UNIVERZITA KARLOVA

Právnická fakulta

Marek Teššer

Legitimita masivního sledování a sběru dat v mezinárodním právu

Diplomová práce

Vedoucí diplomové práce: JUDr. Milan Lipovský, Ph.D.

Katedra mezinárodního práva

Datum vypracování práce (uzavření rukopisu) : 12. září 2017

UNIVERZITA KARLOVA

Právnická fakulta

Marek Teššer

Legitimita masívneho sledovania a zberu dát v medzinárodnom práve

Diplomová práca

Vedúci diplomovej práce: JUDr. Milan Lipovský, Ph.D.

Katedra medzinárodného práva

Dátum vypracovania práce (uzavretie rukopisu) : 12. septembra 2017

Prohlašuji, že předloženou diplomovou práci jsem vypracoval samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Marek Teššer

V Praze dne 15. září 2017

Poďakovanie

Úprimne by som sa týmto chcel poďakovať môjmu vedúcemu práce, pánovi doktorovi Lipovskému, za jeho ochotu viesť túto prácu, pomáhať mi, poskytovať cenné rady a za to, že mi dal možnosť zúčastniť sa medzinárodného mootcourtu Jessup, ktorého prípad ma inšpiroval k výberu témy diplomovej práce. Zároveň by som sa chcel poďakovať všetkým členom katedry medzinárodného práva, ktorí mi počas štúdia a môjho pôsobenia na katedre boli vždy oporou a príjemnou spoločnosťou.

Obsah

Úvod

Od udalostí z 11. septembra 2001 sa väčšina legislatívnej činnosti venujúcej sa boju proti terorizmu zamerala práve na rozširovanie právomocí vládnych orgánov v sledovacom odvetví.[1] Efektívny boj proti terorizmu a organizovanému zločinu je jednou z najväčších výziev dnešnej doby na poli bezpečnosti. Žiaľ, aj tieto formy kriminálnej činnosti idú tak povediac „s dobou" a prispôsobujú svoje aktivity moderným technológiám. Terorizmus aj organizovaný zločin stále vo väčšom používajú ku komunikácií a koordinácií prostriedky ako internet a iné digitálne technológie. Je preto samozrejmé, že sa aj pozornosť tajných služieb upriamuje na túto formu komunikácie. V dôsledku toho boli vytvorené a schválené sledovacie programy, ktoré majú na jednej strane potenciál úspešne bojovať proti terorizmu, no na druhej strane, v prípade svojho zneužitia, môžu vážne ohroziť základy slobody a demokracie v našej spoločnosti.

V roku 2013 šokoval mladý zamestnanec firmy *Booz Allen Hamilton* celý svet, keď novinárom z britského denníka *The Guardian* poskytol prísne tajné informácie o elektronických sledovacích programoch americkej Národnej bezpečnostnej agentúry (ďalej len „NSA") a britského Vládneho komunikačného ústredia (ďalej len „GCHQ). Zatiaľ čo novinári začali vo veľkom informovať svet o sledovacích praktikách tajných služieb, *whistleblower* Edward Snowden sa stal v očiach americkej vlády nepriateľom číslo jeden. Ľudia a vlády po celom svete zostávali v najbližších mesiacoch v nemom úžase nad rozsahom sledovacích aktivít. Medzinárodný škandál vyvolalo nie len to, že tieto tajné služby mali k dispozícií technické možnosti v reálnom čase sledovať v podstate kohokoľvek, ale aj to, že sa aktívne zapájali do sledovania hláv iných štátov, často aj ich najbližších spojencov.

V dôsledku vyššie spomenutého úniku pomerne detailných informácií o niektorých najvýznamnejších programoch americkej a britskej vlády sa v tejto práci venujem práve analýze súladu týchto programov s medzinárodným právom. Dôraz pritom kladiem na ich kompatibilitu s medzinárodne uznávanými štandardmi ľudských práv, hlavne s právom jednotlivca na ochranu súkromia, vyjadrenými v Medzinárodnom pakte o občianskych a politických právach[2] (ďalej len „Pakt") a Európskom dohovore o ochrane

[1] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 December 2009, A/HRC/13/37, para. 20.
[2] Medzinárodný pakt o občianskych a politických právach, 16. december 1966, 999 UNTS 171 (účinnosť 23. marec 1976).

ľudských práv a základných slobôd[3] (ďalej len „Dohovor“). Otázky, ktoré som si pre účely práce položil, sú nasledovné:

1. Sú tieto medzinárodnoprávne dokumenty aplikovateľné v tomto kontexte (aj extrateritoriálne)?
2. Je vôbec v nejakej situácií prípustné (z pohľadu medzinárodného práva), aby štát vykonával masívne sledovanie? Pokiaľ áno, aké podmienky musia byť splnené, aby nedošlo k svojvoľnému zásahu do súkromia osôb?

Prvá kapitola sa zaoberá všeobecnou charakteristikou súkromia ako takého a jednotlivých inštrumentov ochrany ľudských práv, ktoré ho upravujú. Detailne sa venuje hlavne systému ochrany podľa Paktu a Dohovoru, nakoľko tie sú aplikovateľné na skúmané prípady zásahu do súkromia.

Druhá kapitola približuje problematiku kyberpriestoru ako sféry práva a predstavuje druhy sledovania pričom popisuje ako elektronické sledovanie a zber informácií ohrozuje právo na súkromie a súvisiace práva. Nasleduje analýza aplikovateľnosti Paktu a Dohovoru v kontexte elektronického sledovania s dôrazom na stále aktuálnu otázku extrateritoriálnej aplikovateľnosti týchto zmlúv.

Tretia kapitola začína stručným popisom fungovania najznámejších programov NSA a GCHQ na sledovanie a následne analyzuje kompatibilitu týchto programov s medzinárodným právom so zameraním na aspekt ochrany ľudských práv.

Štvrtá kapitola sa venuje druhému aspektu elektronického sledovania – hospodárskej a diplomatickej špionáži. Nakoľko sa táto práca zameriava hlavne na zásah do súkromia a táto téma by vydala na samostatnú prácu, sú v tejto kapitole len v stručnosti načrtnuté najzávažnejšie problémy s tým, že vo zvyšku autor odkazuje na ďalšie skúmanie.

Nakoľko sa jedná o prácu z oblasti medzinárodného práva, väčšina prameňov je cudzojazyčného charakteru. Niektoré citácie pod čiarou sú ponechané v origináli a všetky preklady sú neoficiálne, urobené autorom práce. Pre účely tejto práce bolo treba pracovať s materiálmi týkajúcimi sa tajných programov NSA a GCHQ, ktoré sú neoficiálne a pochádzajú z archívov E. Snowdena. Tieto dokumenty sú voľne prístupné na internete.

[3] Európsky Dohovor o ochrane ľudských práv a základných slobôd, 4. november 1950, ETS No. 5, (účinnosť 3. september 1953).

1. O práve na súkromie všeobecne

Táto kapitola popisuje základné pojmy ako právo na súkromie a jeho ochrana. Pre účely diplomovej práce je dôležitá hlavne z toho dôvodu, že približuje fungovanie ochrany súkromia v praxi, popisuje najdôležitejšie orgány na poli ochrany súkromia a vysvetľuje, aké základné princípy musia byť dodržiavané, ak chce štát do súkromia osôb zasiahnuť v súlade s medzinárodným právom.

1.1 Definícia súkromia a právo na súkromie

Správne zadefinovať súkromie je jedna z najzložitejších úloh pri jeho skúmaní. Definícií súkromia existuje mnoho, niektoré sú širšie, niektoré užšie. Z historického hľadiska bol pojem súkromia, lat. *privatus,* chápaný skôr pejoratívne. Popisoval osobu, ktorá sa buď nechcela, alebo nemohla zúčastniť správy vecí verejných.[4] V modernej dobe sa pojem súkromie pretransformoval až do podoby, akú poznáme dnes, no ani tá nie je úplne ustálená.

Problém zadefinovať súkromie sa prejavil už pri príprave Paktu, kedy článok 17, ktorý upravuje právo na súkromie, nebol skoro vôbec predmetom diskusií.[5] Nie je potom divu, že sa dodnes vedú neustále spory o tom, čo to „súkromie" vlastne znamená a kde sú jeho hranice. V súvislosti s touto problematikou sa výstižne vyjadril Herndl vo svojom nesúhlasnom stanovisku k prípadu *Coeriel*[6], keď situáciu popísal nasledovne:

> *„Článok 17 je jedným zo záhadnejších ustanovení Paktu. Predovšetkým pojem „súkromie" je, zdá sa, otvorené výkladu. Čo súkromie vlastne znamená? Vo svojej práci „Global protection of Human Rights – Civil Rights", Lillich nazýva súkromím koncept zatiaľ natoľko beztvárnym, že to zamedzuje jeho akceptácii v rámci medzinárodného obyčajového práva."*[7]

[4] Savin, Andrej, and Edward Elgar Publishing. *EU Internet Law*. Northampton, Mass., E. Elgar, 2013, s.1.
[5] Nowak, Manfred. *U. N. Covenant on Civil and Political Rights: CCPR Commentary*. Kehl [Etc.], Engel, 1993, s. 294.
[6] HRC: Coeriel et al. v. Holandsko, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994).
[7] HRC: Coeriel et al. v. Holandsko, Individual opinion by Mr. Kurt Herndl (dissenting).

Vo všeobecnosti sa však súkromie charakterizuje ako priestor každej osoby na samostatný vývoj, interakciu a slobodu, teda svoju vlastnú súkromnú sféru, či už so súčinnosťou okolia, alebo nie, oslobodenú od zásahov štátu a od neprimeraných a nežiadúcich zásahov iných osôb.[8] Inak povedané, ide o záujem osoby utajiť o sebe určité informácie.

V poslednej dobe ale pojem súkromie a záujem oň upadá.[9] Objavujú sa dokonca názory, že súkromie, ako ho poznáme, je vecou minulosti.[10] S rozvojom informačných technológií o sebe dnes majú možnosť ľudia vedieť oveľa viac ako kedysi a pomyselná čiara medzi verejným a súkromným sa tak stráca. Dôsledkom toho je, že si ľudia môžu zužovať koncept súkromia a chápať ho len ako ochranu osobných údajov. Súkromie je ale omnoho širší koncept. *Privacy international*[11] pracuje so 4 aspektami súkromia:

a) súkromie teritoriálne;
b) súkromie fyzické (telesné) ;
c) súkromie informačné;
d) súkromie komunikácie.[12]

Teritoriálne súkromie zahŕňa ochranu pred zásahom do fyzického priestoru, pričom sa neobmedzuje len na domáce prostredie, ale zahŕňa napríklad aj pracovné priestory. Súkromie fyzické (telesné), ako aj názov naznačuje, je súkromie týkajúce sa bezprostredne tela osôb. Informačné súkromie zahŕňa ochranu osobných informácií, ako sú napríklad lekárske záznamy. No a konečne súkromie komunikácií chráni osoby pred zásahom do ich komunikácie, nech už je v akejkoľvek forme (list, e-mail, telefonický hovor).

Právo na súkromie v sebe zahŕňa povinnosť štátu toto právo rešpektovať, chrániť a napĺňať. Štát sa musí zdržať neodôvodnených zásahov, musí si vo vlastnom právnom poriadku upraviť konkrétny zákaz zasahovania aj pre tretie osoby a efektívne ho vynucovať. Štát má teda celý rad pozitívnych aj negatívnych záväzkov, ktoré musí naplniť. Zároveň je ale potrebné zdôrazniť, že žiaden medzinárodný dokument nechápe právo

[8] Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004, para. 4.82.
[9] Rule, James. Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience, OUP, 2009.
[10] Cohen, Julie E. "What Privacy Is for. (Privacy Self-Management and the Consent Dilemma)." *Harvard Law Review*, vol. 126, no. 7, 2013, pp. 1904–1933, s. 1.
[11] Privacy International je nezisková organizácia, založená v roku 1990, ktorá má za cieľ „*byť strážnym psom (rozmachu) dohľadu (nad obyvateľstvom) zo strany vlád a korporácií*".
[12] Zureik, E., Stalker, L., & Smith, E. Surveillance, Privacy, and the Globalization of Personal Information International Comparisons. Montreal: McGill-Queen's University Press, 2014, s. 13.

na súkromie ako právo absolútne. Jeho relatívnosť je logická, nakoľko je pomerne často v konflikte s inými právami, najčastejšie s právom na slobodu prejavu.[13]

Právo na súkromie náuka rozdeľuje do troch dimenzií.[14] Toto rozdelenie je však možné pozorovať aj v jednotlivých medzinárodných zmluvách. Ide o rešpektovanie:

1. Súkromia;
2. Komunikácie;
3. Domova.

Rešpektovanie súkromia je najširšia kategória. Niektoré medzinárodné zmluvy, napríklad Dohovor, to pomenúvajú ako ochrana súkromného, prípadne rodinného života. Zatiaľ čo Pakt chráni súkromie (*privacy*), Všeobecná deklarácia ľudských práv[15] (ďalej len „Deklarácia") a aj Dohovor chránia súkromný život (*private life*). Vo všeobecnosti sa jedná o zabezpečenie priestoru pre individuálne sebaurčenie a rozvoj jedinca bez vonkajšieho zasahovania.[16] Sem sa teda zaraďuje aj samotná ochrana pred sledovaním zo strany štátu. Európsky súd pre ľudské práva (ďalej len „ESLP") do tejto skupiny pridáva aj ochranu súkromia v súvislosti s publikáciou intímnych záležitostí osoby bez jej súhlasu v médiách[17] a ochranu práva rozhodovať o svojom vlastnom tele v prípadoch, kedy nebol dosiahnutý prah článku 3 Dohovoru.[18] Medzi ďalšie komponenty patriace do tejto kategórie náuka a judikatúra zaraďujú právo na ochranu identity, právo na rešpektovanie intímneho vzťahu medzi jednotlivcami, právo na ochranu cti a reputácie osoby[19] a mnoho ďalších.

Rešpektovaním komunikácie sa všeobecne rozumie ochrana listového tajomstva a ochrana pred zasahovaním do korešpondencie. Najrozšírenejšia judikatúra je k prípadom zásahu do korešpondencie medzi obžalovaným a jeho právnikom v rámci trestného procesu.[20] V súvislosti s tým je nutné zdôrazniť, že sa nejedná len o ochranu hmotných

[13] Evropská úmluva o lidských právech: komentář. Praha: C.H. Beck, 2012, s. 865.
[14] Kälin, W., & Künzli, J. *The law of international human rights protection*. Oxford: Oxford University Press., 2009, s. 383-389
[15] Všeobecná deklarácia ľudských práv, 10 december 1948, 217 A (III).
[16] Nowak, Manfred. U. N. Covenant on Civil and Political Rights: CCPR Commentary., op. cit., s. 377.
[17] ESLP: Von Hannover v. Nemecko, (App. no. 59320/00), ECHR 2004-VI.
[18] Ochrana pred neľudským alebo ponižujúcim zachádzaním, viď napr. ESLP: Raninen v. Fínsko, (App. no. 20972/92), Reports of Judgments and Decisions 1997-VIII, para 63.
[19] Kälin, W., & Künzli, J. *The law of international human rights protection*, op. cit., s. 385-389.
[20] *Ibid*. s. 389; Napríklad v prípadoch, kedy majú zamestnanci väzenia dostatočný dôvod sa domnievať, že zásielka určená z/do väzenia obsahuje zakázané predmety, majú právo ju otvoriť, no nie čítať obsah. Obsah môžu čítať len vo výnimočných prípadoch, kedy existujú dôvodné obavy, že je tento spôsob komunikácie zneužívaný pre kriminálne aktivity (viď ESLP: Campbell v. UK (App. no. 13590/88), Series A no. 233, para. 47).

listových zásielok, ale aj o elektronickú korešpondenciu. Posledná kategória, rešpektovanie domova, zahŕňa ochranu pred nezákonnými raziami, vysťahovaním a podobne.

