu pro své přesvědčení,*

[109] Rozsudek ESLP: *Tele2 Sverige a Secretary…,* odst. 103.
[110] Zpráva zvláštního zpravodaje *A/HRC/34/60*, odst. 18.
[111] Rozsudek ESLP ze dne 4. prosince 2015, *Roman Zakharov v. Rusko*, 47143/06, odst. 233
[112] Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2, čl. 19
[113] Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod

a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a bez ohledu na hranice.“[114].

Jak vyplývá z názvu podkapitoly, jedná se o dvě práva, která jsou spolu vzájemně propojena. Právo na svobodu projevu je pak v podstatě tzv. deštník, který je propojený s dalšími právy jako jsou mimo jiné svoboda tisku, svoboda názoru, svoboda shromažďování a sdružování, svoboda myšlení a svědomí, svoboda náboženství, právo na soukromí, zákaz cenzury a zásah státu do korespondence a osobního vlastnictví.[115]

4.2.1. Úprava na půdě OSN

Stejně jako u práva na soukromí, zvláštní zpravodaj OSN k právu na svobodu projevu ve zprávě z roku 2016 zmiňuje, že „*státy nesou primární odpovědnost za ochranu a respektování práva k vykonávání svobody projevu a názoru.*“[116] Státy nesmí skrze zákony, opatření nebo další instrumenty nutit soukromý sektor k podniknutí takových kroků, které by zasahovaly do práva na svobodu projevu.[117]

Jedná se o právo hojně diskutováno i v rámci rezolucí Rady OSN pro lidská práva. Například v rezoluci A/HRC/RES/44/12 Svoboda projevu a názoru se říká, že *„…právo na svobodu projevu a názoru, jak online, tak offline, je lidské právo garantované všem, v souladu s článkem 19 VDLP a MPOPP…“*[118].

Omezení práva na svobodu projevu, bývá většinou velmi úzce spjato se stíháním novinářů a dalších obránců lidských práv. Proto existují rezoluce Rady OSN pro lidská práva zamřené jen na tuto problematiku. Např. rezoluce A/HRC/RES/39/6 Bezpečí novinářů, říká, že „*odsuzuje jednoznačná opatření v rozporu s mezinárodním právem v oblasti lidských práv, která mají za cíl, nebo která úmyslně zabraňují, nebo narušují přístup nebo šíření informací online a offline, čímž narušují práci novinářů při informování veřejnosti…“*[119]

4.2.2. Umělá inteligence

S právem na svobodu projevu a názoru je velmi úzce spojeno využívání umělé inteligence. Ad hoc expertní skupina UNESCO (*Organizace OSN pro vzdělání, vědu a kulturu*) přistupuje k AI jako k technologickému systému, který má schopnost

[114] Všeobecná deklarace lidských práv ze dne 10. prosince 1948, čl. 19
[115] SMITH, Rhona K.M. *Textbook on international human rights*. Oxford, New York, N.Y.: Oxford University Press, 2010, s. 291.
[116] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 11. května 2016, A/HRC/32/38, odst. 85.
[117] Zpráva zvláštního zpravodaje: *A/HRC/32/38*, odst. 85.
[118] Rezoluce Rady OSN pro lidská práva ze dne 24. července 2020, A/HRC/RES/44/12
[119] Rezoluce Rady OSN pro lidská práva ze dne 5. října 2018, A/HRC/RES/39/6

zpracovávat různá data a informace na základě aspektů uvažování, učení, vnímání, predikce, plánování nebo kontroly, jež se dají přirovnat k inteligentnímu chování. Je navržený tak, aby fungoval na základě prvků autonomního uvažování s využíváním poskytnutých dat.[120] Umělá inteligence přináší spoustu výhod pro život, stejně tak jako nevýhod.

Mezi výhody můžeme zařadit usnadňování fungování běžného života jako je vyhledávání informací, využívání aplikací v chytrém telefonu, chytrá domácnost, algoritmy na sociálních sítí, zacílené reklamy nebo širší šíření informací, stejně jako jejich přijímání.[121] Nevýhody nastupují v tu chvíli, kdy je jejich původně neutrální podstata využita k účelům, jež mohou mít za následek porušení lidských práv.

Příkladem může být algoritmus, který využívaly orgány státní správy v Nizozemsku, jak dále zmiňuje výzkumná zpráva Amnesty International. Nedávná zpráva vydaná v září 2020 se týká policejního monitorování osob v Nizozemsku využívajícího algoritmus, který rozhodoval na základě diskriminačních prvků.

Zpráva pojednává o policejní taktice k odhalení potenciálních pachatelů trestného činu krádeže v městečku Roermond. Na základě sesbíraných dat a pomocí algoritmu profiluje osoby s vysokým rizikem pravděpodobnosti spáchání tohoto činu. Ačkoliv je tento algoritmus prezentovaný jako nediskriminační, Amnesty International ve zprávě uvádí, že tíhne k většímu zaměření na osoby pocházející z východní Evropy, v důsledku čehož dochází k diskriminaci na základě národnosti.[122]

Aby nedocházelo k podobným případům, musí státy a soukromé společnosti při navrhování, vyvíjení a rozmísťování dodržovat lidskoprávní závazky.[123] „*právo lidských práv ukládá státům jednak negativní povinnosti, zdržet se provádění opatření, která zasahují do výkonu svobody přesvědčení a projevu, jednak pozitivní povinnosti, prosazovat práva na svobodu projevu a názoru chránit jejich výkon*.“[124]

---

[120] UNESCO. *First Draft Of The Recommendation On The Ethics Of Artificial Intelligence.* Paříž: Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, 2020.

[121] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 29. srpna 2018, A/73/348, odst. 1.

[122] *We Sense Trouble: Automated Discrimination And Mass Surveillance In Predictive Policing In The Netherlands* [online]. Amnesty International, 29. září 2020 [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/documents/eur35/2971/2020/en/>.

[123] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 29. srpna 2018, A/73/348, odst. 19.

[124] Zpráva zvláštního zpravodaje: *A/73/348*, odst. 19.

4.2.3. Přístup k informacím

S právem na svobodu projevu a názoru je logicky spjaté i opačné právo, zaručující přístup k informacím. V dnešní době je klíčové, aby kdokoliv měl možnost si zjistit informace o událostech, které se právě odehrávají. Tím spíš, když většina zásadních informací je dostupná pouze na internetu. Špatný přístup k informacím může mít za následek i negativní dopad na další práva jako jsou ekonomická, sociální či kulturní.[125]

Článek 19 MPOPP však neobsahuje právo na přístup k informacím, je v něm zmíněno pouze „…*toto právo zahrnuje svobodu vyhledávat, přijímat a rozšiřovat informace a myšlenky všeho druhu…"*[126] Je tedy potřeba použít analogického výkladu. K tomu se uchýlil Výbor pro lidská práva v obecném komentáři č. 34 z roku 2011, kde v odstavci 18 říká, že „*článek 19, odstavec 2 zahrnuje právo na přístup k informacím uchovávanými orgány veřejné moci*."[127] Tímto tak rozšířil výklad článku i na přístup k informacím.

Kromě Výboru pro lidská práva zmiňují toto právo i některé rezoluce Rady OSN pro lidská práva. V jejich případě se sice nejedná o právně závazné dokumenty, avšak lze je považovat za jistý politický závazek včetně rozeznání tohoto práva státy. Jedná se například o rezoluci A/HRC/RES/44/12 Svoboda projevu a názoru, kde se státy shodly na tom, že *„…všechny státy zajišťují veřejný přístup k informacím a ochraňují lidská práva a základní svobody, v souladu s národní legislativou a mezinárodními smlouvami*."[128].