Medzi jednotlivými kategóriami neexistuje hierarchia v rámci stupňa ochrany. Nedá sa teda povedať, že by súkromný život požíval väčšej ochrany ako domov.[21] Orgány k tomu určené by mali vždy postupovať prípad od prípadu, aby zabezpečili náležitú ochranu tohto práva.

Právo na ochranu súkromia upravujú všetky najvýznamnejšie medzinárodnoprávne dokumenty ako je Deklarácia, Pakt, ale aj regionálne inštrumenty na ochranu ľudských práv ako je Dohovor, Charta základných práv Európskej Únie[22] či Americký dohovor o ľudských právach[23]. Najvýznamnejšími aktérmi na poli ochrany súkromia je potom práve ESLP rozhodujúci o dodržiavaní Dohovoru a Výbor pre ľudské práva (ďalej len „Výbor“) majúci na starosti výklad Paktu.

1.2 Všeobecná deklarácia ľudských práv

Všeobecná deklarácia ľudských práv, schválená Valným zhromaždením OSN 10. 12. 1948, upravuje právo na súkromie v článku 12, ktorý hovorí:

> *„Nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, do rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takýmto zásahom alebo útokom.“*

Výkon práv vyjadrených v Deklarácii je možné obmedziť len takými zákonmi, ktoré majú „*zaistiť uznanie a zachovanie práv a slobôd ostatných a vyhovieť spravodlivým požiadavkám morálky, verejného poriadku a obecného blaha v demokratickej spoločnosti*“[24]. Aj keď má Deklarácia len odporúčaciu povahu, je dôležité ju tu tiež spomenúť, nakoľko sa jedná o významný dokument, na ktorého základe štáty vypracovali vlastnú úpravu ochrany ľudských práv a na ktorého základe boli taktiež založené najvýznamnejšie medzinárodné zmluvy o ochrane ľudských práv.

---

[21] Evropská úmluva o lidských právech: komentář, 2012, op.cit., s. 865.
[22] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02
[23] Americký dohovor o ľudských právach, 22. november 1969, OAS Treaty Series No. 36, (účinnosť 18. júl 1978)
[24] Potočný, Miroslav a Jan Ondřej. Mezinárodní právo veřejné: zvláštní část. 6., doplněné a rozšířené vydání. Praha: C.H. Beck, 2011, s. 100.

1.3 Medzinárodný pakt o občianskych a politických právach

Medzinárodný pakt o občianskych a politických právach, schválený 16. 12. 1966, je jedným z najdôležitejších medzinárodných dokumentov na ochranu ľudských práv. Právo na ochranu súkromia upravuje v článku 17 nasledovne:

> *„1. Nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, do rodiny, domova alebo korešpondencie ani útokom na svoju česť a povesť.*
>
> *2. Každý má právo na zákonnú ochranu proti takým zásahom alebo útokom.“*

1.3.1 Rozbor článku 17 ods. 1 Paktu

Pakt chráni voči svojvoľnému zasahovaniu niekoľko hodnôt. V prvom rade ide o súkromie ako také. Na tomto mieste je nutné zdôrazniť nepresnosť v slovenskom preklade z anglického oficiálneho znenia. Oficiálna verzia Paktu nehovorí o ochrane „súkromného života“ (*private life*), ako je to preložené, ale o ochrane „súkromia“ (*privacy*). Aj keď sa na prvý pohľad môže zdať, že ide o synonymá, súkromný život je, aj podľa autorov Dohovoru, širší pojem.[25]

Všeobecný komentár (g*eneral comment)* (ďalej len „GC“) č. 16 k článku 17 Paktu definuje niektoré pojmy z tohto článku, no zďaleka nie je tak vyčerpávajúci, ako by mohol a mal byť. Výbor, orgán povolaný k výkladu Paktu prostredníctvom GC, sa v ňom ani nepokúša pojem súkromie definovať. Zo zvyšku výkladu je však zrejmé, že sa vo všeobecnosti kloní skôr k extenzívnemu výkladu tohto článku. Napríklad pri pojme „rodina“, Výbor zdôrazňuje nutnosť širokej interpretácie tak, aby zahrňovala celú potenciálnu rodinu v danej spoločnosti.[26] Výbor tak reaguje na univerzálnosť Paktu a na to, že v rôznych kultúrach môže byť pojem rodina vnímaný rôznymi spôsobmi.[27]

Celkovo je ale GC č. 16 pomerne zastaralý, zvlášť s prihliadnutím k tomu, aká je vo všeobecnosti jeho úloha. Výbor by v GC mal interpretovať články Paktu tak, aby reagoval na prípadné interpretačné problémy a upevňoval tak právnu istotu. Od roku 1988,

[25] Evropská úmluva o lidských právech: komentář, 2012, op.cit., s. 867.
[26] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 4.
[27] Aj vo svojej rozhodovacej činnosti Výbor aplikuje pomerne extenzívnu metódu výkladu. Tak napríklad v už spomínanom ESLP: *Coeriel et al v. Holandsko* Výbor uznal, že sa článok 17 vzťahuje aj na právo jednotlivca na vyjadrenie svojej identity (*Coeriel et al. v. Holandsko*, para. 10.2).

kedy bol tento GC vydaný, sa svet premenil spôsobom, ktorý má obrovský vplyv na súkromie (rozvoj informačných technológií) a preto je veľkým nedostatkom, že zatiaľ nevznikol nový GC, ktorý by na to adekvátne reagoval a čelil tak výzvam modernej doby.

1.3.2 Procesný systém fungovania ochrany podľa Paktu

Pakt, na rozdiel od Deklarácie, už má relatívne záväznú povahu a je preň vypracovaný systém opatrení a postupov v prípadoch, kedy by bol porušovaný. Bol zriadený už vyššie spomínaný Výbor, pozostávajúci z 18 volených členov, ktorí majú byť „*osobami vysokého morálneho charakteru a uznávaných schopností v oblasti ľudských práv*“[28].

Úlohou Výboru je preštudovať správy podávané pravidelne zmluvnými stranami Paktu o opatreniach prijatých na uvedenie práv uznaných v Pakte do života a ďalej informovať o pokroku, ktorý zmluvná strana dosiahla pri ich ochrane. Výbor taktiež vypracováva vlastnú správu a pripomienky, ktoré zasiela zmluvnej strane.[29] Ak zmluvná strana v súlade s článkom 41 Paktu vyhlási, že uznáva príslušnosť Výboru prijať a posúdiť oznámenie štátu o tom, že iný štát neplní svoje záväzky podľa Paktu, je Výbor oprávnený preskúmať sťažnosti inej zmluvnej strany. Toto je veľký posun od Deklarácie, ktorá takýto mechanizmus nemá. Navyše bol spolu s Paktom schválený aj Prvý opčný protokol, ktorý umožňuje podávať individuálne sťažnosti jednotlivcom proti štátu (samozrejme len v prípade, že daný štát prijal tento protokol).

Jednotlivci, ktorí sa sťažujú, že niektoré z ich práv uvedených v Pakte bolo porušené, v prípade, že vyčerpali všetky dostupné vnútroštátne prostriedky na nápravu, môžu predložiť Výboru na posúdenie písomné oznámenie.[30] Výbor sťažnosť preskúma na neverejných zasadaniach, pričom si vyžiada aj stanovisko príslušného štátu. Následne Výbor oznámi svoj názor obom stranám. Už z formulácie uvedeného ako „názor“[31] je zrejmé, že sa nejedná o výslovne vynútiteľné rozhodnutie. Výbor teda nedisponuje rozhodovacou právomocou, ako je to bežné u súdov, ale má k dispozícii len nezáväzné mediačné kompetencie.[32] Napriek tomu systém vydávania názorov vykazuje niektoré dôležité prvky súdneho rozhodovania. Jedná sa napríklad o nestrannosť a nezávislosť členov

[28] Pakt, čl. 28(2).
[29] *Ibid*, čl. 40(4).
[30] Prvý opčný protokol k Paktu, čl. 2.
[31] V angličtine „*view*“ a francúzštine „*constatations*“.
[32] Čepelka, Č., Šturma, P., *Mezinárodní právo veřejné*. Praha: Beck, 2008, s. 423, marg. 112.

Výboru, posudzovanie a výklad Paktu a rozhodujúci charakter týchto názorov.[33] Štáty sa však z vyššie uvedených dôvodov chýbajúcej záväznosti nepodriaďujú požiadavkám Výboru vždy.[34]

Podľa článku 2 odseku 3 Paktu sa každý štát, ktorý je zmluvnou stranou, zaväzuje zabezpečiť ktorejkoľvek osobe, ktorej práva alebo slobody uznané Paktom boli porušené, účinnú ochranu bez ohľadu na to, či sa porušenia jej práva alebo slobody dopustili osoby v úradnej funkcii. Na tomto mieste je taktiež dôležité pripomenúť, že Výbor je orgán, ktorého úlohou je práve výklad Paktu, ku ktorému sa zmluvné strany dobrovoľne zaviazali, že ho budú dodržiavať. S tým súvisí aj povinnosť jednať v dobrej viere založená článkom 26 Viedenského dohovoru o zmluvnom práve[35] (ďalej len „VDZP"), ktorý hovorí: „*Každá platná zmluva zaväzuje zmluvné strany a musí byť nimi plnená dobromyseľne.*"

Dá sa teda vyvodiť, že pristúpením k Paktu a zvlášť aj k Opčnému protokolu zmluvné strany uznali právomoc Výboru rozhodovať o tom, či došlo k porušeniu Paktu. V prípade, že k nemu došlo, samotný Pakt ich zaväzuje k tomu, aby podnikli nevyhnutné kroky v súlade so svojimi ústavnými postupmi a ustanoveniami Paktu, aby schválili také zákonodarné alebo iné opatrenia potrebné na to, aby zabezpečili efektívnu ochranu práv uznaných v Pakte. Jedná sa o argumentáciu, ktorú Výbor sústavne používa pri vydávaní názorov.[36] Zároveň má Výbor k dispozícii akýsi „morálny postih" vo forme uverejnenia nedostatkov v dodržiavaní povinností konkrétnym štátom vo svojej výročnej správe, ktorú predkladá Valnému zhromaždeniu OSN.

1.3.3 Derogácia a limitácia článku 17.

Už zo znenia článku 17 je zrejmé, že právo na súkromie tak, ako ho chráni Pakt, nie je absolútne. Tu si dovolím upozorniť už na druhú nepresnosť v preklade tohto článku do slovenského jazyka. Zatiaľ čo slovenský preklad uvádza, že nikto nesmie byť vystavený „svojvoľnému zasahovaniu", z čoho by vyplývalo, že daný zásah len nesmie byť

[33] UN Human Rights Committee (HRC), General comment no. 33, Obligations of States parties under the Optional Protocol to the International Covenant on Civil and Political Rights, 25 June 2009, CCPR/C/GC/33, para 11.
[34] Čepelka, Č., Šturma, P., *Mezinárodní právo veřejné,* op.cit., s. 415, marg 110.
[35] Viedenský dohovor o zmluvnom práve, 1155 UNTS 331, zjednaný 22. mája 1969, v platnosti od 27. januára 1980.
[36] *General comment* no. 33, op. cit., para 14.

svojvoľný (*arbitrary*), anglická verzia pracuje navyše s pojmom nezákonný (*unlawful*). Taktiež francúzska verzia vymenúva okrem pojmu „*arbitraires*“ aj pojem „*illégales*“.

Zásah do tohto práva teda je možný, no len za súčasného splnenia určitých podmienok. Kritériá sa vyvinuli časom a to hlavne prostredníctvom súdnych rozhodnutí a jurisprudencie. Už v roku 1984 sa v Syrakúzach stretlo 31 významných expertov na medzinárodné právo a spoločne vytvorili to, čomu sa hovorí tzv. „Syrakúzske princípy“[37]. Jedná sa o súhrn princípov, ktoré je treba dodržiavať v prípadoch derogácie a limitácie práva v súlade s Paktom.

a) Derogácia

Derogácia je zakotvená v článku 4 Paktu:

> „*Ak je za mimoriadnej situácie, ktorá je úradne vyhlásená, ohrozený život národa, môžu štáty, zmluvné strany paktu, prijať opatrenia zmierňujúce ich záväzky podľa paktu v rozsahu, ktorý si vyžiadajú potreby takej situácie za podmienky, že tieto opatrenia nie sú v rozpore s ich inými záväzkami podľa medzinárodného práva a neznamenajú diskrimináciu podľa rasy, farby, pohlavia, jazyka, náboženstva alebo sociálneho pôvodu.*“

Derogáciu v súlade s Paktom sprevádzajú nutné formálne kroky, ktoré musí štát učiniť. V prvom rade musí prostredníctvom generálneho tajomníka Organizácie Spojených národov (ďalej len „OSN“) upovedomiť ostatné zmluvné strany Paktu, že deroguje, aké právo deroguje a z akého dôvodu.[38] Notifikácia by mala zahŕňať aj predpokladaný dopad na ostatné práva uznané Paktom. Derogácia od určitých taxatívne vymenovaných práv je vylúčená. Samotná fráza „ohrozený život národa“ je vysvetlená v už spomínaných Syrakúzskych princípoch. Jedná sa o hrozbu, ktorá:

1. Ovplyvňuje celú populáciu národa a zároveň buď celé územie štátu, alebo jeho časť.
2. Ohrozuje fyzickú integritu obyvateľstva, politickú nezávislosť alebo územnú celistvosť štátu, alebo existenciu, alebo základné fungovanie inštitúcií nevyhnutných na zabezpečenie a ochranu práv uznaných v Pakte.[39]

[37] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4.
[38] Pakt, čl. 4(3).
[39] Syrakúzske princípy, op.cit., para. 39.

Derogácia by mala trvať len skutočne nevyhnutný čas a musí byť proporcionálna.[40] Proporcionalitu a pristúpenie k derogácii ako k poslednej možnosti zdôrazňuje aj GC č. 29 k článku 4 Paktu.[41]

b) Limitácia

V prípade, že chce štát len limitovať výkon určitého práva, je nutné, aby vždy zároveň rešpektoval podstatu tohto práva a konal tak v súlade s príslušnými ustanoveniami Paktu. Keď sa vrátim k samotnému zneniu Paktu, je zrejmé, aj napriek zlému prekladu, že podmienky prípadného zásahu do práva na súkromie sú dve:

1. Zásah nesmie byť svojvoľný.
2. Zásah nesmie byť nezákonný.

Tieto dve podmienky sú navzájom previazané a dopĺňajú sa. Aby nebol zásah považovaný za svojvoľný, je potrebné aby bol dostatočne odôvodnený a proporcionálny. Odôvodnenosťou je myslený tzv. legitímny cieľ, ktorý chce štát dosiahnuť zásahom do tohto práva. Najčastejšie sa zo strany štátov jedná o argument národnou bezpečnosťou, verejným poriadkom, prebiehajúcim vyšetrovaním a podobne. Proporcionalita potom znamená to, že rozsah zásahu je primeraný chránenému záujmu. Musí sa jednať o čo „*najmenší zásah, ktorý je ešte dostatočný na to, aby dosiahol požadovaný cieľ*".[42] Možné prípady, kedy je prípustný takýto zásah, musí predvídať zákon a zároveň musia byť v súlade s medzinárodným právom.