4.2.4. Přístup k informacím a veřejné zdraví

Nutnost znát všechny aktuální informace se ukázala jako zásadní při rozpuku pandemie COVID-19 v roce 2019. Během následujícího roku zasáhla pandemie celý svět a informace státních orgánů, jak postupovat, či jaká opatření jsou nově zavedená, se měnily v řádu hodin. Bez plného přístupu k informacím by fungování ve společnosti bylo značně ztížené, nehledě na to, že při porušení zavedených opatření hrozil i finanční či jiný postih.

K tomu se vyjádřil i zvláštní zpravodaj OSN k právu na svobodu projevu a názoru ve zprávě z roku 2020. *„výchozí poloha musí být taková, že veřejné orgány*

[125] Rezoluce Rady OSN pro lidská práva ze dne 24. července 2020, A/HRC/RES/44/12
[126] Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2, čl. 19 odst. 2
[127] Obecný komentář Výboru pro lidská práva ze dne 12. září 2011, CCPR/C/GC/34, odst. 18.
[128] Rezoluce Rady OSN pro lidská práva: *A/HRC/RES/44/12.*

nečekají na žádost o informace; musí mít aktivní politiku uvolňování všech příslušných informací způsoby, které jsou srozumitelné pro netechnickou veřejnost a které prosazují priority v oblasti veřejného zdraví.“[129]

4.2.5. Právo na přístup k internetu: nové lidské právo

V poslední době se často diskutuje vznik tzv. nového práva na přístup k internetu. V kontextu rychlého vývoje nových technologií a celkové digitalizace společnosti, se to zdá býti krok správným směrem. Podobná myšlenka je zmíněna i v knize od Rhona K. M. Smitha „*„stopa“ lidských práv v kyberprostoru je tak velká, že odborníci diskutují o tom, zda přístup na internet je, nebo by měl být, novým lidským právem.*“ .[130]

K právu na přístup k internetu se vyjadřují i zvláštní zpravodajové OSN. Například ve zprávě z roku 2018 zmiňují, že nátlak na prosazování univerzálního přístupu k internetu je na státy vytvářen jak regionálními, tak mezinárodními orgány.[131] Čímž se myslí například rezoluce Rady OSN pro lidská práva k prosazování, ochraně a užívání lidských práv na internetu z roku 2016, která vyzývá státy, aby „…*zvážily formulování, skrze transparentní a inklusivní proces se všemi zúčastněnými stranami, a přijetí národního postoje k internetu, který by naplňoval prvky univerzálního přístupu a užívání lidských práv*“[132].

Další zpráva, vydaná minulý rok, se váže ke globální pandemii a jejímu propojení s internetem a informacemi. „*v okamžiku globální pandemie by mělo být právo na přístup k internetu přeformulováno a mělo by být chápáno tak, jaký je jeho účel: kritický prvek politiky a praxe v oblasti zdravotní péče, veřejných informací a dokonce práva na život*.“[133]

Mezi odborníky panuje názor, že právo na přístup k internetu je stěžejní, jak můžeme vyčíst z jejich zpráv. Kdežto na mezivládní rovině, i přes určitý nátlak a vliv, zatím nedošlo k většímu pokroku než k uznání důležitosti k přístupu k internetu.[134]

Nicméně uznání práva na přístup k internetu jako takového, vyžaduje mnohem delší cestu vyjednávání a konsenzu než pouhé prohlášení odborníky. Už jen

[129] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 23. dubna 2020, A/HRC/44/49, odst. 18.
[130] TSAGOURIAS, Nicholas, BUCHAN, Russell. *Research handbook on international law and cyberspace*. Cheltenham, UK, Northampton, MA: Edward Elgar Publishing, 2017, s. 94.
[131] Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 6. dubna 2018, A/HRC/38/35, odst. 6.
[132] Rezoluce Rady OSN pro lidská práva ze dne 18. července 2016, A/HRC/RES/32/13, odst. 12
[133] Zpráva zvláštního zpravodaje: *A/HRC/44/49*, odst. 24.
[134] Tamtéž.

samotné rozšíření výkladu článku 19 MPOPP o přístup k informacím, trvalo několik desítek let.

4.3. Čl. 21 a 22: právo na svobodu shromažďování a sdružování

„*Uznává se právo na pokojné shromažďování. Výkon tohoto práva nesmí být žádným způsobem omezován s výjimkami, jež stanoví zákon a jež jsou nutné v demokratické společnosti v zájmu národní bezpečnosti nebo veřejné bezpečnosti, veřejného pořádku, ochrany veřejného zdraví nebo morálky nebo ochrany práv a svobod jiných*.“[135]

„*2. Každý má právo na svobodu sdružovat se s jinými, i právo zakládat na ochranu svých zájmů odborové organizace a přistupovat k nim.“*[136]

Právo na svobodu shromažďování a sdružování je bráno jako jedno právo, i když často bývá uzákoněno v odlišných ustanoveních, jako například výše citovaná definice z MPOPP. Stejně jako předchozí práva i toto právo vychází ze Všeobecné deklarace lidských práv, a to z článku 20 odstavce 1: „*Každému je zaručena svoboda pokojného shromažďování a sdružování*.“[137]. V Listině ČR pak toto právo můžeme najít ve čl. 20 a 21.[138]

4.3.1. Úprava na půdě OSN

Právo na svobodu shromažďování v online prostředí je v poslední době více a více důležité. I předtím, než v celém světě vypukla pandemie COVID-19 a skoro ve všech státech bylo, alespoň po nějakou dobu, zakázáno se shromažďovat, kvůli čemuž občanská společnost mohla vyslovovat nesouhlas jenom převážně pomocí sociálních sítí, hrály online platformy důležitou roli. Ostatně to dokazuje například i zpráva zvláštního zpravodaje OSN pro svobodu shromažďování a sdružování z roku 2019.[139]

Zpravodaj vidí důležitou roli sociálních sítí třeba v události týkající se tzv. sametové revoluce v Arménii v roce 2018, při které rezignoval tehdejší premiér a následně byl zvolen nový, jenž prosazoval odlišné priority směřované více

[135] Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2, čl. 21
[136] Tamtéž, čl. 22 odst. 1.
[137] Všeobecná deklarace lidských práv ze dne 10. prosince 1948, čl. 20 odst. 1
[138] Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod, čl. 19 odst. 1, čl. 20 odst.1
[139] Zpráva zvláštního zpravodaje ke svobodě shromažďování a sdružování ze dne 17. května 2019, A/HRC/41/41.

prozápadně.[140] K tomu, aby tato změna byla umožněna byla potřeba podpora občanské společnosti, která byla právě získávána sociálními platformami, médii a dalšími komunikačními aplikacemi, mimo jiné i z důvodu vládní kontroly klasických médií. Díky těmto nástrojům došlo ke sdílení informací, hashtagů vyjadřujících podporu a k mobilizaci široké veřejnosti.[141]

Opačným příkladem, kdy nedochází k podpoře práva na svobodu shromažďování a sdružování, ale naopak za jeho realizaci hrozí zadržení, je situace v Myanmaru. Jedinci, jež projevují jiný politický názor jsou perzekuováni. Tato hrozba v minulém roce měla dopad i na práci novinářů, kteří byli nuceni ke svévolné cenzuře ze strachu o svůj život.[142] Omezení jejich práce má dopad i na širokou veřejnost ve smyslu těžšího získávání potřebných informací.

Právě nástroje aktivistů, občanské společnosti a obránců lidských práv bývají často předmětem omezení a kontroly ze strany vládních aparátu. Dochází tak mimo jiné k zamezení přístupu k sociálním sítím, cenzuře, vypínání internetového připojení nebo blokování webových stránek neziskových organizací, a to převážně při příležitostech konání voleb a demonstrací. Kromě těchto plošnějších omezení dochází i k digitálnímu sledování a online zastrašování politické opozice, aktivistů a dalších obránců lidských práv. Veškeré podniknuté kroky státu vůči těmto osobám vedou k zásahu do jejich lidských práv a k oslabení veřejného nejen politického života[143].

„Mezinárodní právo chrání právo na svobodu pokojného shromažďování a sdružování, ať už vykonávané osobně, prostřednictvím dnešních technologií nebo prostřednictvím technologií, které budou objeveny v budoucnu.“[144] Právo na svobodu shromažďování a sdružování v online prostředí vyjádřily také státy v rezolucích Rady OSN pro lidská práva. V rezoluci z roku 2020 vyzývají státy k „…*podpoře bezpečného a příznivého prostředí pro jednotlivce i skupiny osob pro uplatnění jejich práva na svobodu pokojného shromažďování, projevu a sdružování, a to jak online i offline…*“[145].

---

[140] MIROVALEV, Mansur. *Can Armenia's PM survive protests and a 'coup' attempt?* [online]. Aljazeera, 26. února 2021 [cit. 22. května 2021]. Dostupné na <https://www.aljazeera.com/news/2021/2/26/can-armenias-pm-survive-protests-and-a-coup-attempt>.
[141] Zpráva zvláštního zpravodaje: *A/HRC/41/41*, odst. 22.
[142] *Myanmar 2020* [online]. Amnesty International [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/countries/asia-and-the-pacific/myanmar/report-myanmar/>.
[143] Zpráva zvláštního zpravodaje: *A/HRC/41/41*, odst. 29.
[144] Tamtéž, odst. 66.
[145] Rezoluce Rady OSN pro lidská práva ze dne 23. července 2020, A/HRC/RES/44/20, odst. 4

Do této doby se však jednalo pouze o nezávazné akty, které nejsou vymahatelné. Přelom přišel minulý rok, kdy Výbor pro lidská práva vydal obecný komentář k článku 21 MPOPP, kde v odstavci 6 říká, že „*článek 21 úmluvy chrání pokojné shromažďování kdekoliv se koná: venku, uvnitř a online…*“.[146] Tímto výbor rozšířil výklad tohoto práva i do další roviny, a zajistil tak právní ochranu všem aktivistům a dalším obráncům lidských práv. Kromě práva na pokojné shromažďování však zmiňuje i provázanost s dalšími právy, kterým je třeba zajistit ochranu, „*plná ochrana práva na pokojné shromáždění je možná jenom pokud ostatní, často překrývající se, práva jsou také ochráněna, přesněji svoboda projevu, svoboda sdružování a politické zapojení.*“[147].

Z těchto dvou odstavců bychom mohli odvozovat, že jelikož se ochrana práva na shromažďování vztahuje i na online prostředí, a zároveň, že toto právo požívá plné ochrany pouze pokud i další práva jsou chráněna, tak z toho vyplývá, že aby došlo k naplnění těchto dvou odstavců, tak musí být dosažena i ochrana práva na svobodu projevu a další práva demonstrativně uvedená v tomto obecném komentáři.

[146] Obecný komentář Výboru pro lidská práva ze dne 17. září 2020, CCPR/C/GC/37, odst. 6.
[147] Tamtéž, odst. 9.

5. Přetrvávající otázky v kyberprostoru

5.1. Potřeba právně závazného dokumentu?

Kyberprostor není bezprávní vakuum, z čeho ale vychází jeho právní regulace a jakým způsobem ji aplikovat je otázkou. Možnou odpovědí by mohlo být vytvoření mezinárodní smlouvy, která by zakotvila základní terminologii, práva, a povinnosti států v tomto prostoru.

Přesto, že taková smlouva prozatím neexistuje, snahy o její vytvoření tu rozhodně byly a stále jsou. V roce 1996 Francie předložila dokument Charta pro mezinárodní spolupráci na internetu podpořený Radou Evropské unie, s úmyslem, že tato iniciativa by mohla sloužit k následné regulaci kyberprostoru podobně jako je upraveno mezinárodní mořské právo. Tento návrh však nebyl dostatečně podpořen ostatními státy.[148]

Za francouzskou iniciativou následoval návrh Kodexu chování pro informační bezpečnost předložený Čínou, Ruskem, Tádžikistánem a Uzbekistánem na Valném shromáždění OSN, a to dokonce dvakrát, v roce 2011 a 2015 (podruhé podpořený i Kazachstánem a Kyrgyzstánem). Jejich návrhy se však nesetkaly s kladnou reakcí ostatních států.

Spojené království například vyjádřilo pochybnosti s vágním a terminologicky abstraktním termínem „informační bezpečnost“. *„Termín „informační bezpečnost“ s sebou nese potencionální zmatení, …Spojené království neuznává platnost pojmu „informační bezpečnost“ při jeho užití v tomto kontextu, z důvodu, že by mohl být využitý za účelem legitimování kontrol svobody projevu, které překračují limity stanovené ve Všeobecné deklaraci lidských práv a Mezinárodním paktu o občanských a politických právech.“*[149]

Podpora k vytvoření nového právního instrumentu nebyla vyjádřena ani na úrovni mezivládních odborných skupin při VS OSN. Zprávy GGE neobsahují ve svých doporučeních závazek pokračovat tímto směrem. Změna narativu v této otázce se nabízela při vyjednávání závěrečné zprávy OEWG, která se tímto tématem zabývala. Nicméně na zařazení tohoto bodu do závěrečné zprávy se nakonec státy neshodly, a proto lze najít reference k této diskuzi pouze ve zprávě předsedy

[148] WU, Timothy S. Cyberspace Sovereignty? – The Internet and The International System. *Harvard Journal of Law & Technology,* 1997, roč. 10, s. 660.
[149] Projev Spojeného království z roku 2014, *Response to General Assembly resolution 68/243 “Developments in the field of information and telecommunications in the context of international security”*.

OEWG.[150] Jelikož nedošlo ke shodě na potřebě nového závazného dokumentu, který by byl po právní stránce vymahatelný[151], je zřejmé, že toto bude ještě dlouhodobým předmětem diskuzí o kyberprostoru.

Nicméně určité pokusy, mimo mezinárodní fórum, o regulaci kyberprostoru a stanovení pravidel aplikovatelných v tomto prostoru tu již byly. Tyto pokusy mají společné to, že se jedná pouze o nezávazné dokumenty doporučujícího charakteru.

Jedná se například o Tallinnský manuál, jenž byl vytvořen v roce 2013, a následně aktualizován v roce 2017. Na jeho vytvoření se podíleli světoví odborníci. Tento projekt vznikl na podnět NATO Cooperative Cyber Defence Centre of Excellence, se sídlem v Tallinnu. Estonsko je považováno za tzv. matku kyberprostoru.