V otázke zákonnosti je potrebné dbať na to, aby sa prípadný zásah do súkromia dial v rámci platnej legislatívy a teda len z dôvodov, ktoré daný zákon predvída ako dostatočné na to, aby bolo legitímne zasiahnuť do práva na súkromie. Musí sa jednať o jasne definované podmienky a proces musí byť podrobený efektívnemu súdnemu dohľadu a kontrole. Taktiež je nutné, aby zákon, ktorý takýto zásah predvída, bol v súlade s ustanoveniami a cieľmi Paktu.[43] Je teda dôležité posudzovať nie len to, či bol daný zásah v súlade s ustanoveniami zákona, ale aj či samotný zákon je v súlade s princípmi, na ktorých je založený Pakt.

[40] Syrakúzske princípy, op.cit., para. 51.
[41] UN Human Rights Committee (HRC), CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency, 31 August 2001, para 6.
[42] UN Human Rights Committee (HRC), CCPR General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, para. 14.
[43] *General comment* no. 16, op. cit., para. 3.

Výbor navyše vo svojej praxi pracuje s termínom „rozumnosti“ (*reasonableness*), ktorý znamená, že zvolený postup musí byť „rozumný v daných okolnostiach“. Aj keď je zásah v súlade so zákonom, štát musí mať jasné odôvodnenie prečo postupoval práve určitým spôsobom.[44] Tento princíp dobre demonštruje prípad *Rojas Garcia*[45]. V tomto prípade bolo uznané, že štát Kolumbia nebol schopný dostatočne odôvodniť nutnosť vykonať násilný vstup do domu podozrivého cez strechu o druhej ráno, za použitia ozbrojených policajných jednotiek (*Cuerpo Técnico de Investigación de la Fiscalía*), pričom títo ozbrojenci vystrelili niekoľko varovných výstrelov a verbálne urážali a hrozili zbraňami ako samotnému sťažovateľovi, tak aj jeho rodine. V byte boli prítomné aj jeho malé deti, ktoré utrpeli traumu. Kolumbia sa následne snažila brániť argumentáciou, že zásah bol v súlade s kolumbijským trestným poriadkom a teda nedošlo k porušeniu zákona. Výbor však uznal, že štát Kolumbia nebol schopný dostatočne preukázať, že bol daný zásah skutočne v daných okolnostiach potrebný v takejto podobe.

Martin Scheinin, Zvláštny spravodajca pre ľudské práva v rámci boja proti terorizmu, vo svojej správe[46] z roku 2009 reaguje na činnosť Výboru a popisuje tzv. test prípustnosti obmedzení (*permissible limitation test*), ktorý by mal štát splniť v prípade, že chce zasiahnuť do práva na súkromie. Test vyzerá nasledovne:

1. Možné obmedzenia musia byť stanovené zákonom.
2. Samotná podstata daného práva nesmie byť predmetom obmedzení.
3. Obmedzenia musia byť nevyhnutné v demokratickej spoločnosti.
4. Akákoľvek diskrečná právomoc, ktorá umožňuje implementáciu daného obmedzenia, nesmie byť neobmedzená.
5. Aby bolo obmedzenie prípustné, nestačí ak slúži vymedzenému legitímnemu cieľu. Musí byť pre daný cieľ nevyhnutné.
6. Obmedzenia musia byť v súlade s princípom proporcionality. Musia byť vhodné na dosiahnutie ich ochrannej funkcie a musí sa jednať o najmenej rušivý prostriedok k dosiahnutiu žiadaného výsledku. Zároveň musia byť primerané k záujmu, ktorý majú chrániť.

[44] General comment no. 16, op. cit., para. 4.
[45] HRC: Rafael Armando Rojas García v. Kolumbia, Communication No. 687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).
[46] The right to privacy. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/13/37, December 2009).

7. Všetky obmedzenia musia byť v súlade s ostatnými právami, ktoré Pakt zaručuje.[47]

1.4 Európsky dohovor o ochrane ľudských práv a základných slobôd

Európsky súd pre ľudské práva, rozhodujúci podľa Európskeho dohovoru o ochrane ľudských práv a základných slobôd a príslušných protokolov, je spolu s Výborom najprogresívnejší vo výklade práva na ochranu súkromia. Na rozdiel od Výboru sa však jedná o regionálny orgán, nakoľko Dohovor je medzinárodná zmluva v rámci Rady Európy. Dohovor vstúpil v platnosť 3. 9. 1953 a upravuje právo na ochranu súkromia v článku 8 odseku 1 nasledovne:

> „*Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.*“

1.4.1 Rozbor článku 8 ods. 1 Dohovoru

Ako bolo spomenuté vyššie, Dohovor chráni, na rozdiel od Paktu, tzv. „súkromný život“, čo je vnímané ako širšia kategória oproti „súkromiu“. Vyčerpávajúca definícia súkromného života neexistuje, vďaka čomu ho ESLP môže prispôsobovať konkrétnym okolnostiam prípadu, čím sa prejavuje vnímanie Dohovoru ako tzv. „živého inštrumentu“.[48] ESLP sa tak už niekoľko krát vo svojej rozhodovacej praxi vyjadril, že súkromný život je „*široký pojem, nepoddajný vyčerpávajúcej definícii*“[49]. Je dôležité zdôrazniť, že ESLP nevníma právo na súkromný život len ako oblasť súkromných záležitostí jednotlivca, no posudzuje aj spoločenský aspekt tohto práva a vykladá ho aj ako právo rozvíjať vzťahy s inými osobami vonkajšieho sveta v rámci rozvíjania vlastnej osobnosti.[50]

Čo sa týka pojmu „rodinný život“, ESLP opäť postupuje vo výklade prípad od prípadu a nemá ustálenú definíciu. Pojem „domov“ je tak vykladaný ako miesto, kde sa rozvíja súkromný a rodinný život.[51] Opäť sa ale nejedná o striktnú definíciu, nakoľko

[47] The right to privacy, Martin Scheinin, op. cit., para 17.
[48] Pre príklady toho čo všetko ESLP zaraďuje pod pojem súkromný život viď Evropská úmluva o lidských právech: komentář, 2012, op.cit., s. 870 marg. 14.
[49] ESLP: S. a Marper v. UK, (App. no. 30562/04 and 30566/04), para. 66 alebo ESLP: Costello-Roberts v. UK (App. no. 13134/87), para. 36.
[50] ESLP: Niemitz v. Nemecko (App no. 13710/88), para. 29.
[51] Evropská úmluva o lidských právech: komentář, 2012, op. cit., s. 874 marg. 22.

ESLP tento pojem niekoľkokrát vo svojej praxi rozšíril.[52] Ochranu korešpondencie ESLP vníma ako ochranu práva na výmenu informácii medzi ľuďmi a ochranu dôvernosti tejto informácie.[53] V tomto kontexte je ESLP veľmi progresívny a uznáva ochranu všetkých foriem korešpondencie, vrátane elektronickej.

Zo znenia článku 8 ako „práva na rešpektovanie" by sa mohlo zdať, že Dohovor tak v podstate ukladá zmluvným stranám len negatívne záväzky. Metóda efektívnej interpretácie Dohovoru však znamená, že ochrana práv musí byť v praxi aj účinná a tak umožňuje ESLP požadovať v konkrétnych prípadoch od zmluvných strán aj aktívne chovanie a teda aj pozitívne záväzky.[54] Tento princíp ESLP vyjadril napríklad v prípade *X a Y v Holandsko*[55]:

> *„Súd pripomína, že hoci cieľom článku 8 je v zásade ochrana jednotlivca pred svojvoľným zásahom zo strany štátnych orgánov, to neznamená len povinnosť štátu zdržať sa takéhoto zásahu: navyše k tomuto primárne negatívnemu záväzku, môžu existovať pozitívne povinnosti vyplývajúce z účinného rešpektovania súkromného alebo rodinného života. Tieto povinnosti môžu zahŕňať prijatie opatrení zameraných na zabezpečenie rešpektovania súkromného života aj v oblasti vzťahov medzi jednotlivcami."*[56]

1.4.2 Procesný postup pred ESLP

Dohovor má pre zmluvné strany záväznú povahu. Regionálna úprava má pochopiteľne oproti univerzálnemu Paktu aj lepšie výsledky, čo sa týka efektívnej ochrany. Tento jav je všeobecne možné pozorovať pri regionálnych úpravách a to hlavne tam, kde účastnícke štáty vyznávajú zhodné spoločensko-ekonomické a civilizačné hodnoty.[57]

Implementačným orgánom Dohovoru je už spomínaný ESLP so sídlom v Štrasburgu. Ten už má, na rozdiel od Výboru, aj skutočne rozhodovaciu právomoc. Článok 33 Dohovoru dáva ESLP právomoc rozhodovať spory medzi zmluvnými stranami. ESLP je však ďaleko známejší z posudzovania individuálnych žiadostí, kedy sa naň obracajú jed-

[52] Napríklad v ESLP: Niemitz v. Nemecko ESLP uznal za „domov" aj kancelárie slúžiace ako miesto výkonu práce.
[53] Evropská úmluva o lidských právech: komentář, 2012, op. cit., s. 877 marg. 27.
[54] *Ibid*, s. 884 marg. 36.
[55] ESLP: X a Y v. Holandsko (App. no. 8978/80).
[56] *Ibid*, para. 23.
[57] Čepelka, Č., Šturma, P., *Mezinárodní právo veřejné,* op.cit., s. 421 marg. 112.

notlivci, fyzické aj právnické osoby, so svojimi podaniami, za predpokladu, že tiež spĺňajú kritéria prípustnosti.[58] Ak ESLP uzná prípustnosť podania, pokračuje v prerokovávaní prípadu. ESLP najprv zisťuje, či záležitosti ktoré sťažovateľ vylíčil, spadajú pod ochranu článku 8. Ak áno, musí si zodpovedať otázku, či došlo k zásahu do niektorého z týchto záujmov zo strany orgánu verejnej moci. Ak nie, tak sa jedná o pozitívne záväzky, ako boli popísané vyššie. Ak bol zásah skutočne uskutočnený zo strany štátu, postupuje sa ďalej podľa článku 8 odseku 2 a ESLP posudzuje legalitu, legitimitu a proporcionalitu zásahu.[59]

Jednanie končí rozsudkom, prípadne zmierom. Konečný rozsudok je záväzný pre zmluvné strany v danom spore, ktoré sa ním musia riadiť.[60] Na rozdiel od Paktu sa teda v prípade Dohovoru jedná o skutočne vynútiteľný mechanizmus ochrany ľudských práv.

1.4.3 Zásahy do práva na ochranu súkromia podľa článku 8

Ani Dohovor však nevníma právo na ochranu súkromia ako právo absolútne a tak hneď v druhom odseku článku 8 upravuje limitáciu tohto práva:

> „*Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.*“

Samotná existencia zásahu tak ešte nemusí nutne znamenať porušenie Dohovoru. Sťažovateľ musí v prvom rade Súdu dokázať, že je obeťou tohto zásahu. Toto sa najmä v prípadoch elektronického sledovania dokazuje pomerne ťažko, nakoľko je sledovanie vykonávané v utajení a cieľ nemá o sledovaní zo strany štátu priame dôkazy. Dohovor neuznáva tzv. *actio popularis* a teda by v takýchto prípadoch malo obecne dôjsť k rozhodnutiu o neprípustnosti sťažnosti vzhľadom na nedostatok v jurisdikcii *ratione personae*. To by však za určitých okolností mohlo viesť k odopretiu spravodlivosti. Problém v nedostatku dôkazných prostriedkov a teda nedostatočným preukázaním, že k zásahu skutočne došlo, rieši ESLP tak, že v určitých situáciách stačí, ak sťažovateľ dokáže, že k zásahu dôjsť mohlo (napríklad existuje platná legislatíva, ktorá taký zásah povoľuje)

[58] Procedurálne kritéria viď čl 35 Dohovoru.
[59] Korff D., *The standard approach under Articles 8-11 ECHR and Article 2 ECHR*.
[60] Dohovor, čl. 46(1).

a je vysoko pravdepodobné, že aj došlo. Takto napríklad v prípade *Campbell*[61], kde sťažovateľ namietal, že bolo narušené jeho právo na ochranu korešpondencie, keď mu údajne boli príslušníkmi väzenskej stráže otvárané súkromné listy, ESLP uznal (aj napriek tomu, že sťažovateľ nebol schopný doložiť jediný otvorený list alebo iný dôkaz), že už len existencia systému v danom nápravnom zariadení, ktorý umožňuje takéto svojvoľné otváranie a čítanie korešpondencie, postačuje na porušenie článku 8.[62]

V prípade, že ESLP dôjde k názoru, že do práva na ochranu súkromia bolo zasiahnuté zo strany štátu, musí ďalej skúmať či bol daný zásah v súlade s článkom 8 odsekom 2. Štát neporušil svoju povinnosť podľa Dohovoru vtedy, ak zásah kumulatívne spĺňa tieto kritéria:

1. Bol v súlade so zákonom (kritérium legality).
2. Sledoval legitímny cieľ (kritérium legitimity).
3. Bol nevyhnutný v demokratickej spoločnosti (kritérium proporcionality).

a) Kritérium legality.

Toto kritérium, podobne ako predpoklad zákonnosti u Paktu, predpokladá, že pre zásah musí existovať opora v zákone. Ak by takáto opora neexistovala v čase zásahu, jednalo by sa automaticky o nelegálny zásah, porušujúci článok 8 Dohovoru. Nesmie však ísť o akýkoľvek zákon, no o zákon dostatočnej kvality a v súlade s právnymi princípmi Dohovoru ako sú formulované v preambule.[63] Zákon teda musí obsahovať dostatočné záruky pred jeho zneužitím, ako sú napríklad účinný dozor a kontrola.[64]

Dôležitou zložkou zákona je aj jeho predvídateľnosť (*foreseeability*). Tá je nevyhnutnou zložkou kritéria legálnosti a znamená, že daný zákon je verejne dostupný a zároveň konštruovaný dostatočne precízne na to, aby umožnil osobám predvídať, do určitého stupňa primeraného okolnostiam, prípadné následky ich konania.[65] Samozrejme to ale neznamená, že štát musí v prípadoch, kedy chce napríklad používať operatívno-pátracie prostriedky v rámci trestného konania informovať potencionálnych páchateľov o svojom postupe. V prípade *Malone* sa tomuto ESLP venoval detailne a dospel k záveru, že:

[61] ESLP: Campbell v. UK, (App. no. 13590/88), Series A no. 233
[62] *Ibid*, para 33.
[63] ESLP: Malone v. UK, (App no 8691/79), para 67; viď tiež Silver and Others judgment, (App. no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), para 34.
[64] ESLP: Gillan and Quinton v. UK, (App. no. 4158/05), para 87.
[65] ESLP: Dubská a Krejzová v. Česká republika (App. no 28859/11 and 28473/12), para 167.