Jedná se o poměrně rozsáhlý dokument, který se věnuje vícero oblastem včetně jurisdikce, přičitatelnosti a okrajově i lidským právům. Slouží jako výchozí podklad do dalších diskuzích o mezinárodní regulaci kyberprostoru. Ustanovení totiž vycházejí z obyčejů mezinárodního práva nebo z dalších úmluv. Mačák uvádí, že záměr Talinského manuálu byl v jeho výkladu mezinárodního práva na chování v kyberprostoru, a ne na rozvíjení nebo vytváření nových právních norem. Přestože jsou normy jasně a přesně stanoveny, linie mezi výkladem a tvorbou práva je v tomto případě velmi tenká. Nejedná se tedy o právně závazný text, na kterém by bylo možno dále stavět.[152]

K mezistátním a akademickým pokusům o navrhnutí regulace kyberprostoru, se řadí i iniciativa ze soukromé sféry. Mezinárodní normy kyberprostoru: snižování konfliktů ve světě závislém na internetu (*International Cybersecurity Norms: Reducing conflict in an Internet-dependent world*) je první rozsáhlý a kompletní dokument Microsoftu představený v roce 2014.

Text obsahuje normy zaměřené na zodpovědné chování v online prostoru. Cílem norem bylo zaměření se na definování přijatelného a nepřijatelného chování států a limitovaní tak protiprávních aktivit.[153] Zajímavým prvkem dokumentu je, že doporučuje normy kromě soukromému sektoru, jak se od společnosti dalo předpokládat, i státům. Tvrdí, že normy uvedené v tomto dokumentu by měly být dále

[150] Shrnutí předsedy OEWG ze dne 10. března 2021, A/AC.290/2021/CRP.3*.
[151] Zpráva otevřené pracovní skupiny ze dne 10. března 2021, A/AC.290/2021/CRP.2.
[152] MAČÁK, Kubo. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, 2017, roč. 30, s. 890.
[153] Dokument Microsoftu z roku 2015, *International Cybersecurity Norms* s. 2–3.

použity politiky, diplomaty, akademiky a podnikateli. Microsoft dále pomocí tohoto dokumentu vyzval státy k politické závaznosti obsahu těchto norem. Přesun od právně nezávazných ustanovení k právně závazným normám viděl v zapojení kyberbezpečnosti do agendy OSN, konkrétně začlenění do Návrhu článků o odpovědnosti státu za mezinárodně protiprávní chování. Tento krok vnímal jako nezbytný, avšak zároveň dlouhotrvající a vyžadující spolupráci napříč různými oblastmi.[154]

Microsoft pak v návaznosti na tento dokument (a další vydaný v roce 2016) vyzval státy, aby definované normy kodifikovaly v mezinárodní úmluvě s názvem Ženevská digitální úmluva (*Digital Geneva Convention*). Tato výzva proběhla v roce 2017, nesetkala se však s podporou států, převážně z toho důvodu, že představený návrh nepředkládal závažné důvody, proč by státy měly takovou úmluvu přijmout.[155]

Kyberprostor není jedinou dimenzí, která se ze začátku potýkala s nedostatkem závazných instrumentů, které by ji regulovaly. Příklad můžeme vidět třeba v úpravě vesmíru, který byl po dlouhou dobu podřízen pouze nezávazným normám.[156] I když se může zdát, že přirovnání kyberprostoru k vesmíru je ideální varianta, opak je pravdou. Kyberprostor je na rozdíl od vesmíru uměle vytvořený, s vysokým počtem subjektů využívajících tyto prostory[157] a s proměnlivou povahou. V kyberprostoru se pohybuje mnohem více subjektů než ve vesmíru a zároveň se jedná o oblast, která se neustále vyvíjí mnohem rychleji než vesmír. Nicméně průsečík obou dimenzí se najde i tady, a to v jejich abstraktnosti a složitějším definování hranic.

Další oblast, ze které by se dala čerpat inspirace pro vytvoření mezinárodního instrumentu je Antarktida. Jedná se o oblast, která je upravena arktickým smluvním systémem, který zahrnuje zejména Smlouvu o Antarktidě z roku 1959. Tato smlouva upravila následné vztahy mezi státy, jež si území nárokovaly, a vymezila účel této oblasti.[158] Po této právně závazné smlouvě následovala různá nezávazná ustanovení

[154] Dokument Microsoftu z roku 2015, *International Cybersecurity Norms* s. 2–3.
[155] WALLACE, David, VISGER, Mark. Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. *Journal of Law & Cyber Warfare,* 2018, roč. 6, s. 40.
[156] MAČÁK: *From Cyber Norms*…, s. 892.
[157] MEYER, Paul. Outer Space and Cyberspace: A Tale of Two Security Realms*. International Cyber Norms: Legal, Policy & Industry Perspectives*, 2016, s. 159.
[158] DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. vydání. Praha: Leges, 2011. s. 310.

dále upravující vztahy a pravidla mezi státy k této oblasti, která se postupem času zaintegrovala mezi právně závazné smlouvy.[159]

Mačák ve svém článku dále uvádí jako další vzor i regulaci jaderné bezpečnosti. Tato oblast na právně závazné dokumenty čekala přes tři desítky let, do té doby byla řízena pouze nezávaznými pravidly.[160] Dalším příkladem mohou být také mezinárodní úmluvy pro starší technologie, které fungovaly velmi dobře a byly odrazem mezinárodní spolupráce v této problematice.[161]

V každém z uvedených případů došlo nakonec k regulaci předmětného prostoru právně závaznými dokumenty. Do budoucna to lze vnímat jako důkaz toho, že pouze politicky motivovaná pravidla nejsou dostatečná, ale jsou nezbytná pro nastartování celého procesu.

Výrazným prvkem v celém procesu je převážně role států. Většina zmíněných dokumentů byla iniciována a podporována státy.[162] Jednalo se o jejich priority zájmy, proto se politické závazky překlonily do právních. To je něco, co v problematice kyberprostoru chybí, návrhy jsou buď bez široké podpory napříč státy, či jsou předkládány soukromými subjekty bez většího napojení a spolupráce se státním sektorem.

Nepopíratelnou roli při utváření mezinárodního práva hraje mimo jiné i vliv nevládních organizací. Jejich tematické kampaně mívají kolikrát zásadní dopad.[163] Tyto organizace mohou vytvářet návrhy předmětných smluv, nehledě na to, že se většinou jedná o organizace, které vychází z odborných a výzkumných zpráv, nezávislých na státní politice. Návrhy pak mohou sloužit jako podklad pro stanoviska států a mohou jim nabídnout další pohledy na věc.

To, že tyto organizace mají vliv na zákonodárný proces na mezinárodní úrovni se už několikrát prokázalo v praxi. Jedná se například o Úmluvu proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání (*Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*), která vstoupila v platnost v roce 1987. Jejímu přijetí v roce 1984 předcházela dlouholetá jedenáctiletá kampaň vedená Amnesty International. Kampaň probíhala

[159] MAČÁK: *From Cyber Norms*…, s. 893.
[160] Tamtéž.
[161] PERRITT, Henry H. Jr. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. *Indiana Journal of Global Legal Studies*, 1998, roč. 5, s. 433.
[162] MAČÁK: *From Cyber Norms*…, s. 893.
[163] RYNGAERT, Cedric. Non-State Actors: Carving out a Space in a State-Centred International Legal System. *Netherlands International Law Review*, 2016, s. 188.

v době, kdy se i v OSN diskutovalo přijetí předmětné úmluvy. Iniciativy se pak ujalo Švédsko,[164] které jako členský stát OSN zajistilo potřebnou podporu napříč státy. Dalším příkladem, z nedávné doby je Úmluva OSN o zákazu jaderných zbraní, která vstoupila v platnost v lednu 2021.[165] Za tuto úmluvu silně a dlouhodobě bojovala nezisková organizace ICAN (*The International Campaign to Abolish Nuclear Weapons*), která spolu s dalšími subjekty považuje tento výsledek za důsledek dlouholeté kampaně za jaderné odzbrojení.[166]

Přijetí právně závazného dokumentu podpořil i zvláštní zpravodaj OSN k právu na soukromí ve zprávě z roku 2017, kde uvádí, že *„…právní instrument k regulaci dohledu v kyberprostoru by byl doplňující krok k dalším již existujícím kybernetickým smlouvám...*“[167].

Klíčovým prvkem pro vznik mezinárodní úmluvy bude bezpochyby nutná spolupráce států ve smyslu konkretizování problémů a hledání jejich odpovědí.[168] „*Regulace internetu je globální problém, stejně jako životní prostředí nebo klimatická změna, z toho důvodu, že žádná země se dostatečně nemůže s tímto problémem vypořádat sama.*“[169] Řešením by mohla být harmonizace veškeré národní legislativy, což je ale prakticky nemožné, proto by vznik mezinárodní úmluvy stanovující základní pravidla a terminologii mohl být adekvátní náhradou.[170]

5.2. Kyberprostor jako mezinárodní prostor

Mezinárodní právo se týká oblastí mezi něž se řadí zemský povrch, zemské nitro a mimozemské prostory (kosmický prostor a nebeská tělesa). Podle výkonu svrchovanosti je dělíme na ty, které si státy mohou přivlastnit a na ty, které si přivlastnit nesmějí, tzv. mezinárodní prostory.[171] Právě mezinárodní prostory jsou ty, které nás budu zajímat. Kromě toho, že mezi ně spadá kosmický prostor, nebeská

---

[164] *‘No safe haven for torturers’ – The rocky road to the Convention against Torture* [online]. Amnesty International, 19. listopadu 2014 [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/latest/news/2014/11/no-safe-haven-torturers-rocky-road-convention-against-torture/>.

[165] *Treaty banning nuclear weapons to enter into force* [online]. Aljazeera, 25. října 2020 [cit. 22. května 2021]. Dostupné na <https://www.aljazeera.com/news/2020/10/25/un-treaty-banning-nuclear-weapons-to-enter-into-force>.

[166]. *UN treaty banning nuclear weapons set to enter into force in January force* [online]. UN News, 25. října 2020 [cit. 22. května 2021]. Dostupné na 25. října 2020 <https://news.un.org/en/story/2020/10/1076082>.

[167] Zpráva zvláštního zpravodaje k právu na soukromí ze dne 6. září 2017, A/HRC/34/60, odst. 69.

[168] GOLDSMITH, Jack. Cybersecurity Treaties: A Skeptical View. *Future Challenges in National Security and Law*, 2011, s. 2.

[169] PERRITT: *The Internet as a Threat*…, s. 429.

[170] Tamtéž, s. 430.

[171] DAVID: *Mezinárodní právo…,* s. 291.

tělesa, Antarktida a některé části moře, se diskutuje, zda by mezi ně mohl patřit i kyberprostor. Jedná se totiž o prostor, do kterého mají přístup všechny subjekty, a který jako takový by mohl sloužit všem bez rozdílu. Jeho využívání může být však pozitivní či negativní, proto je potřeba zajistit, že budou platit určité normy a odpovědnost za jejich porušení.

S mezinárodními prostory souvisí i zásada společného dědictví lidstva, jež vyjadřuje právní režim některých prostorů. Tato zásada spočívá v tom, že zamezuje přivlastnění si mezinárodních prostorů, označuje je za věc patřící všem, zavazuje státy k nediskriminačnímu a rovnému podílení se na výzkumu a využívání těchto prostorů, k rozdělování prospěchu, a omezuje je k využívání pouze pro mírové účely.[172] Právě poslední podmínka, využívání mezinárodních prostorů pouze k mírovým účelům, by mohla odrazovat státy od definování kyberprostoru jako dalšího mezinárodního prostoru, čímž by nedošlo k jeho podřazení pod tuto zásadu a jeho užití k válečným aktivitám by nebylo omezeno. Z podobného důvodu je možné se domnívat, že se státy brání aplikaci humanitárního práva v kyberprostoru, protože by to mohlo označit jejich aktivity jako chování ve smyslu ozbrojeného konfliktu.

Zásada společného dědictví lidstva se týká kromě Antarktidy a volného moře všech mezinárodních prostorů. Tyto oblasti jsou také všechny upraveny mimo jiné závaznými mezinárodními úmluvami. I přesto, že se jejich regulace neustále vyvíjí, je to vždy v souladu s touto zásadou. Z poslední doby jsou to například nezávazné dohody Artemis Accords podepsané v říjnu 2020.[173]

To, že je kyberprostor podobný těmto mezinárodním prostorům alespoň některými prvky, je zřejmé již z kapitoly 5.1. této práce. Překážkou by mohla být skutečnost, že se se jedná o prostor, jenž neustále prochází vývojem, ale to, jak je zmíněno výše, by nemusel být problém vzhledem k tomu, že i u ostatních prostorů dochází k upravování podmínek.

K vnímání kyberprostoru jako další možné dimenze mezinárodního práva kladně přistupuje i diskuze vedená z pohledu zajištění obrany. S ohledem na vysokou míru provázanosti kyberprostoru a dalších vojenských domén *„…dále nemá smysl, respektive je neúčelné, a neefektivní uvažovat o vojenských operacích v*

[172] Tamtéž, s. 292.
[173] SVIATKIN, Ivan. *Aktuality vesmírného práva: Výklad pojmu "společné dědictví lidstva" podle Artemis Accords* [online]. epravo.cz, 4. května 2021 [cit. 3. června 2021]. Dostupné na <https://www.epravo.cz/top/clanky/aktuality-vesmirneho-prava-vyklad-pojmu-spolecne-dedictvi-lidstva-podle-artemis-accords-112921.html>.

kyberprostoru jako izolovaných aktech.“[174] Kyberprostor jako další válečnou doménu nicméně potvrzuje ve svém článku i Rex Hughes *„…správně či špatně, kyberprostor se vskutku stal pátou válečnou doménou“.*[175]

Nabízela by se otázka, zda kyberprostor již nespadá pod nějaký mezinárodní prostor. Avšak když se podíváme na prvky této oblasti, tak můžeme konstatovat, že se jedná o naprosto jinou dimenzi. Dalo by se říci, že Kyberprostor je takový hybrid. Nejen, že není fyzicky uchopitelný či ohraničitelný jako půda nebo voda, ale zároveň je mnohem více přístupný než vzduch nebo kosmický prostor. Co má však s těmi posledními prostory společné je to, že je všude, a tudíž je odkudkoliv přístupný.

[174] BASTL, Martin, GRUBEROVÁ, Zuzana. Kyberprostor jako „pátá doména"? *Vojenské rozhledy*, 2013, roč. 22.
[175] HUGHES, Rex. A treaty for cyberspace. *International Affairs*, 2010, roč. 86, s. 540.

Závěr

Moderní technologie, internet a další technické systémy mají reálný dopad na lidská práva. Jejich využívání právě pro protiprávní aktivity nabírá velmi širokého rozsahu, jak lze vidět ve čtvrté kapitole. Přičemž samotné technologie nelze rozdělit na dobré a špatné, až jejím využitím pro různé aktivity může dojít k negativním či pozitivním dopadům. Tudíž jejich základní povaha se pak mění vlivem lidské činnosti. Proto je důležité, aby tato činnost byla určitým způsobem regulována.