„*Požiadavky Dohovoru, najmä pokiaľ ide o predvídateľnosť, nemôžu byť úplne rovnaké v osobitnom kontexte odpočúvania komunikácií pre účely policajného vyšetrovania, keďže predmetom príslušného zákona je práve obmedzenie práv jednotlivca. Predovšetkým, požiadavka predvídateľnosti nemôže znamenať, že jednotlivec by mal mať možnosť predvídať, kedy orgány pravdepodobne zachytia jeho komunikáciu, aby mohol zodpovedajúcim spôsobom prispôsobiť svoje správanie. Napriek tomu ale musí byť zákon dostatočne jasný, aby poskytol občanom primeranú informáciu o okolnostiach a podmienkach, za ktorých sú verejné orgány oprávnené uchýliť sa k tomuto tajnému a potenciálne nebezpečnému zasahovaniu do ich práva na rešpektovanie súkromného života a korešpondencie*.“[66]

Ďalší argument, prečo sa musí jednať o zákon a nie iný akt verejnej moci, je ten, že zákon je pomerne náročné často meniť, nie je tak flexibilný. Spôsob zmeny zákona sa pochopiteľne viac či menej v jednotlivých štátoch líši, no vo všeobecnosti zákon nie je možné prispôsobovať situácií tak jednoducho, ako napríklad interné pokyny. Tento argument ESLP potvrdil vo svojom rozhodnutí *Khan*, kedy britské úrady používali k odpočúvaniu zariadenie, ktorého používanie bolo upravené výlučne v pokynoch ministerstva, pričom pokyny neboli ani verejne dostupné, ani právne záväzné. Na základe toho ESLP dospel k názoru, že sa nejedná o zásah v súlade so zákonom.[67]

b) Kritérium legitimity

Kritérium legitimity znamená, že zásah musí sledovať tzv. „legitímny cieľ“ (*legitimate aim*). Tie sú taxatívne vymenované v článku 8 odseku 2 a jedná sa o:

1. národnú bezpečnosť – štáty argumentujú v prípadoch masívneho sledovania najčastejšie práve týmto;
2. verejnú bezpečnosť;
3. hospodársky blahobyt krajiny;
4. predchádzanie nepokojom alebo zločinnosti – s týmto cieľom sa dá stretnúť napríklad v prípadoch cieleného odpočúvania v rámci vyšetrovania trestnej činnosti;
5. ochrana zdravia alebo morálky – napríklad odobranie dieťaťa z opatery rodičov;
6. ochrana práv a slobôd iných.

[66] ESLP: Malone v UK, op. cit., para 67.
[67] ESLP: Khan v UK, (App No 35394/97), para 28.

Nakoľko sa jedná o pomerne široké pojmy, prípustné akejkoľvek interpretácií, ESLP sa konkrétnym cieľom nezaoberá často a len skutočne výnimočne neuzná žiaden legitímny cieľ v konaní štátu.[68]

c) Kritérium proporcionality

Fakt, že ESLP často uzná argumentáciu štátu ohľadom legitímneho cieľa ale automaticky neznamená, že je spôsob akým štát zásah vykonal aj proporcionálny. V jazyku Dohovoru ide o kritérium tzv. „nevyhnutnosti v demokratickej spoločnosti". Pre účely vysvetlenia týchto pojmov dobre slúži judikatúra. V prípade *Dudgeon*[69], sa ESLP vyjadril o požiadavke nevyhnutnosti ako o existencii „*naliehavej spoločenskej potreby*" pre daný zásah. Zároveň ESLP uznal, že prvotné posúdenie je na samotnom štáte a jeho orgánoch, ktoré v tom požívajú tzv. „priestor pre uváženie" (*margin of appreciation*). ESLP ďalej argumentuje, že nielen povaha sledovaného cieľa bude určovať veľkosť tohto priestoru pre uváženie. Dôležitú rolu musí hrať aj povaha zasiahnutých aktivít.

Čo sa týka pojmu „demokratická spoločnosť", ESLP ho presne nedefinuje, no zmieňuje dva charakteristické znaky a to toleranciu a otvorenosť.[70] Testom proporcionality ESLP vlastne porovnáva a zvažuje medzi záujmom jednotlivca a záujmom celku. Konkrétne sa zaoberá samotným chráneným záujmom, povahou zásahu doň a spoločenskou potrebou pre taký zásah. Pomerne výstižne to ESLP vyjadril v prípade *Soering*: „*Neodmysliteľnou súčasťou Dohovoru je hľadanie primeranej rovnováhy medzi požiadavkami obecného záujmu spoločnosti a požiadavkami na ochranu základných práv jednotlivca.*"[71] Čím väčší zásah do práva jednotlivca, tým vážnejší dôvod musí štát mať, aby obstál v teste proporcionality.

[68] Evropská úmluva o lidských právech: komentář, 2012, op. cit., s. 882.
[69] ESLP: Dudgeon v. UK, (App. No. 7525/76).
[70] *Ibid*, para 51-52.
[71] ESLP: Soering v UK, para 89

2. Sledovanie v kyberpriestore a aplikovateľnosť medzinárodných zmlúv

Táto kapitola sa venuje právu na ochranu súkromia v súvislosti s masívnym sledovaním a zberom dát zo strany štátu. Najprv popisuje, čo sa rozumie pod pojmami ako kyberpriestor a sledovanie, aký je ich účel a ako sa k tomuto fenoménu stavia medzinárodné právo. Potom vysvetľuje, ako tajné sledovanie ohrozuje právo na súkromie a ako sa dá zneužiť. Následne sa zameriava na posúdenie aplikovateľnosti medzinárodných dokumentov, konkrétne Paktu a Dohovoru.

2.1 Čo je to kyberpriestor?

Len ťažko si dnes dokážeme predstaviť život bez informačných technológií. Stali sa bežnou súčasťou nášho života a značne nám život zjednodušujú. Dôsledkom toho je, že stále viac ľudí a inštitúcií je doslova závislých na digitálnych technológiách.

Čo to ale kyberpriestor vôbec je? Medzinárodná telekomunikačná únia, odborná organizácia pridružená k OSN, definuje kyberpriestor ako prostredie, kde *„patria používatelia, siete, zariadenia, softvér, procesy, uložené aj prenášané informácie, aplikácie, služby a systémy, ktoré možno prepojiť priamo alebo nepriamo do sietí"*[72]. Dôležitosť kyberpriestoru pre medzinárodné právo dokazuje aj metodika Ministerstva obrany USA, ktorá kyberpriestor zaraďuje medzi potencionálne bojové priestory ako je zem, voda, vzduch a vesmír.[73] Napriek tomu však celosvetovo ustálená a uznaná definícia kyberpriestoru neexistuje a skoro každý štát má svoju vlastnú definíciu.

Vzťahuje sa vôbec dnešné medzinárodné právo na kyberpriestor? Vo všeobecnosti je prijímaný názor, že áno.[74] Niektorí však argumentujú, že kyberpriestor vôbec nepatrí do sféry práva (že je to tzv. „*non-legal domain"*), nakoľko nie je možné určiť jeho hranice, nie je súčasťou fyzického sveta a má všadeprítomný charakter.[75] Ďalší argument

[72] International Telecommunication Union: Series X: Data networks, open system communications and security: overview of cybersecurity, 2008, s. 2.
[73] U.S. Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12(R) (Washington, DC: U.S. Joint Chiefs of Staff, 5 February 2013), s. 15.
[74] Tsagourias, Nicholas, and Buchan, Russell, *Research Handbook on International Law and Cyberspace*. Edward Elgar M.U.A., 2015, s. 13.
[75] Viď napr. Johnson, R. David, and Post, G. David, *Law and borders: The rise of law in cyberspace*, 48 Stanford L Rev 1367, 1996. Contra Goldsmith, L. Jack, '*Against cyberanarchy*', 65 U Chi L Rev 1199, 1998.

prečo nie je správne aby bol kyberpriestor akokoľvek právne regulovaný, je práve myšlienka slobody a otvorenosti kyberpriestoru ako niečoho, čo nie je obmedzované právom a tak môže oveľa slobodnejšie pozitívne pôsobiť v spoločnosti. Je pravda, že kyberpriestor má obrovský potenciál pozitívne ovplyvniť spoločenské, ekonomické aj sociálne vzťahy vo svete. Zároveň je ale nutné si uvedomiť, že kyberpriestor predstavuje pri potencionálnom zneužití obrovskú hrozbu. Všetky výhody, ktoré tieto technológie prinášajú, zdá sa mnohým ľuďom zabraňujú uvedomiť si nástrahy a nebezpečenstvá, ktoré s nimi súvisia. Prípadov zneužitia kyberpriestoru, či už štátnymi, alebo neštátnymi aktérmi v poslednom čase pribúda.[76]

Komu ale kyberpriestor patrí? Poskytovateľom internetových služieb? Štátom? Ak štátom, vzťahuje sa naň aj princíp suverenity? Zodpovedanie tejto otázky je nesmierne dôležité pre právnu istotu a preto, aby bolo možné v kyberpriestore efektívne vynucovať pravidlá medzinárodného práva. Stabilný a bezpečný kyberpriestor je pre budúcnosť našej spoločnosti kľúčový.

Skupina vládnych expertov na vývoj v oblasti informácií a telekomunikácií v kontexte medzinárodnej bezpečnosti, vo svojej správe uvádza, že „*štátna zvrchovanosť a medzinárodné normy a princípy, ktoré vyplývajú zo suverenity, sa vzťahujú na jednanie štátov ohľadom činností súvisiacich s informačno-komunikačnými technológiami a na ich jurisdikciu nad touto infraštruktúrou na ich území*“[77].

Princíp suverenity je nutné odlíšiť od princípu teritoriality. Je síce pravda, že suverenitou sa chápe „*celý súbor práv, ktorý má štát na svojom území*“[78], no to len znamená, že teritorialita a suverenita sú úzko prepojené pojmy a nie že suverenita nutne predpokladá teritorialitu. Územie len ponúka hmotný priestor, kde sa môže suverenita prejavovať z politického a právneho hľadiska.[79]

Spomínaná skupina expertov ďalej vo svojej správe identifikovala tieto princípy ako kľúčové pri aplikácií medzinárodného práva na informačno-komunikačné technológie:

a) zvrchovaná rovnosť;

[76] UN GA, A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, para. 3.
[77] *Ibid*, para. 27.
[78] Corfu Chanel Case (UK v Albania) (Separate Opinion of Judge Alvarez) [1949] ICJ Rep 43.
[79] Tsagourias, Nicholas, and Buchan, Russell, *Research Handbook on International Law and Cyberspace*. Edward Elgar M.U.A., 2015, s.18.

b) *riešenie medzinárodných sporov mierovými prostriedkami tak, že nie je ohrozený medzinárodný mier, bezpečnosť a spravodlivosť;*
c) *vyhýbanie sa hrozbe silou alebo použitiu sily proti územnej celistvosti alebo politickej nezávislosti ktoréhokoľvek štátu alebo akýmkoľvek iným jednaním, ktoré nie sú v súlade s cieľmi Organizácie Spojených národov;*
d) *dodržiavanie ľudských práv a základných slobôd;*
e) *nezasahovanie do vnútorných záležitostí iných štátov*.[80]

Rezolúcia Valného zhromaždenia OSN taktiež potvrdzuje, že rovnaké práva, ktoré majú ľudia *offline*, musia byť tiež chránené *online*, vrátane práva na súkromie.[81]

2.2 Čo je to sledovanie?

Na tomto mieste je dôležité vysvetliť pojem špionáž (*espionage*) a pojem sledovanie (*surveillance*).

Prvý pojem, laikom asi známejší, je špionáž. Delí sa na vojnovú a mierovú. V prípade vojnovej (*wartime espionage*), sa jedná o „*zhromažďovanie alebo pokus o zhromažďovanie informácií na území kontrolovanom nepriateľskou stranou, prostredníctvom činov konaných na základe falošných zámienok alebo úmyselne tajným spôsobom*“[82]. Vojnová špionáž je štátmi v podstate akceptovaná ako legitímna súčasť vedenia vojny. Hugo Grotius už v 17. storočí tvrdil, že vysielanie špehov je „*bezpochyby v súlade s právom národov*“[83]. Moderné humanitárne právo taktiež ráta s využívaním špiónov počas ozbrojeného konfliktu. Tento druh špionáže sa ale zásadne líši od špionáže v čase mieru (*peacetime espionage*).[84]

Mierová špionáž zahŕňa mnoho činností od tajného získavania informácií o aktivitách a zámeroch iných štátov (v závislosti na cieli, prostriedkoch a dôvode sledovania sa potom rozlišuje špionáž politická, diplomatická alebo ekonomická) až po odpočúvanie telefónov a sledovania emailovej komunikácie súkromných osôb. Sledovanie môže prebiehať buď vo fyzickom svete, alebo ako je to stále častejšie – elektronicky. Aj napriek

[80] UN GA, A/70/174, op. cit., para. 26.
[81] UN GA Resolution. 68/167, “The right to privacy in the digital age,” U.N. Doc. A/RES/68/167 (Jan. 21, 2014).
[82] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, čl. 29.
[83] Hugo Grotius, *De Jure Belli Ac Pacis Libri Tres* 655 (Francis W. Kelsey trans., 1925) (1646).
[84] Niektorí autori nerozlišujú medzi špionážou vojenskou a mierovou.

tomu, že sa stále o samotnej špionáži hovorí ako o tzv. *lacuna*, teda ako o oblasti neupravenej medzinárodným právom[85], je sledovanie nepriamo regulované prostredníctvom záväzkov štátov v oblasti ochrany ľudských práv a taktiež v povinnosti rešpektovať suverenitu a nezasahovať do vnútorných záležitostí iných štátov. Táto práca sa venuje výlučne mierovej špionáži, resp. sledovaniu (*surveillance*), konkrétne elektronickému.

2.2.1 Druhy sledovania

V prvom rade je dôležité od seba rozlíšiť tzv. vnútroštátne sledovanie (*domestic surveillance*) a sledovanie zahraničné (*foreign surveillance*). Vnútroštátne elektronické sledovanie, ako aj názov napovedá, je sledovanie výlučne vnútroštátnej komunikácie. V prípade zahraničného elektronického sledovania sa jedná o prípady, kedy štát monitoruje komunikáciu, ktorá prebieha elektronickými prostriedkami buď to úplne alebo aspoň čiastočne mimo teritórium sledujúceho štátu.[86] Podľa toho sa ešte zahraničné elektronické sledovanie delí na tzv. „extrateritoriálne sledovanie", teda sledovanie ktoré prebieha výlučne mimo územie sledujúceho štátu a sledovanie „nadnárodné" kedy daná komunikácia prebieha len čiastočne mimo sledujúci štát.[87]

Milanovič zahraničné sledovanie chápe v troch rovinách. V prvej kategórií sa jedná o štátom riadené aktivity voči predstaviteľom alebo členom iných štátov alebo medzinárodných organizácií. Ďalšia kategória zahŕňa aktivity namierené voči jednotlivcom cudzej štátnej národnosti, teda cudzincom, nezávisle na tom, kde sa nachádzajú. Posledná kategória sú osoby nachádzajúce sa mimo územie štátu, pričom nerozhoduje ich štátna príslušnosť. [88]

Druhým rozdelením je sledovanie cielené (*targeted surveillance*) a sledovanie masívne (*mass surveillance*). Cielené sledovanie sa najčastejšie používa ako operatívne-pátrací prostriedok pri vyšetrovaní trestnej činnosti. Ide napríklad o odpočúvanie telefónu konkrétnej osoby podozrivej zo spáchania trestného činu. Masívne sledovanie označuje monitorovanie všetkej dostupnej komunikácie všetkých osôb nerozlišujúc, či je konkrétny cieľ podozrivý z trestnej činnosti.