Je zřejmé, že na aplikaci lidskoprávních instrumentů v kyberprostoru panuje mezi státy politická shoda. Není tedy potřeba se touto otázkou dále zabývat. Další diskuzí by spíše mělo být definování jakým způsobem tyto závazky aplikovat. Přičemž se často zapomíná na to, že zde již platné mezinárodní právo máme, a podobně jako se aplikuje na ostatní mezinárodní prostory by bylo možné ho aplikovat i na kyberprostor.

Z práce vyplývá, že vynucování práv obsažených v MPOPP v kyberprostoru nic nebrání. Co se týče jurisdikce, dá se pomocí extrateritoriálního principu aplikovat i na osoby či území umístěné mimo státní hranice, což je v kontextu kyberprostoru zásadní. Aby však nad daným chováním mohl stát uplatnit svou jurisdikci, je potřeba, ale bylo přičitatelné státu. V tomto bodě tak nastává největší problém, hackerské útoky bývají často podniknuty soukromými společnostmi, které sice vykonávají vůli státu, ale není možné, nebo je to velmi obtížné, opravdu zjistit původního pachatele, a tudíž přičíst toto chování státu. Ve třetí kapitole, se nabízí několik možných řešení, alespoň z akademického hlediska. Hlavní myšlenka spočívá v tom, že se využijí podmínky, které se aplikují při fyzických útocích, a upraví se na útoky hackerské.

Přestože na akademické půdě jsou již některé názory zformulovány, pro vývoj kyberprostoru a lidských práv jsou nezbytné i další kroky, a to aktivnější přístup států, zapojení dalších zúčastněných stran, a vytvoření mezinárodního instrumentu.

Mezinárodní právo a jeho tvorba je závislá na vůli států. Nabízí se tak, jako jedna z možných variant, aktivnější přístup států spolu se soudními institucemi. Pokud by státy při formování svých stanovisek a při mezinárodních diskuzích využívaly akademických výzkumů a zpráv příslušných orgánů, mohlo by dojít k určitému posunu z otázky, jak aplikovat mezinárodní právo včetně lidských práv k jejich skutečnému dodržování. Zároveň se zde nabízí i využití role soudů. Ty ve svých rozhodnutích dotváří právo, jejich velký význam byl několikrát zmíněn během

této práce. Pokud by soudy v rozhodnutích týkajících se, byť jen okrajově, informačních a komunikačních technologií formovaly určitý dílčí právní názor, tak už by se jednalo o posun směrem kupředu. Jako příklad může sloužit i situace ohledně Čagoských ostrovů, jež byla dlouhou dobu předmětem sporu mezi Spojeným královstvím a Mauriciem. Mezinárodní tribunál pro mořské právo však v nedávné době, v rozsudku týkajícím se jiné věci, uvedl, že souostroví Čagos spadá pod suverenitu Mauricia. Vzhledem k tomu, že tento rozsudek je právně závazný, dá se z něho implikovat i závaznost této skutečnosti.[176]

S aktivním přístupem výše zmíněných subjektů plně souvisí zapojení dalších aktérů. Především pak neziskových organizací a technických expertů. Jelikož neziskové organizace většinou reprezentují občanskou společnost, a díky jejich nezávislosti na státní moci mají důvěru jedinců, tak se jedná o ideální skupinu, která může zvyšovat povědomí o negativních dopadech moderních technologií. Jejich role je unikátní také v tom ohledu, že zároveň mohou vytvářet i určitý nátlak na státy, a tím zajišťovat jejich odpovědnost za učiněné sliby či při dodržování závazků. I když samozřejmě existují takové organizace, které se tomuto tématu věnují, jako je například Article 19, stále jich není dostatek.

Co se týče druhého prvku, a to technických expertů, spolupráce s nimi je důležitá ze dvou úhlů pohledu. Zaprvé zapojení těchto osob je nezbytné právě při řešení technických náležitostí přičitatelnosti chování státu, jak jde vidět ve třetí kapitole, přičitatelnost vytváří jeden z největších problémů v kyberprostoru. V praxi kolikrát tvoří velký problém právě nalezení prvotního pachatele daného chování. V tom by právě větší zapojení expertů mohlo být nápomocné, nehledě na to, že by mohli působit již proaktivně, spíše než jen reaktivně.

Další zapojení odborníků a využití jejich expertízy je důležité právě při vytváření právně závazného dokumentu. Pochopení fungování internetu a informačních a komunikačních technologií je klíčem pro nastavení regulativy, která by opravdu cílila na podporu a ochranu lidských práv při jejich využívání. Propojením všech zúčastněných stran a kladením důrazu na sdílené znalosti by mohlo dojít k pozitivnímu pokroku v tomto směru.

---

[176] PETKAR, Vishwanath. *UN maritime tribunal rules no UK sovereignty over Chagos Islands* [online]. Jurist, 30. ledna 2021 [cit. 3. června 2021]. Dostupné na <https://www.jurist.org/news/2021/01/un-maritime-tribunal-rules-no-uk-sovereignty-over-chagos-islands/>.

Poslední oblast, jež v budoucnu bude hrát velmi důležitou roli je právě tvorba mezinárodního instrumentu. Vývoj tohoto kroku je nastíněn v páté kapitole. I přes převažující neshodu států ohledně tohoto tématu, však z akademických článků a příspěvků vyplývá, že mezinárodní úmluva na kyberprostor je tím správným krokem. Tento názor je stavěn na základě okolností vzniku jiných regulací, jako je například arktický či vesmírný právní systém. Regulace oblasti, jež je velmi podobná dalším mezinárodním prostorům by měla být upravena mezinárodní smlouvou, která bude dále navazovat na již existující smlouvy a závazky států. Protiargumentem tohoto názoru je fakt, že kyberprostor je oblast, která se vyvíjí rychleji, než je právní systém schopen reagovat. Každých pár let se objevují nové a nové technologie a systémy, na které by se tato úmluva měla také vztahovat. Otázkou tak zůstává, jak to podchytit, aby úmluva nepůsobila obsoletně. Jisté však je, že správnou odpovědí nebude případná nečinnost států v tomto ohledu, ale naopak proaktivní a inovativní přístup a náhled na tuto situaci.

Nabízela by se zde ještě i možnost vzniku mezinárodního práva pomocí pramenů ve formě obyčejových pravidel. Pro jejich vznik je však potřeba naplnění dvou prvků, jenž v sobě nesou mimo jiné i opakování, nepřetržitost a stejnorodost. V kontextu kyberprostoru by právě dosažení těchto náležitostí mohlo působit problém vzhledem k rychlému vývoji, proto by se přijetí mezinárodní úmluvy mohlo jevit jako schůdnější cesta. I přes prvotní neshody mezi státy, jak bylo možné vidět ze zpráv GGE a OEWG, je zde určitý pokrok vpřed. Přinejmenším zde panuje shoda a vůle na pokračování v dialogu.

Zřejmé je, že tato problematika bude předmětem několika následujících let, a to na všech platformách. Jisté taky je, že kyberprostor není bezprávní vakuum, a nejen lidskoprávní závazky v něm musí být dodržovány.

Seznam použité literatury

Monografie a učebnice

ČEPELKA, Čestmír, ŠTURMA, Pavel. *Mezinárodní právo veřejné*. Praha: C.H. Beck, 2018. 549 s.