---

[85] Deeks, Ashley S. An International Legal Framework for Surveillance, *Virginia Journal of International Law* 55.2, 2015, 291-368, s. 301
[86] *Ibid*, s. 299.
[87] *Ibid*, s. 300.
[88] Milanovic, Marko. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, *Harvard International Law Journal*, vol. 56, no. 1, 2015, pp. 81–146, s. 86.

V praxi samozrejme dochádza k miešaniu jednotlivých druhov sledovania. Pojem „sledovanie“ bude pre účely tejto práce používaný pomerne široko, ako akékoľvek získavanie informácií, či už ide o odpočúvanie telefónov alebo monitorovanie internetovej komunikácie.

V súvislosti so sledovaním je ešte nutné zadefinovať pojem „metadáta“. Metadáta sú všetky údaje o komunikácií, okrem samotného obsahu. Obsah je jadro komunikácie, teda to, čo chce odosielateľ adresátovi povedať a ostatné údaje o danej komunikácií ako odosielateľ, príjemca, čas, IP adresa a podobne, sa nazývajú metadáta.[89]

2.2.2 Ako sledovanie ohrozuje právo na súkromie?

Rozvoj v technológiách má za následok, že štáty vedia stále efektívnejšie vykonávať elektronické sledovanie osôb.[90] Ľudia si pod narušením ich súkromia tradične predstavujú situácie, kedy im niekto prehľadáva byt, prezerá si ich lekárske záznamy, číta im poštu alebo inštaluje videokamery v ich domácnosti. Vo všetkých týchto prípadoch sa jednoznačne jedná o zásah do súkromnej sféry jednotlivca, ktorú sa nerozhodol dobrovoľne ukázať verejnosti. S rozvojom informačných technológií sa však okruh miest, ktoré by ľudia mohli považovať za ich súkromnú sféru, značne zvýšil. Jedna sa o celú ich súkromnú komunikáciu a dáta v kyberpriestore – či už je to emailová schránka, súkromné správy cez Skype, Facebook, alebo aj len súbory uložené v osobnom počítači. Skrátka ide o všetky informácie, ktoré sa daná osoba rozhodla buď vôbec nezverejniť, alebo zdieľať len s určitým okruhom ľudí. Tieto informácie by mali požívať rovnakej ochrany ako ich fyzickí predchodcovia. Ak sa za narušenie súkromia považuje prehľadávanie bytu alebo čítanie pošty, bude narušením súkromia aj prehľadávanie disku na počítači alebo čítanie emailovej komunikácie. Je samozrejmé, že NSA ani GCHQ nemajú kapacitu si čítať každú jednu správu a mail. Ako ale argumentoval ESLP v prípade *Weber a Saravia*, narušením súkromia môže byť už to, že majú štátne orgány kapacitu komunikáciu zachytiť.[91]

[89] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court January 23, 2014, s. 8.
[90] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, para. 33.
[91] ESLP: Weber a Saravia v. Nemecko (App no. 54934/00), ECHR 2006-XI, para. 78; Malone v. UK, op. cit., para. 64.

Sledovanie však neohrozuje len právo na súkromie. Aj iné práva, vykonávané prostredníctvom digitálnych technológií, môžu byť narušené, ak je narušené právo na súkromie. Patria sem najmä právo na slobodu názoru a prejavu, právo vyhľadávať, prijímať a šíriť informácie alebo právo na slobodu zhromažďovania a združovania.[92] Správa amerického Výboru pre súkromie a občianske slobody argumentuje:

> „*Dá sa očakávať, že masívne zhromažďovanie telefónnych záznamov bude mať mrazivý účinok na slobodné vykonávanie práva na slobodu prejavu a združovania, pretože jednotlivci a skupiny zapojené do citlivých alebo kontroverzných prác majú dôvod neveriť v dôvernosť svojich vzťahov, ako odhalili vzory ich chovania. Neschopnosť očakávať rešpektovanie súkromia vo vzťahu k vláde v telefónnej komunikácii znamená, že ľudia, ktorí síce vykonávajú úplne legálne činnosti - ale ktorí z rôznych dôvodov oprávnene nechcú, aby vláda vedela o ich komunikácii - sa musia buď zriecť takýchto aktivít, znížiť ich frekvenciu, alebo prijať nákladné opatrenia aby sa skryli pred štátnym sledovaním.*“[93]

Podľa správy PEN International[94] z novembra 2013, o vplyve sledovania NSA, sa drvivá väčšina autorov obáva vládneho dohľadu a v dôsledku toho sa dopúšťajú samocenzúry.[95] V extrémnom prípade takáto situácia môže vyústiť až do situácie tzv. „panopticonu“[96].

V extrémnych prípadoch je elektronické sledovanie, ak je v nesprávnych rukách, smrteľne nebezpečné a ohrozuje aj také základné práva ako je právo na život alebo právo

---

[92] The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37, para. 14.

[93] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Cour, op. cit., s. 12.

[94] PEN International je popredná svetová literárna a ľudskoprávna organizácia, ktorá operuje vo viac ako 100 krajinách za účelom ochrany slobodného prejavu a na obranu spisovateľov a novinárov, ktorí sú v dôsledku výkonu povolania uväznení, ohrození, prenasledovaní alebo napadnutí.

[95] PEN American Center, “*Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*”, (November 12, 2013).

[96] Panoptikon - navrhnutý anglickým filozofom Jeremy Benthamom na konci 18. storočia a popularizovaný vďaka Foucaultovi v "*Surveiller et punir: naissance de la prison*" (1975) - je architektonický plán koncipovaný tak, aby si vynútil poriadok zločincov a bláznov v danom zariadení. Toto zariadenie, nazývané tiež "Inšpekčný dom" (*inspection house*), je prstencovitého tvaru a zahŕňa polokruhovú budovu s niekoľkými jednotlivými väzenskými bunkami, ktoré sú viditeľné z kontrolnej veže umiestnenej v strede polkruhu. Rozhľadňa je konštruovaná tak, aby umožňovala vidieť všetkých väzňov, zatiaľ čo väzni nikdy nevidia, či sú alebo nie sú práve sledovaní. Dokonca nemajú ani ako zistiť, či je práve niekto vo veži (Bentham, 1995). Asymetrický mocenský vzťah vytvorený touto budovou zabezpečuje automatické fungovanie kontroly a disciplíny a uľahčuje klasifikáciu a riadenie väzňov nútených žiť v úplnej a trvalej viditeľnosti, zatiaľ čo ich strážcovia sú pre nich neviditeľní. Farinosi, Manuela. “Deconstructing Bentham’s Panopticon: The New Metaphors of Surveillance in the Web 2.0 Environment.” TripleC, vol. 9, no. 1, 2011, pp. 62–76.

na ochranu pred mučením a iným ponižujúcim zaobchádzaním. Jedná sa o prípady, kedy elektronické sledovanie vykonávajú rôzne autoritárske režimy za účelom potlačenia disentu.[97] Takéto praktiky môžu vyústiť až do nezákonného väznenia a popravovania nepohodlných osôb. Keď revolucionári tzv. „arabského jara“, prevzali kontrolu nad štátnymi bezpečnostnými agentúrami v Tunisku, Egypte a Líbyi, zistili, že západná technológia sledovania bola používaná na monitorovanie politických aktivistov.[98] Drvivá väčšina krajín sveta nemá technologické vymoženosti ako má NSA alebo GCHQ a tak používajú kúpený software, vyrábaný súkromnými spoločnosťami, ktoré žiaľ častokrát nemajú problém tento software predať aj do autoritárskych režimov. Jedná sa napríklad o program FinFisher, vytvorený nemeckou spoločnosťou Gamma International. FinFisher má údajne schopnosť monitorovať tisíce ľudí prostredníctvom ich elektronických zariadení ako sú mobilné telefóny alebo cez ich sociálne siete a iné online aktivity.[99] Snahu zastrašiť pomocou digitálnej technológie demonštroval aj bývalý režim Viktora Janukoviča na Ukrajine, keď počas masových demonštrácií v Kyjeve v roku 2014 všetky osoby prítomné neďaleko miesta demonštrácie dostali na svoje mobilné telefóny SMS správu: „*Vážený účastník, ste zaregistrovaný ako účastník masového nepokoja.*“.[100]

Čo sa týka zberu metadát, na prvý pohľad by sa mohlo zdať, že sa jedná o miernejší zásah do súkromia ako pri zbieraní samotného obsahu komunikácie. Takto situáciu po Snowdenových odhaleniach upokojoval vtedajší prezident USA, Barack Obama:

> „*Nepočúvame vaše hovory. Ten program nie je o tom. Ako bolo uvedené, to, čo spravodajské služby robia, je sledovanie čísiel a dĺžky hovorov. Nepoze-*

[97] Assembly debate on 21 April 2015 (12th Sitting) (see Doc. 13734, report of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Pieter Omtzigt; and Doc. 13748, opinion of the Committee on Culture, Science, Education and Media, rapporteur: Sir Roger Gale). Text adopted by the Assembly on 21 April 2015 (12th Sitting), para. 8.

[98] Horwitz, Sari, Asokan, Shyamantha and Tate, Julie. Trade in surveillance technology raises worries, *Washington Post*, 1 December 2011, https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAF-FZOGO_story.html?utm_term=.02e8b72e495c.

[99] https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys Pre viac viď Goodman, Marc. „*Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*.“ First edition. Doubleday, 2015.

[100] Walker, Shaun and Grytsenko, Oksana. “Text messages warn Ukraine protesters they are 'participants in mass riot'”, *The Guardian*, 21 January 2014, https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

rajú sa na mená a nepozerajú sa na obsah, ale preberanie takzvaných metadát, môže viesť k identifikácií potencionálnych vodítok k osobám, ktoré sa môžu dopustiť terorizmu."[101]

Vlády sa niekedy zvyknú obvineniam z narušenia súkromia sledovaním brániť práve argumentom, že zbierali len metadáta a tak nedošlo k narušeniu súkromia, nakoľko samotný obsah telefonického rozhovoru, emailu, SMS správy nepoznajú. Údajne nepoznajú ani meno volajúceho, len telefónne číslo. Nakoľko ale táto argumentácia obstojí? Ak by ale boli metadáta tak nedôležité, dali by si štátne orgány tú námahu ich zbierať? Je skutočne pravda, že masívny zber metadát ľudí na súkromí neohrozuje? Alebo je to len trik vlád aby nemuseli oficiálne dodržiavať štandardy ľudských práv pri zásahu do súkromia, keďže argumentujú, že o zásah do súkromia sa vlastne ani nejedná?

Štátne orgány sa už dávno naučili, že režim zberu metadát je značne liberálnejší ako zber tvrdých informácií. Práve odhalenie masívneho zberu metadát, podľa oddielu č. 215 amerického Patriot Actu[102], bolo jedným z najkontroverznejších odhalení o aktivitách NSA na území USA.

V praxi je aj vyššie spomenutá definícia obsahu komunikácie pomerne zložitá. V prípade bežného emailu je to ešte relatívne jednoduché – obsah je samotný text správy a metadáta sú všetky ostatné údaje o danej komunikácii. Niekedy sa ale môže stať, že daná komunikovaná informácia je v jednej situácii obsah a v druhej nie. Napríklad, ak niekomu napíšem správu „som v meste", je informácia kde sa nachádzam fakticky obsahom a teda by k nej nemal byť prístup. Ak by si ale niekto našiel moje GPS súradnice, povedalo by mu to rovnakú vec, no tentokrát už vo forme metadát.[103] Často sa v súvislosti s metadátami používa metafora tzv. „zapečatenej obálky". Čo je v obálke zapečatené je obsah a je teda chránené, zatiaľ čo všetky ostatné informácie napísané na vonkajšej strane obálky, metadáta, sú zámerne nechané na očiach verejnosti a teda nepožívajú rovnakej ochrany. Táto metafora ale pri elektronických metadátach nie je vhodná. Elektronické metadáta totiž nie sú zverejnené odosielateľom zámerne. Práve naopak, väčšina ľudí ani

[101] Matthew DeLuca, Obama: 'Nobody Is Listening to Your Phone Calls,' NBC NEWS, June 7, 2013, http://usnews.nbcnews.com/_news/2013/06/07/18824941-obama-nobody-is-listening-to-your-telephone-calls.
[102] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.
[103] In Re Application of the United States of America for Historical Cell Site Data, No. 11-20884 (5th Cir. July 30, 2013), http://www.volokh.com/wp-content/uploads/2013/07/11-20884_Documents.pdf; United States v. Graham, 11-0094, LEXIS 26954 (D. Md. Mar. 1, 2012).

netuší, že ich telefón vytvára záznam o ich polohe, nakoľko neustále komunikuje s najbližšími prijímačmi, aby sa udržal v sieti.[104]

Digitálne technológie sú súčasťou každodenného života ľudí a tak má zber metadát obrovský potenciál odhaliť o ľuďoch aj pomerne citlivé informácie. Aj keď vlády argumentujú, že nevidia meno volaného, len telefónne číslo, v podstate im stačí pripojenie k internetu a pár telefonátov a vo väčšine prípadov nie je problém si majiteľa čísla dohľadať. Nakoľko zber metadát znamená aj zber informácií o polohe osoby[105], je pomerne jednoduché vytvoriť si po určitom čase prehľad o návykoch osoby, napríklad kedy chodí z práce, koho navštevuje, ako často a kam chodí. Výskum navyše ukazuje, že informácia o štyroch bodoch polohy stačí na identifikáciu 95% ľudí.[106] Prostredníctvom zberu metadát sa tak dá zistiť, či sledovaná osoba navštevuje kostol, synagógu, alebo mešitu, prípadne či sa účastní rôznych politických pochodov. Z týchto informácií, skombinovaných so znalosťou toho komu daná osoba volá, kedy, ako často a ako dlho trvá hovor, sa dá vyvodiť pomerne jasný obrázok, či už sa jedná o voľnočasové aktivity, pracovné návyky, ale aj intímnejšie informácie ako zdravotný stav, politické názory, náboženstvo, sexuálna orientácia, problémy v rodine, a tak podobne.[107] Práve tie najintímnejšie informácie sú najviac ohrozené zberom metadát. Študenti na MIT (*Massachusetts Institute of Technology*) napríklad ukázali, že vedia pomerne presne určiť sexuálnu orientáciu jednotlivca len na základe analýzy jeho kontaktov na sociálnych sieťach.[108] Ako píše Jane Mayer: *„Môžete vidieť telefonát gynekológovi, potom onkológovi a potom členom rodiny“*[109].

Edward Felten, profesor na Princetonskej univerzite, navyše tvrdí, že odpočúvanie samotného obsahu telefonických rozhovorov môže byť dosť komplikované vzhľadom na jazykové rozdiely, prízvuk, náhle zmeny tém, slangové výrazy, zámerné kódovanie

---

[104] Conley, Chris, *Metadata: Piecing together a privacy solution*, ACLU of Northern California, Inkworks Press, 2014, s. 13.
[105] ACLU of Northern California, Location-Based Services: Time for a Privacy Check-In 5, http://aclunc-tech.org/files/lbs-privacy-checkin.pdf.
[106] De Montjoye, Yves-alexandre, et al., Unique in the Crowd: The Privacy Bounds of Human Mobility, *Scientific Reports* (Nature Publisher Group), vol. 3, 2013, s. 1376.
[107] United States v. Maynard, No. 08-3080, 2010 U.S. App. LEXIS 16417, at *39-40 (D.C. Cir. Aug. 6, 2010).
[108] Carolyn Y. Johnson, Project ‘Gaydar’, BOSTON.COM, Sep. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.
[109] Jane Mayer, *What’s the Matter with Metadata? NEW YORKER*, June 6, 2013, http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html.

a iné vlastnosti verbálneho prejavu, ktoré zahmlievajú význam.[110] Obsah rozhovoru sa analyzuje automatizovanými metódami oveľa ťažšie práve preto, lebo sa nedá identifikovať jeho smerovanie, zatiaľ čo metadáta sú matematicky presné a štruktúrované, čo umožňuje jednoduchšie analytické skúmanie.[111] Je teda viac než pravdepodobné, že masívny zber elektronických metadát, je rovnako vážnym, ak nie ešte vážnejším narušením súkromia jednotlivcov. Práve preto by sa aj na tento spôsob sledovania mali uplatňovať hranice určené medzinárodnými štandardmi ochrany ľudských práv.

2.3 Aplikovateľnosť medzinárodných dokumentov v kontexte elektronického sledovania

Ľudské práva boli dlho prijímané ako výsostne garantované občanom na území príslušného štátu. Šlo o vzťah medzi štátom a jeho občanmi. Neskôr boli tieto práva garantované aj obyvateľom, ktorí síce nemali občianstvo tohto štátu, no žili na jeho území.[112] Dnes je nespochybniteľné, že medzinárodné zmluvy o ochrane ľudských práv, zaväzujú zmluvné strany, aby na svojom území dodržiavali štandard ochrany všetkým tak, ako im tieto zmluvy ukladajú. V poslednom čase sa však tento výlučne územný koncept opúšťa a stále viac sa diskutuje aj o extrateritoriálnej aplikácií ľudských práv. Vzhľadom na bezhraničný charakter internetu a informačných technológií celkovo, je prirodzené, že aj dáta a informácie putujú rôznymi časťami kyberpriestoru po celom svete. Nie je preto ojedinelé, že správa poslaná adresátovi, ktorý sa nachádza v rovnakom štáte ako odosielateľ, pred doručením niekoľkokrát „prekročí hranice“ v rámci kyberpriestoru. Z pohľadu ochrany súkromia je preto dôležité, aby boli medzinárodné zmluvy o ochrane ľudských práv aplikovateľné aj extrateritoriálne.

2.3.1 Aplikovateľnosť Paktu.

Asi najkontroverznejšia je debata o extrateritoriálnej aplikácii Paktu. Článok 2 odsek 1 Paktu definuje aplikovateľnosť nasledovne:

> „*Každý štát, ktorý je zmluvnou stranou paktu, sa zaväzuje všetkým jednotlivcom na svojom území a podliehajúcim jeho jurisdikcii zabezpečiť a rešpektovať práva uznané v tomto pakte bez akéhokoľvek rozlišovania podľa rasy,*

[110] Greenwald, Glenn*, Nikto sa neskryje*, Tatran, 2015, ISBN 9788022207317, s. 149.
[111] *Ibid*, s. 149-150.
[112] Viď napr. UN General Assembly, Res. 40/144, 13 December 1985, UN Doc. A/RES/40/144.

farby, pohlavia, náboženstva, politického alebo iného zmýšľania, národnostného alebo sociálneho pôvodu, majetku, rodu alebo iného postavenia.“[113]

Prvý problém je, že „na svojom území a podliehajúcim jeho jurisdikcii“ je možné vyložiť dvojako. Spor je v tom, či je nutné podmienky územia a jurisdikcie naplniť kumulatívne. Druhý problém s formuláciou tohto článku je v tom, že nie je jasné, čo sa vlastne v kontexte Paktu myslí pod pojmom „jurisdikcia“.

2.3.1.1 Je nutné podmienky územia a jurisdikcie naplniť kumulatívne?

Najprv k otázke toho, ako rozumieť vete „na svojom území a podliehajúcim jeho jurisdikcii“. Interpretácia prezentovaná hlavne zo strany USA je, že tieto dve podmienky musia byť splnené kumulatívne. Táto argumentácia ale neobstojí z troch dôvodov:

a) Samotné historické súvislosti prípravy Paktu a *travaux préparatoires*.
b) Výklad a interpretácia Paktu v súlade s medzinárodným právom.
c) Judikatúra Medzinárodného súdneho dvora (ďalej len „MSD“) a stanovisko Výboru.

a) Historické súvislosti prípravy Paktu

Boli to práve Spojené štáty, ktoré počas vytvárania Paktu naliehali na to, aby sa znenie zmenilo a nezahrňovalo len jurisdikciu, ale zároveň aj územie.[114] Úryvok zo zasadnutia Ekonomickej a sociálnej rady OSN, orgánu poverenému navrhnúť znenie Paktu, objasňuje vtedajšiu hlavnú argumentáciu zástupcov Spojených štátov (E. Roosevelt):

„Spojené štáty sa obávali, že bez tohto doplnenia by návrh Paktu mohol byť vykladaný tak, že zaväzuje zmluvné strany, aby prijali právne predpisy týkajúce sa osôb, ktoré sú síce mimo ich územia, ale technicky v rámci ich jurisdikcie, na určité účely. Ako ilustrácia by mohli slúžiť okupované územia Nemecka, Rakúska a Japonska: osoby na týchto územiach podliehali jurisdikcii okupačných štátov v určitých aspektoch, no boli mimo pôsobnosti legislatívy týchto štátov. Ďalšia ilustrácia môže byť prípad prenajatých území: niektoré krajiny prenajali určité časti územia iným štátom na limitované účely a mohol

[113] Jedná sa o preklad autora práce. Oficiálny preklad, tak ako bol publikovaný v zbierke zákonov Slovenskej republiky, bol (už aj podľa očakávania) zlý. Nerozumiem, ako mohli preložiť vetu „*within its territory and subject to its jurisdiction*“ na „*na svojom území podliehajúcim jeho jurisdikcii*“.
[114] Milanovic, op. cit., s. 102.

by tu nastať konflikt právomocí medzi prenajímajúcim štátom a nájomcom.“[115]

Je nutné spomenúť aj druhú stranu, napríklad zástupca francúzskej delegácie (P. Juvigny) navrhoval vypustiť zo znenia Paktu „na svojom území a“ presne z dôvodu, aby sa zabránilo potencionálne nevhodnému doslovnému výkladu, v dôsledku ktorého by sa Pakt nevzťahoval na osoby, ktoré síce podliehajú jurisdikcii štátu, no nie sú na jeho území.[116] Návrhov k článku 2 ods. 1 padlo počas prípravy Paktu mnoho, no nedá sa rozhodne určiť, či autori Paktu mali skutočne v úmysle úplne vylúčiť extrateritoriálnu aplikovateľnosť Paktu.[117] Je ale zaujímavé, že autori sa počas celého tohto sporu sústredili výlučne len na otázku toho, ako garantovať práva podľa Paktu občanom štátu žijúcim v zahraničí. To súvisí s chápaním jurisdikcie. Nakoľko to autori vnímali tak, že keď nad niekým v zahraničí bude mať štát jurisdikciu, budú to len jeho vlastní občania, otázka garancie práv aj iným osobám mimo vlastných občanov v podstate otvorená nebola.[118]

Zvlášť s prihliadnutím k tomu, že v čase prípravy Paktu nešlo predpokladať budúci vývoj technológií a globalizáciu, si dovolím tvrdiť, že autori Paktu nemohli pre tento prípad extrateritoriálnu aplikovateľnosť vylúčiť. ICJ taktiež stanovil, že medzinárodné zmluvy je potrebné vykladať v rámci právneho systému prevládajúceho v čase výkladu a nie v čase prijímania textu zmluvy.[119] Argumentácia Spojených štátov *travaux préparatoires* je teda mylná.

b) Výklad a interpretácia článku 2 odseku 1

Pakt spĺňa definíciu medzinárodnej zmluvy podľa článku 2 odseku 1 písmena a) VDZP a zároveň neobsahuje vlastné špecifické výkladové ustanovenia. Pri jeho výklade teda budem vychádzať z všeobecných pravidiel výkladu pre medzinárodné zmluvy, ako ich zavádza VDZP.

VDZP nám vo svojom článku 31 udáva základné pravidlo výkladu medzinárodnej zmluvy:

---

[115] Summary Record of the Hundred and Thirty-Eighth Meeting, U.N. ESCOR Hum. Rts. Comm., 6th Sess., 138th mtg at 10, para 34, U.N. Doc. E/CN.4/SR.138 (1950).
[116] Mr Juvigny (France) E/CN.4/SR.328, of 24 June 1952, s. 10.
[117] Milanovic, op. cit., s. 103.
[118] Da Costa, Karen. *The Extraterritorial Application of Selected Human Rights Treaties*. Leiden; Boston, Martinus Nijhoff Publishers, 2013, s. 36.
[119] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970) para. 52.

„Zmluva sa musí vykladať v dobrej viere, v súlade s obvyklým významom, ktorý sa dáva výrazom v zmluve v ich celkovej súvislosti, a takisto s prihliadnutím na predmet a účel zmluvy.“

Jedná sa o kombináciu metód výkladu prevzatých z obecnej teórie práva, teda výkladu gramatického, systematického, logického, historického a teleologického.[120] Toto výkladové pravidlo je následne v článku 32 VDZP doplnené o tzv. „doplnkové prostriedky výkladu“, pre prípad, že by výklad podľa článku 31 ponechával význam „*nejednoznačným, nejasným, alebo by viedol k výsledku zrejme nezmyselnému a nerozumnému, ktoré zahŕňajú štúdium prípravných materiálov na zmluve a okolností, za ktorých bola zmluva uzavretá*“[121].

Základné výkladové pravidlo sa teda skladá z troch hlavných princípov:

a) dobrá viera – vyjadruje zásadu článku 26 VDZP, že zmluvy sa majú dodržovať (*pacta sunt servanda*)
b) obvyklý význam v celkovej súvislosti – ide o domnienku, že zmluvné strany mali v úmysle vykladať dané ustanovenie podľa bežného významu slov (gramatický výklad) ktoré v nej použili, no zároveň je dôležité tieto výrazy vykladať v celkovej súvislosti (systematický výklad)
c) predmet a účel zmluvy – princíp, že zmluvy by sa nemali vykladať abstraktne a bez zamyslenia sa nad tým, čo je predmetom zmluvy a akému účelu zmluva vlastne slúži (teleologický výklad)

Ako som už písal vyššie, problematické pri výklade článku 2(1) Paktu je to, že veta *„štát* [...] *sa zaväzuje všetkým jednotlivcom na svojom území a podliehajúcim jeho jurisdikcii zabezpečiť* [...] *práva* [...]*“* sa dá vyložiť dvojako. Čisto z gramatického výkladu nie je jasné, či spojka „a“ znamená, že podmienky musia byť splnené kumulatívne alebo nie. Dalo by sa argumentovať, že ak by tieto podmienky nemali byť naplnené kumulatívne, vhodnejším by namiesto spojky „a“ bola spojka „alebo“. Rovnako sa ale dá argumentovať z druhej strany, že ak by tieto podmienky mali byť naplnené kumulatívne, vhodnejšie by bolo namiesto „a“ použiť „a zároveň“. V tomto prípade sú relevantné oba výklady a teda by sme mali používať ten, ktorý je viac v súlade s predmetom a účelom zmluvy.

[120] Čepelka, Č., Šturma, P., *Mezinárodní právo veřejné*, op. cit., s. 149 marg. 48.
[121] VDZP čl. 32.

Tu je na mieste taktiež zdôrazniť, že medzinárodné zmluvy o ľudských právach sa od klasických medzinárodných zmlúv odlišujú a výklad predmetu a účelu týchto zmlúv teda vyžaduje, aby sa zohľadnili ich osobitné charakteristiky. Klasické medzinárodné zmluvy napríklad regulujú vzťahy medzi subjektmi medzinárodného práva - štátmi - zatiaľ čo medzinárodné zmluvy o ľudských právach upravujú vzťahy medzi štátom ako zmluvnou stranou zmluvy a obyvateľstvom, ktorému štát garantuje určitý štandard ochrany ľudských práv. V druhom prípade neexistuje medzi jednotlivými zmluvnými stranami recipročný vzťah.[122] MSD taktiež uznal špecifickosť medzinárodných zmlúv o ľudských právach, keď v súvislosti s Dohovorom o zabránení a trestaní zločinu genocídy[123] stanovil, že „*zmluvné štáty tu nemajú žiadne vlastné záujmy, majú len jeden spoločný záujem a to dosiahnutie vznešených cieľov, ktoré sú dôvodom existencie tohto dohovoru*“[124]. Z týchto všetkých dôvodov hrá práve predmet a účel zmluvy kľúčovú úlohu pri interpretácií medzinárodných zmlúv o ľudských právach.

Výbor sa k predmetu a účelu paktu vyjadril nasledovne:

> „*Predmetom a účelom Paktu je vytvoriť právne záväzný štandard ľudských práv vymedzením určitých občianskych a politických práv a ich zaradením do rámca povinností, ktoré sú právne záväzné pre štáty, ktoré ich ratifikujú; a poskytnúť účinný mechanizmus dohľadu nad vykonávanými záväzkami.*“[125]

---

[122] Viď napr. Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, Advisory Opinion, ICJ Reports 1951, 15, s. 23. Tento princíp dobre vystihol Inter-americký súd pre ľudské práva v posudku *The Effect of Reservations on the Entry Into Force of the American Convention on Human Rights: „The Court must emphasize, however, that modern human rights treaties in general, and the American Convention in particular, are not multilateral treaties of the traditional type concluded to accomplish the reciprocal exchange of rights for the mutual benefit of the contracting States. Their object and purpose is the protection of the basic rights of individual human beings irrespective of their nationality, both against the State of their nationality and all other contracting States. In concluding these human rights treaties, the States can be deemed to submit themselves to a legal order within which they, for the common good, assume various obligations, not in relation to other States, but towards all individuals within their jurisdiction”.* The Effect of Reservations on the Entry Into Force of the American Convention on Human Rights (Arts. 74 and 75), Advisory Opinion OC-2/82, September 24, 1982, Inter-Am. Ct. H.R. (Ser. A) No. 2 (1982).

[123] Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948, 78 U.N.T.S. 277, p. 277.

[124] Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, Advisory Opinion, ICJ Reports 1951, 15, s.8.: „*In such a convention the contracting States do not have any interests of their own ; they merely have, one and all, a common interest, namely, the accomplishment of those high purposes which are the raison d'être of the convention. Consequently, in a convention of this type one cannot speak of individual advantages or disadvantages to States, or of the maintenance of a perfect contractual balance between rights and duties*. “

[125] UN Human Rights Committee (HRC), General Comment No. 24 (52), General comment on issues relating to reservations made upon ratification or accession to the Covenant or the Optional Protocols thereto, or in relation to declarations under article 41 of the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.6 (1994). para. 7.