DAVID Vladislav a kol. *Mezinárodní právo veřejné s kazuistikou*. 2. vydání. Praha: Leges, 2011. 448 s.

FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 1, Dokumenty.* Praha: Leges, 2015, 429 s.

FAIX, Martin, BUREŠ, Pavel, SVAČEK, Ondřej. *Rukověť ke studiu mezinárodního práva 2, Praktikum.* Praha: Leges, 2017, 174 s.

ONDŘEJ, Jan, MRÁZEK Josef, KUNZ Oto. *Základy mezinárodního práva veřejného*. Praha: C.H. Beck, 2018. 271 s.

RYNGAERT, Cedric. *Jurisdiction in International Law*. Oxford: New York, N.Y.: Oxford University Press, 2008. 241 s.

SHAW, Malcolm N. *International Law*. UK: Cambridge University Press, 2008. 1542 s.

SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013, 282 s.

SMITH, Rhona K.M. *Textbook on international human rights*. Oxford, New York, N.Y.: Oxford University Press, 2010, 399 s.

TSAGOURIAS, Nicholas, BUCHAN, Russell. *Research handbook on international law and cyberspace*. Cheltenham, UK, Northampton, MA: Edward Elgar Publishing, 2017, 517 s.

Články z odborných časopisů

BASTL, Martin, GRUBEROVÁ, Zuzana. Kyberprostor jako „pátá doména"? *Vojenské rozhledy*, 2013, roč. 22.

GOLDSMITH, Jack. Cybersecurity Treaties: A Skeptical View. *Future Challenges in National Security and Law*, 2011.

HUGHES, Rex. A treaty for cyberspace. *International Affairs*, 2010, roč. 86, s. 523 - 541.

MAČÁK, Kubo. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict & Security Law,* 2016, roč. 21, s. 405–428.

MAČÁK, Kubo. From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, 2017, roč. 30, s. 877 - 899.

MEYER, Paul. Outer Space and Cyberspace: A Tale of Two Security Realms. *International Cyber Norms: Legal, Policy & Industry Perspectives*, 2016, s. 155 - 169.

PERRITT, Henry H. Jr. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. *Indiana Journal of Global Legal Studies*, 1998, roč. 5, s. 423 - 442.

RYNGAERT, Cedric. Non-State Actors: Carving out a Space in a State-Centred International Legal System. *Netherlands International Law Review*, 2016, s. 183 - 195.

TSAGOURIAS, Nicholas. Cyber attacks, self-defence and the problem of Attribution. *Journal of Conflict & Security Law,* 2012, roč. 17, s. 229 – 244.

WALLACE, David, VISGER, Mark. Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. *Journal of Law & Cyber Warfare,* 2018, roč. 6, s. 3 - 55.

WU, Timothy S. Cyberspace Sovereignty? – The Internet and The International System. *Harvard Journal of Law & Technology,* 1997, roč. 10, s. 648 – 666.

Internetové zdroje

Developments in the field of information and telecommunications in the context of international security [online]. UNODA, [cit. 22. května 2021]. Dostupné na <https://www.un.org/disarmament/ict-security/>.

Edward Snowden: Leaks that exposed US spy programme [online]. BBC, 17. ledna 2014 [cit. 22. května 2021]. Dostupné na <https://www.bbc.com/news/world-us-canada-23123964>.

ERBEN, Lukáš. *Příchod hackerů: příběh Stuxnetu* [online]. root.cz, 29. dubna 2014 [cit. 10. května 2021]. Dostupné na <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/>.

FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. CSO, 22. srpna 2017 [cit. 15. května 2021]. Dostupné na <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html>.

G8 Declaration - Renewed Commitment For Freedom And Democracy [online]. NATO [cit. 22. března 2021]. Dostupné na <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf>.

International human rights law [online]. Dostupné na <https://cyberlaw.ccdcoe.org/wiki/International_human_rights_law>.

ITTELSON, Pavlina, RADUNOVIC, Vladimir. *What's new with cybersecurity negotiations? UN Cyber OEWG Final Report analysis* [online]. Diplo, 19. března 2021 [cit. 23. května 2021]. Dostupné na <https://www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-cyber-oewg-final-report-analysis>.

KUSHNER, David. *The Real Story of Stuxnet* [online]. ieee spectrum, 26. února 2013 [cit. 15. května 2021]. Dostupné na <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.

Metadata [online]. Tech Terms, [cit. 10. května 2021]. Dostupné na <https://techterms.com/definition/metadata>.

MIROVALEV, Mansur. *Can Armenia's PM survive protests and a 'coup' attempt?* [online]. Aljazeera, 26. února 2021 [cit. 22. května 2021]. Dostupné na <https://www.aljazeera.com/news/2021/2/26/can-armenias-pm-survive-protests-and-a-coup-attempt>.

Myanmar 2020 [online]. Amnesty International [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/countries/asia-and-the-pacific/myanmar/report-myanmar/>.

NAKASHIMA, Ellen. *Stuxnet was work of U.S. and Israeli experts officials say* [online]. The Washington Post, 2. června 2012 [cit. 27. května 2021]. Dostupné na <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.

'No safe haven for torturers' – The rocky road to the Convention against Torture [online]. Amnesty International, 19. listopadu 2014 [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/latest/news/2014/11/no-safe-haven-torturers-rocky-road-convention-against-torture/>.

O'NEILL, Patrick Howell. *Ransomware did not kill a German hospital patient* [online]. MIT Technology Review, 12. prosince 2020 [cit. 22. února 2021]. Dostupné na <https://www.technologyreview.com/2020/11/12/1012015/ransomware-did-not-kill-a-german-hospital-patient/>.

PAUL, Kari, BECKETT, Lois. *What we know – and still don't – about the worst-ever US government cyber-attack* [online]. The Guardian, 19. prosince 2020 [cit. 22. února 2021]. Dostupné na <https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government>.

PETKAR, Vishwanath. *UN maritime tribunal rules no UK sovereignty over Chagos Islands* [online]. Jurist, 30. ledna 2021 [cit. 3. června 2021]. Dostupné na <https://www.jurist.org/news/2021/01/un-maritime-tribunal-rules-no-uk-sovereignty-over-chagos-islands/>.

SVIATKIN, Ivan. *Aktuality vesmírného práva: Výklad pojmu "společné dědictví lidstva" podle Artemis Accords* [online]. epravo.cz, 4. května 2021 [cit. 3. června 2021]. Dostupné na <https://www.epravo.cz/top/clanky/aktuality-vesmirneho-prava-vyklad-pojmu-spolecne-dedictvi-lidstva-podle-artemis-accords-112921.html>.

TIDY, Joe. *Police launch homicide inquiry after German hospital hack* [online]. BBC, 18. září 2020 [cit. 22. února 2021]. Dostupné na <https://www.bbc.com/news/technology-54204356>.

TIDY, Joe. *SolarWinds hack: Russian denial 'unconvincing'* [online]. BBC, 18. května 2021 [cit. 5. června 2021]. Dostupné na <https://www.bbc.com/news/technology-57156197>.

Treaty banning nuclear weapons to enter into force [online]. Aljazeera, 25. října 2020 [cit. 22. května 2021]. Dostupné na <https://www.aljazeera.com/news/2020/10/25/un-treaty-banning-nuclear-weapons-to-enter-into-force>.

UN treaty banning nuclear weapons set to enter into force in January force [online]. UN News, 25. října 2020 [cit. 22. května 2021]. Dostupné na 25. října 2020 <https://news.un.org/en/story/2020/10/1076082>.