Už z preambuly Paktu je zrejmé, že účelom je naplniť záväzok štátov vyplývajúci z Charty OSN podporovať všeobecnú úctu k ľudským právam a slobodám a k ich zachovaniu. Preambula sa hlási k prirodzenej dôstojnosti a k myšlienke rovnakých a neodňateľných práv pre všetkých. V minulosti by možno bolo pre naplnenie tohto účelu dostačujúce, aby každá zmluvná strana garantovala práva v rámci svojho územia, no v dnešnej dobe táto interpretácia obstojí len ťažko. Keby sme sa držali interpretácie kumulatívneho naplnenia podmienok v Pakte, tak by vzhľadom na masívne cezhraničné sledovanie dochádzalo k absolútnemu popretiu zmyslu Paktu. Dovolím si tvrdiť, že by dochádzalo až k absurdným dôsledkom, ako ich popisuje Sinha:

> „*Ak by sme zovšeobecnili argumentáciu Spojených štátov, Pakt by chránil súkromie Američanov iba proti svojvoľnému a ilegálnemu zásahu zo strany Spojených štátov, a nechal ich zraniteľných voči zásahom každou inou vládou na svete.*“[126]

Táto prax by navyše mohla mať za následok, že by si štáty jednoducho „*outsourcovali*“ informácie získané zahraničným sledovaním od iných štátov a z pohľadu Paktu by teda nedochádzalo k porušeniu. Takýmto výkladom by Pakt rozhodne nezabezpečoval ľudom dostatočnú ochranu ich práv, čo je v rozpore s jeho prirodzenoprávnym základom odkazujúcim na Všeobecnú deklaráciu ľudských práv. Argumentácia kumulatívnym splnením podmienok je teda aj z tohto pohľadu mylná a mala by za príčinu neefektívny systém ochrany ľudských práv.

c) Stanovisko Výboru

Tretím a zároveň posledným argumentom, prečo je Pakt aplikovateľný extrateritoriálne, je stanovisko Výboru podporené aj judikatúrou MSD. Výbor sa k extrateritorialite Paktu vyjadril pomerne jasne vo Všeobecnom komentári (GC) č. 10:

> „*Zmluvné strany sú podľa článku 2 ods. 1 povinné rešpektovať a zabezpečovať práva podľa Paktu všetkým osobám, ktoré sú na ich území a všetkým osobám, ktoré podliehajú ich jurisdikcii. To znamená, že zmluvná strana musí rešpektovať a zabezpečiť práva ustanovené v Pakte každému, kto podlieha*

[126] Sinha, G. Alex, „NSA Surveillance since 9/11 and the human right to privacy.“ *Loyola Law Review* 59, 2013, 861-1049, s. 902.

efektívnej kontrole tejto zmluvnej strany, aj keď sa nenachádza na území tejto zmluvnej strany.“[127]

Toto je jednoznačné stanovisko Výboru v prospech aplikovateľnosti Paktu na osoby mimo územia štátu, za predpokladu, že podliehajú jeho jurisdikcii. Výbor tento výklad dlhodobo potvrdzuje aj vo svojej praxi posudzovania oznámení jednotlivcov, kde už v 80. rokoch minulého storočia argumentuje, že „*by bolo neprimerané interpretovať zodpovednosť podľa článku 2 Paktu tak, že zmluvný štát môže páchať porušenia na území iného štátu, ktoré na vlastnom území páchať nesmie*“ [128].

Prípadné pochybnosti o argumentácii Výboru, nakoľko sa formálne nejedná o záväzné rozhodnutia, odstraňuje MSD v prípade *Wall*[129], kde vyslovene odkazuje na argumentáciu Výboru, čím potvrdzuje tento postoj ako skutočne správny z pohľadu medzinárodného práva.[130]

2.3.1.2 Čo sa rozumie pod jurisdikciou štátu?

Druhou dôležitou otázkou pre aplikovateľnosť Paktu na masívne sledovanie, zvlášť to zahraničné, je otázka, kedy vlastne osoby podliehajú pod jurisdikciu štátu. Vo všeobecnosti je v medzinárodnom práve pojem jurisdikcia chápaný buď to ako vykonávanie kontroly nad územím (územná jurisdikcia), alebo nad jednotlivcami (osobná jurisdikcia). Pre účely aplikovateľnosti Paktu na zahraničné sledovanie ale nestačí, aby sa jurisdikcia štátu uplatňovala len na teritoriálnom princípe. Či štát nad niekým má alebo nemá jurisdikciu závisí na tom, či nad ním vykonáva tzv. „efektívnu kontrolu“.

Jediný spôsob ako Paktom chrániť pred masívnym sledovaním aj osoby v zahraničí, je dokázať, že aspoň dočasne podliehajú efektívnej kontrole sledujúceho štátu. Výbor už v minulosti uznal extrateritoriálnu aplikáciu Paktu v prípadoch, kedy agenti štátu vykonávali moc a kontrolu nad osobami v zahraničí.[131] Je nutné si uvedomiť, že v prípade digitálneho sledovania majú činy štátnych orgánov, fyzicky sa nachádzajúcich na území

[127] UN Human Rights Committee (HRC) General Comment No. 31, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (26 May 2004), para.10.
[128] HRC: Lopez Burgos v. Uruguay, Communication No. R.12/52, Supp. No. 40, 176, UN Doc. A/36/40 (1981), para.12.3;
[129] Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 July 2004, para 109-111.
[130] Wilde, Ralph. „*Human Rights Beyond Borders at the World Court: The Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties*.“ Chinese Journal of International Law 12.4 (2013): 639-777, s. 27
[131] HRC: Lopez Burgos v. Uruguay. op. cit.

domovského štátu, priame následky v zahraničí. Tieto orgány navyše nikdy nestrácajú nad situáciou kontrolu, čím sa vytvára priamy vzťah medzi štátom a sledovaným jednotlivcom.[132] Nakoľko ide o priamu kontrolu a moc nad osobnými dátami ľudí, toto ich jednanie by nemalo byť oslobodené od povinností podľa Paktu. Vysoký Komisár OSN pre ľudské práva to taktiež potvrdzuje v jednej z najdôležitejších správ týkajúcich sa digitálneho prostredia, kde argumentuje nasledovne:

> „*Digitálne sledovanie môže spustiť záväzky štátu v oblasti ľudských práv, ak toto sledovanie zahŕňa výkon štátnej moci alebo účinnú kontrolu vo vzťahu k infraštruktúre digitálnej komunikácie a to bez ohľadu na to, kde sa nachádza, napríklad priamym napojením na túto infraštruktúru alebo preniknutím do nej. Rovnako, ak štát vykonáva dohľad nad treťou osobou, ktorá fyzicky kontroluje dáta, tento štát bude mať taktiež povinnosti vyplývajúce z Paktu.*“[133]

2.3.2 Aplikovateľnosť Dohovoru

Článok 1 Dohovoru vymedzuje jeho aplikovateľnosť nasledovne:

> „*Vysoké zmluvné strany priznávajú každému, kto podlieha ich jurisdikcii, práva a slobody uvedené v hlave I tohto dohovoru*“

Dohovor teda obsahuje len odkaz na jurisdikciu a vynecháva podmienku teritoriality. Avšak, nakoľko sa ESLP zatiaľ jednoznačne k otázke aplikovateľnosti Dohovoru na cezhraničné sledovanie nevyjadril, je opäť nutná interpretácia Dohovoru. Pri výklade je dôležité pamätať na to, že sa musí zohľadniť osobitný charakter Dohovoru, ako judikoval ESLP:

> „*Cieľ a účel Dohovoru ako nástroja ochrany jednotlivcov preto vyžaduje, aby jeho ustanovenia boli interpretované a uplatňované tak, aby boli záruky praktické a účinné. Navyše, akýkoľvek výklad garantovaných práv a slobôd musí byť v súlade s duchom Dohovoru, nástroja určeného na zachovanie a podporu ideálov a hodnôt demokratickej spoločnosti*.“[134]

2.3.2.1 Judikatúra ESLP k otázke extrateritoriálnej aplikácií Dohovoru.

Aj napriek tomu, že sa ESLP stále jasne nevyjadril v prospech extrateritoriálnej aplikácie Dohovoru v súvislosti s cezhraničným sledovaním, je možné povedať, že sa

[132] HRC: Lopez Burgos v. Uruguay, op. cit., para. 12.2.
[133] A/HRC/27/37, op. cit., para. 34.
[134] ESLP: Soering v. UK (App. No. 14038/88) 7 July 1989, para. 87.

k tomu vo svojej argumentácii v jednotlivých prípadoch stále približuje. Prejavuje sa tak zásada dynamického výkladu Dohovoru, chápaného ako „živého nástroja“ (*living instrument*). ESLP teda postupne berie pri interpretácií Dohovoru do úvahy vývoj spoločnosti a prispôsobuje tak výklad moderným podmienkam. Ani tento princíp ale neplatí bez výnimky.

Jedným z prvých prípadov kedy sa ESLP vyjadril k extrateritorialite Dohovoru bol prípad *Loizidou*[135], kde ESLP stanovil, že zmluvné strany Dohovoru môžu byť brané k zodpovednosti za porušenia Dohovoru aj na území mimo svojho štátu v tom prípade, že vykonávajú nad daným územím účinnú kontrolu.[136] Tento výklad sa síce viaže len na účinnú kontrolu nad územím, no jedná sa o prvé kroky k objasneniu extrateritoriality Dohovoru.

Ako krok späť potom pôsobí výklad extrateritoriality v prípade *Bankovic*[137]. ESLP prípad *Banković* odmietol pre neprípustnosť a argumentoval, že extrateritoriálna aplikácia Dohovoru by mala byť len výnimočná a posudzovaná pre jednotlivé prípady zvlášť.[138] Vojsko Organizácie Severoatlantickej zmluvy (ďalej len „NATO“), ktoré letecky zbombardovalo televíznu vežu v Belehrade v roku 1999, podľa úvahy ESLP, nevykonávalo účinnú kontrolu nad územím, nakoľko v oblasti nemalo prítomné pozemné jednotky. Toto rozhodnutie je pomerne kontroverzné najmä z toho dôvodu, že ESLP sa uchýlil, aj napriek stálemu opakovaniu a zdôrazňovaniu dôležitosti dynamického výkladu vo svojej judikatúre, k argumentácií gramatickým výkladom pričom tvrdil, že ak by autori Dohovoru zamýšľali takú aplikovateľnosť, prijali by Dohovor v inom znení.[139]

Prelomovým rozhodnutím, odchyľujúcim sa od výkladu *Banković*, je rozhodnutie v prípade *Al-Skeini*[140]. V tomto rozhodnutí ESLP pripustil dva možné dôvody extrateritoriálnej aplikácie Dohovoru:

a) moc a kontrola štátneho orgánu nad jednotlivcami (aj mimo územia)[141]
b) účinná kontrola nad územím[142]

---

[135] ESLP: Loizidou v. Turecko (App no. 15318/89) 23 March 1995.
[136] *Ibid*, para. 52.
[137] ESLP: Banković et al v. Belgicko et al (App. no. 52207/99) 12 December 2001.
[138] *Ibid*., para. 67.
[139] Tým samozrejme nechcem povedať, že gramatický výklad nie je pri interpretácii medzinárodnej zmluvy dôležitý. V tomto prípade sa ale podľa mňa ESLP odchýlil od svojej praxe výkladu Dohovoru ako živého inštrumentu, čo napokon potvrdzuje aj jeho následná judikatúra. ESLP: Banković para. 75.
[140] ESLP: Al-Skeini et al v. UK (App no 55721/07) 7 July 2011.
[141] *Ibid*, para. 133-137.
[142] *Ibid*, para. 138-140.

Pre účely sledovania digitálnej komunikácie je relevantná prvá forma – moc a kontrola štátneho orgánu. Síce sa v prípade Al-Skeini ešte stále jednalo len o fyzickú moc a kontrolu nad jednotlivcom v zmysle fyzického zadržiavania danej osoby, v následnej judikatúre, ako napríklad v prípadoch *Jaloud*[143] a *Pad*[144], už fyzická kontrola nad jednotlivcom nebola zo strany štátu vykonávaná a ESLP taktiež dospel k názoru, že Dohovor aplikovateľný je.[145] ESLP sa v týchto prípadoch zjavne kloní k názoru, že už len fakt, že štát má moc efektívne zasiahnuť do práva danej osoby, vytvára štátu záväzky podľa Dohovoru. Pri takejto interpretácií by sa dalo v prípade sledovania, zberu a ukladaní digitálnej komunikácie argumentovať, že štáty nad nimi vykonávajú účinnú kontrolu. Zaujímavou je aj argumentácia tzv. „virtuálnou kontrolou", akousi paralelou na účinnú kontrolu nad územím alebo jednotlivcom, ktorá predpokladá, že štáty vykonávajú účinnú kontrolu nad dátami v kyberpriestore a vzťahujú sa na nich záväzky podľa Dohovoru.[146]

[143] ESLP: Jaloud v. Holandsko (Application no. 47708/08) 20 November 2014
[144] ESLP: Pad et al. v. Turecko (App no. 60167/00) 28 June 2007.
[145] ESLP: Pad et al. v. Turecko bol však odmietnutý pre nevyčerpanie všetkých opravných prostriedkov.
[146] Viac k myšlienke virtuálnej kontroly viď Margulies, Peter. The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, Fordham Law Review 82.5 (2014): 2137-1677.

3. Sledovacie programy NSA a GCHQ a ich súlad s medzinárodným právom

V rámci tejto kapitoly je analyzovaný súlad najznámejších programov masívneho sledovania s medzinárodným právom. Kapitola začína stručnou charakteristikou daných programov a následne sú na nich aplikované štandardy medzinárodných zmlúv o ľudských právach charakterizovaných vyššie. Pre účely tejto kapitoly je teda predpokladaná extrateritoriálna aplikovateľnosť Paktu a Dohovoru.

3.1 Obecný popis programov sledovania

Zameriam sa na programy americkej NSA a britskej GCHQ, nakoľko sú najviac zdokumentované. Vychádzať pritom budem ako z informácií dostupných vďaka ich vyneseniu americkým *whistleblowerom* Edwardom Snowdenom, tak aj z oficiálnych štátnych zdrojov. Popis programov je zjednodušený, aby bol zrozumiteľný pre potreby tejto práce.

Jeden z prvých dokumentov zverejnených Snowdenom sa venoval programu „Boundless informant" a získavaniu telefónnych metadát americkou NSA. Išlo o zverejnenie údajného tajného súdneho príkazu[147], ktorý vydal americký Súd pre dohľad nad zahraničnou spravodajskou službou (*Foreign Intelligence Surveillance Court*, ďalej len „FISC") podľa zákona *Foreign Intelligence Surveillance Act*[148] (ďalej len „FISA"). Tieto dokumenty dokazujú, že FISC rozhodnutím z 25. apríla 2013 nariadil spoločnosti Verizon[149] dočasne sprístupniť NSA informácie o metadátach ich zákazníkov.[150] Súd sa v príkaze opiera o ustanovenia vyššie spomínaného Patriot Actu z roku 2001 a argumentuje, že je splnená podmienka 50 U.S.C. § 1861 a jedná sa o „obchodné záznamy". V skutočnosti ale ide o blanketné zmocnenie NSA zbierať údaje o hovoroch zákazníkov Verizonu a teda aj o amerických občanoch. Práve program Boundless informant má následne za úlohu takéto metadáta z celého sveta analyzovať.

---

[147] Celý príkaz viď https://edwardsnowden.com/2013/06/06/verizon-fisa-court-order/

[148] An Act to authorize electronic surveillance to obtain foreign intelligence information, October 25, 1978.

[149] Verizon Communications, Inc. je nadnárodný telekomunikačný konglomerát a najväčšieho poskytovateľ bezdrôtových komunikačných služieb v USA.

[150] "*It is hereby ordered that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications*

(i) between the United States and abroad; or

(ii) wholly within the United States, including local telephone calls."