VÄLJATAGA, Ann. *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly* [online]. CCDCOE, [cit. 23. května 2021]. Dostupné na <https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/>.

Warsaw Summit Communiqué [online]. NATO, 9. července 2016 [cit. 22. března 2021]. Dostupné na <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.

We Sense Trouble: Automated Discrimination And Mass Surveillance In Predictive Policing In The Netherlands [online]. Amnesty International, 29. září 2020 [cit. 22. května 2021]. Dostupné na <https://www.amnesty.org/en/documents/eur35/2971/2020/en/>.

Dokumenty mezinárodních orgánů a dalších expertů

Dokument Výboru pro lidská práva ze dne 17. listopadu 2016, CCPR/C/COL/CO/7.

Shrnutí předsedy OEWG ze dne 10. března 2021, A/AC.290/2021/CRP.3*.

UNESCO. *First Draft Of The Recommendation On The Ethics Of Artificial Intelligence.* Paříž: Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, 2020.

Zpráva otevřené pracovní skupiny ze dne 10. března 2021, A/AC.290/2021/CRP.2.

Zpráva skupiny vládních expertů ze dne 24. června 2013, A/68/98.

Zpráva skupiny vládních expertů ze dne 22. července 2015, A/70/174.

Zpráva UNIDIR z roku 2017, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*.

Zpráva Úřadu vysoké komisařky OSN pro lidská práva ze dne 30. června 2014, A/HRC/27/37.
Zpráva Úřadu vysoké komisařky OSN pro lidská práva ze dne 3. srpna 2018, A/HRC/39/29.

Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 11. května 2016, A/HRC/32/38.

Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 6. dubna 2018, A/HRC/38/35.

Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 29. srpna 2018, A/73/348.

Zpráva zvláštního zpravodaje ke svobodě projevu a názoru ze dne 23. dubna 2020, A/HRC/44/49.

Zpráva zvláštního zpravodaje ke svobodě shromažďování a sdružování ze dne 17. května 2019, A/HRC/41/41.

Zpráva zvláštního zpravodaje k právu na soukromí ze dne 6. září 2017, A/HRC/34/60.

Zpráva zvláštního zpravodaje k právu na soukromí ze dne 28. února 2018, A/HRC/37/62, příloha.

Mezinárodní právní prameny

Mezinárodní pakt o občanských a politických právech ze dne 19. prosince 1966 přijatého na půdě Organizace spojených národů, s Protokoly č. 1 a 2

Návrh článků o odpovědnosti státu za mezinárodně protiprávní chování z roku 2001

Všeobecná deklarace lidských práv ze dne 10. prosince 1948

Právní předpisy

Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

Komentáře

International Law Commission. *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 2001.

Obecný komentář Výboru pro lidská práva ze dne 29. března 2004, CCPR/C/21/Rev.1/Add. 1326.

Obecný komentář Výboru pro lidská práva ze dne 12. září 2011, CCPR/C/GC/34.

Obecný komentář Výboru pro lidská práva ze dne 17. září 2020, CCPR/C/GC/37.

Rezoluce OSN

Rezoluce Rady OSN pro lidská práva ze dne 18. července 2016, A/HRC/RES/32/13

Rezoluce Rady OSN pro lidská práva ze dne 17. července 2018, A/HRC/RES/38/7

Rezoluce Rady OSN pro lidská práva ze dne 5. října 2018, A/HRC/RES/39/6

Rezoluce Rady OSN pro lidská práva ze dne 7. října 2019, A/HRC/RES/42/15

Rezoluce Rady OSN pro lidská práva ze dne 23. července 2020, A/HRC/RES/44/20

Rezoluce Rady OSN pro lidská práva ze dne 24. července 2020, A/HRC/RES/44/12

Rezoluce Valného shromáždění OSN ze dne 30. října 2020, A/C.3/75/L.40

Rozhodnutí soudů a jiných tribunálů

Poradní posudek Mezinárodního soudního dvora ze dne 9. července 2004, *Právní dopady výstavby zdi na okupovaném palestinském území*.

Rozsudek Evropského soudu pro lidská práva ze dne 23. března 1995, *Loizidou v. Turecko*, 15318/89

Rozsudek Evropského soudu pro lidská práva ze dne 4. prosince 2015, *Roman Zakharov v. Rusko*, 47143/06

Rozsudek Evropského soudu pro lidská práva ze dne 21. prosince 2016, *Tele2 Sverige a Secretary of State for the Home Department v. Post- och telestyrelsen a další, s*pojené věci C-203/15 a C-698/15

Rozsudek Mezinárodního soudního dvora z 27. června 1986, *Nikaragua v. USA*.

Rozsudek Mezinárodního soudního dvora z 26. února 2007, *Bosna a Hercegovina v. Srbsko a Černá Hora*.

Rozsudek Mezinárodního trestního tribunálu pro bývalou Jugoslávii z 15. července 1999, *The Prosecutor v.Tadić*.

Další zdroje

Dokument Microsoftu z roku 2015, *International Cybersecurity Norms*.

Projev Spojeného království z roku 2014, *Response to General Assembly resolution 68/243 "Developments in the field of information and telecommunications in the context of international security*".

Abstrakt

Diplomová práce se zaměřuje na zmapování mezinárodních lidskoprávních závazků států v kyberprostoru. Cílem je zodpovězení výzkumných otázek, jež se týkají aplikace mezinárodního práva v kyberprostoru, na což pak navazuje otázka dodržování mezinárodních závazků států v kyberprostoru, a to jak závazných, tak nezávazných. Zbývající otázkou je vztah lidských práv a kyberprostoru, a to jak po stránce právní, tak praktické z pohledu incidentů, které se v minulých letech udály.

Práce je dělena do pěti kapitol. V první kapitole dochází k vymezení pojmu kybernetického prostoru, internetu, a informačních a komunikačních technologií. Další kapitola se pak věnuje přehledu mezinárodních závazků států mimo MPOPP, na který je zaměřena třetí kapitola, která se dotýká i jurisdikce a přičitatelného chování státu v kyberprostoru. Ve čtvrté kapitole jsou podrobněji rozebírána tři lidská práva v kontextu kybernetického prostoru, a poslední kapitola se věnuje otázce přijetí nové mezinárodní úmluvy a definici kyberprostoru jako mezinárodního prostoru.

Abstract

The diploma thesis focuses on mapping the international human rights obligations of states in cyberspace. The aim is to answer the following research questions. Such as the question of whether international law is applicable in cyberspace, followed by the question of the obligations of states to abide by the international law in cyberspace. The remaining question is the relationship between human rights and cyberspace, both legal and practical. Which is expressed by using the real incidents that have occurred in recent years.

The thesis is divided into five chapters. The first chapter defines the concept of cyberspace, Internet, and Information and Communication Technologies. The next chapter covers a short overview regarding international States' obligations, other than arising from ICCPR. Which is the focus of the next chapter together including jurisdiction and attribution of states in cyberspace. The following chapter contains in deep description of three concrete human rights in the context of cyberspace. And the last chapter addresses the issue of the adoption of a new international binding instrument and the definition of cyberspace as an international space.

Klíčová slova

Kybernetický prostor, lidská práva, organizace spojených národů, mezinárodní právo, informační a komunikační technologie, internet, Mezinárodní pakt o občanských a politických právech.

Key words

Cyberspace, Human Rights, United Nations, International law, Information and Communication Technologies, Internet, International Covenant on Civil and Political Rights.