Ďalší z programov NSA, predstavujúci potencionálny zásah do súkromia osôb, má názov PRISM. Tento program fakticky umožňuje NSA prístup k dátam na serveroch spoločností ako je Microsoft, Apple, Google, Facebook, Skype, Yahoo! a ďalších.[151] Jedná sa o spoločnosti, ktoré sprostredkovávajú drvivú väčšinu internetovej komunikácie súkromných osôb. Údaje, ktoré sú takto zbierané, zahŕňajú históriu vyhľadávania, e-mailovú komunikáciu, chat, video, prenos súborov a podobne.

UPSTREAM je súhrnný názov pre systém zberu dát priamo z tzv. „chrbtice internetu", tj. centrálnej siete spájajúcej komerčné, vládne, akademické a iné vysokokapacitné dátové cesty, ktorá umožňuje prenos dát medzi jednotlivými kontinentmi.[152] Podstata programu UPSTREAM je v napojení sa na komunikačnú infraštruktúru, hlavne podmorské optické káble. UPSTREAM tvoria štyri programy s názvami FAIRVIEW, BLARNEY, STORMBREW a OAKSTAR. Tieto programy umožňujú NSA prístup do medzinárodných systémov sietí a následne presmerujú komunikačné záznamy cieľovej krajiny do úložísk NSA.[153] Program FAIRVIEW sa zameriava na zber metadát z celého sveta. OAKSTAR a STORMBREW taktiež využívajú prístup k zahraničným telekomunikačným systémom, pričom program STORMBREW poskytuje prístup k internetovej a telefonickej komunikácii, ktorá prechádza cez územie USA na tzv. „uzloch", čím využíva to, že väčšina internetovej komunikácie v určitom momente prejde aj cez komunikačnú infraštruktúru umiestnenú v USA.[154] Program BLARNEY sa navyše zameriava aj na hospodársku špionáž. Pri svojich aktivitách v rámci hospodárskej a obchodnej špionáže sa NSA zamerala hlavne na „*zahraničnú politiku a obchodne aktivity Belgicka, Francúzska, Nemecka, Talianska a Španielska, ale aj Brazílie, Japonska a Mexika*".[155] Ďalším z kontroverzných príkladov zahŕňajúci tentokrát diplomatickú špionáž, zahŕňa odpočúvanie členov Bezpečnostnej rady OSN, s úmyslom zistiť ich postoj pred hlasovaním o rezolúcii ukladajúcej sankcie Iránu. Takéto informácie, ako sama rozviedka uvádza vo svojej správe[156], im poskytli výhodu pri vyjednávaní. Hospodárskej a diplomatickej špionáži je venovaná záverečná kapitola tejto práce.

---

[151] Cf. Glenn Greenwald and Ewen McAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' The Guardian (June 7 2013) http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni-Article:in /2body%/20ink

[152] https://www.techopedia.com/definition/20115/internet-backbone

[153] Greenwald, op. cit., s. 115.

[154] *Ibid*, s. 119.

[155] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 154.

[156] *Ibid*. s. 161

Program X-KEYSCORE umožňuje analytikom rýchlo a efektívne v množstve získaných dát vyhľadávať. Podľa vynesených dokumentov sa vyhľadávanie v X-KEYSCORE nápadne podobá na akékoľvek iné vyhľadávanie, napríklad vo vyhľadávači Google. Po zadaní požadovaného textu program vyfiltruje všetky potrebné zhodujúce sa informácie. Použitím tohto programu môže NSA prehľadávať ako emailovú komunikáciu a správy na Facebooku, tak aj technické informácie na danom počítači alebo počet a adresy navštívených stránok. Dotyčný analytik si údajne ani nepotrebuje požiadavku dať nikým oficiálne schváliť. Jednoducho len formálne uvedie dôvod daného vyhľadávania.[157]

Program TEMPORA je programom britskej spravodajskej služby GCHQ. Podobne ako americký STORMBREW, britská TEMPORA využíva fakt, že väčšina európskej komunikácie prechádza cez územie Spojeného kráľovstva. GCHQ sa tak napojila na transatlantické optické káble a tým získala prístup k obrovskému množstvu dát[158] z internetovej a mobilnej komunikácie.[159] Získané dáta sú údajne uchovávané na rozbor najbližších 72 hodín aj s obsahom a ďalších 30 dní ešte ako metadáta. V rámci rozboru sú používané tzv. „ukazovatele“ (*selectors*), ktoré filtrujú podozrivú alebo požadovanú komunikáciu na ďalší rozbor, tentokrát už pracovníkmi spravodajskej služby.[160]

Je prirodzené, že spojenci si medzi sebou zdieľajú informácie v snahe navzájom si vypomôcť. Výnimkou samozrejme nie sú ani tajné služby a tak nie je prekvapením, že americká NSA a britská GCHQ dlhodobo spolupracujú a zdieľajú si informácie zozbierané aj v súvislosti s vyššie zmienenými programami. Táto spolupráca má svoje korene už v roku 1946, kedy bola medzi USA a UK uzavretá *British-U.S. Communication Intelligence Agreement*[161], v ktorej sa strany zaviazali k neobmedzenej výmene informácií z rôznych spravodajských operácií, vrátane zberu dát (*collection of traffic*). V roku 1956 bola rozšírená o dodatok[162], v rámci ktorého sa do dohody pridružili aj Kanada, Novy

[157] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 175
[158] Uniknuté dokumenty hovoria až o možných 21 petabajtov dát denne.
[159] Ewen McAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' The Guardian (21 June 2013) http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[160] Georgieva, Ilina. The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. *Utrecht Journal of International and European Law 31.80*, 2015, s. 107.
[161] British U.S. Communication Intelligence Agreement (5 Mar. 1946), https://www.nsa.gov/news-features/declassified-documents/ukusa/assets/files/agreement_outline_5mar46.pdf
[162] Amendment No. 4 To The Appendices To The UK USA Agreement (Third Edition) (10 May 1955).

Zéland a Austrália. Tak vznikla tzv. sieť „Piatich očí“ („*Five Eyes intelligence sharing network*“). Dôsledkom toho je vysoko pravdepodobné, že sa britská GCHQ bez väčších problémov mala možnosť dostať k informáciám zozbieraným americkou NSA napríklad v rámci programu PRISM a NSA zas k informáciám z programu TEMPORA.[163]

Vo všeobecnosti je teda možné konštatovať, že tieto programy vo svojej podstate zasahujú do práva na súkromie osôb, ktoré sú cieľom sledovania. Nakoľko sa jedná o programy masívneho sledovania, je cieľom prakticky ktokoľvek, kto používa digitálne komunikácie. Tieto programy dávajú štátnym orgánom možnosť nie len danú komunikáciu zachytiť (Upstream, Tempora) alebo získať od „partnerov“ (PRISM, metadáta podľa oddielu 215 FISA) ale ju aj triediť, analyzovať a uchovávať (Boundless Informant, X-KEYSCORE)

3.2 Právny základ programov

V prípade NSA sa v prvom rade jedná o vyššie spomínaný zákon FISA na základe ktorého súdy FISC schvaľujú sledovanie. Podľa paragrafu 103 je úlohou FISC rozhodovať o návrhoch na elektronické sledovanie. Tento proces fakticky umožňuje americkej vláde sledovať potencionálne nebezpečné osoby vo vnútri Spojených štátov v súlade so zákonom. FISC by mal zároveň vykonávať aj účinný dohľad nad sledovaním, aby sa tak zabránilo prípadnému zneužitiu moci.

Program získavania metadát o telefonických hovoroch je založený na novelizácií FISA prostredníctvom oddielu č. 215 Patriot Act. Patriot Act je nutné chápať v historických súvislostiach. Bol prijatý pár týždňov po udalostiach 11. septembra 2001 a je teda pochopiteľné, že rozširoval právomoci orgánov v boji proti terorizmu. V prípade tohto programu sa jedná primárne o vnútroštátne sledovanie, zatiaľ čo program PRISM, založený na oddiele č. 702 FISA, je program pre účely zahraničného sledovania. Oddiel č. 215 Patriot Act znie nasledovne:

> *„Riaditeľ Federálneho vyšetrovacieho úradu alebo splnomocnený zástupca riaditeľa […] môže podať návrh na vydanie príkazu vyžadujúceho predloženie akýchkoľvek hmotných vecí (vrátane kníh, záznamov, dokladov a iných vecí) pre účely vyšetrovania na ochranu pred medzinárodným terorizmom*

[163] Nick Hopkins and others, 'GCHQ: inside the top secretworld of Britain's biggest spy agency' The Guardian (1 August 2013) <http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden>

alebo tajnými spravodajskými činnosťami za predpokladu, že takéto vyšetrovanie osoby Spojených štátov sa nevykonáva výhradne na základe činností chránených prvým dodatkom Ústavy."

Paragraf v nasledujúcich odsekoch ukladá, že návrh je potrebné podať sudcovi FISA, za akých podmienok je možné ho podať a taktiež ukladá dohľad vo forme polročných správ pred americkým Kongresom a príslušnými výbormi. Medzi nutné informácie, ktoré musí takáto žiadosť obsahovať patrí informácia, že existujú opodstatnené dôvody domnievať sa, že konkrétne skutočnosti sú relevantné pre už schválené vyšetrovanie.

V roku 2008 americký Kongres novelizoval zákon FISA tzv. FISA Amendments Act[164] (ďalej len „FAA"). FAA uvádza v oddiele č. 702, že ak je cieľom zahraničného sledovania osoba, ktorá nie je „osobou v Spojených štátoch" (čím sa myslí, že nie je občanom USA alebo osobou s obdobou trvalého pobytu) a je dôvod sa rozumne domnievať, že sa nenachádza na území USA, vláda nemusí mať ani dôvodné podozrenie (*probable cause*) domnievať sa, že cieľ je agentom zahraničnej moci a nemusí vyžadovať individuálne povolenie od FISC a to aj vtedy, ak sa zásah uskutočňuje v rámci USA. Na oddiele č. 702 je založený vyššie charakterizovaný program PRISM a ďalšie programy v rámci systému UPSTREAM.

Program TEMPORA bol zavedený v rámci oddielu č. 8(4) zákona *Regulation of Investigatory Powers Act*[165] (ďalej len „RIPA") z roku 2000. Podľa dôvodovej správy je účelom tohto zákona zabezpečiť, aby boli relevantné vyšetrovacie právomoci vykonávané v súlade s ľudskými právami.[166] RIPA obsahuje pomerne bohatý systém záruk proti zneužitiu, vrátane ustanovenia špeciálneho tribunálu[167] tzv. „*Investigatory Powers Tribunal*" (ďalej len „IPT"), ktorý má právomoc posudzovať legálnosť výkonu sledovania podľa tohto zákona.

[164] An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.
[165] Celý názov: "An Act to make provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; to provide for Commissioners and a tribunal with functions and jurisdiction in relation to those matters, to entries on and interferences with property or with wireless telegraphy and to the carrying out of their functions by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters; and for connected purposes".
[166] Big Brother Watch et al v. UK (Statement of facts), (App. no. 58170/13), 7 January 2014, s. 4.
[167] RIPA oddiel č. 65.

3.3 Analýza kompatibility programov masívneho sledovania s medzinárodným právom

Táto časť je zameraná na postupné zhodnotenie vyššie predstavených programov podľa štandardov Paktu a Dohovoru. Programy masívneho sledovania budú hodnotené podľa kritérií, ktoré kombinujú podmienky nutné na to, aby bolo daný zásah do súkromia v súlade s Paktom a Dohovorom. Použitá pritom bude judikatúra ESLP a výklad Dohovoru, tak aj výklad Paktu a vyššie spomínaný test prípustnosti obmedzení. Kombinácia spomínaných kritérií je teda nasledovná:

a) Zásah je založený na zákone, ktorý je predvídateľný a obsahuje dostatočné záruky pred zneužitím (legalita).
b) Zásah sleduje legitímny cieľ (legitimita).
c) Zásah je primeraný a nevyhnutný v demokratickej spoločnosti (proporcionalita).

3.3.1 Legalita programov NSA a GCHQ

Prvé kritérium toho, aby bol zásah do práva na súkromie v súlade s medzinárodným právom, je, že musia byť vykonávané na základe vopred schválených zákonov, ktoré sú verejne dostupné, zásah je predvídateľný a samotné zákony sú v súlade s medzinárodnými štandardami ľudských práv. Vyššie popísané programy sledovania majú svoj právny základ v troch ustanoveniach rôznych zákonov – oddiel č. 215 FISA, oddiel č. 702 FAA a oddiel č. 8(4) RIPA.

Ako to konštatoval ESLP v prípade *Malone*: „*právny predpis musí byť dostatočne jasný, aby občanom poskytol primerané informácie o okolnostiach a podmienkach, za ktorých sú štátne orgány oprávnené uchýliť sa k tomuto tajnému a potenciálne nebezpečnému zasahovaniu do práva na rešpektovanie súkromného života a korešpondencie*“[168].

ESLP v prípade *Weber a Saravia* vypracoval minimálne záruky, ktoré by mali byť stanovené v zákonoch, aby sa predišlo zneužitiu právomocí:

a) *povaha činov, ktoré môžu viesť k príkazu na odpočúvanie;*
b) *vymedzenie kategórií osôb, ktoré by mohli byť odpočúvané;*
c) *obmedzenie trvania odpočúvania;*
d) *postup, ktorý sa má dodržiavať pri skúmaní, používaní a uchovávaní získaných údajov;*

[168] ESLP: Malone, op. cit., para. 67.

e) *preventívne opatrenia, ktoré sa majú prijať pri poskytovaní údajov iným stranám;*

f) *okolnosti, za ktorých môžu alebo musia byť záznamy vymazané alebo zničené.*[169]

Aj keď sa prípad *Malone* venoval cielenému odpočúvaniu konkrétnej osoby, v prípade *Liberty* ESLP konštatoval, že neexistujú dôvody na uplatňovanie rôznych zásad týkajúcich sa cieleného odpočúvania a všeobecnejších programov sledovania.[170]

Najprv k oddielu č. 215 zákona FISA. Podstata tohto ustanovenia je, že rozširuje právomoci vďaka ktorým môže FBI prinútiť tretie osoby, aby poskytli pre účely vyšetrovania hmotné veci. Problém ale nastáva v momente, keď sa toto ustanovenie stalo základom pre masívne zbieranie informácií o telefonických hovoroch osôb žijúcich v USA. Tento zber navyše nevykonávala FBI, ale NSA, ktorá má mať na starosti zahraničnú rozviedku. Je zjavné, že takýto program nemá v danom ustanovení právnu oporu. Túto prax kritizuje aj Výbor pre súkromie a občianske slobody[171], keď vo svojej správe upozorňuje na fakt, že oddiel č. 215 neposkytuje primeraný právny základ na podporu takéhoto programu.[172] V prvom rade sa dané ustanovenie vzťahuje len na právomoci FBI a nie NSA. Zároveň sa jedná o hromadný zber dát a nie je teda naplnená podmienka už schváleného a konkrétneho vyšetrovania. A konečne, každodenne sú na základe tohto programu odovzdávané všetky dáta a nie až následne tie, ktoré daná telefonická spoločnosť má vo svojom vlastníctve, čo je podľa Výboru pre súkromie a občianske slobody v rozpore so samotným zákonom FISA.[173] Kritici taktiež často vyčítajú súdom FISA, že svoju funkciu v skutočnosti neplnia, že ide len o inštitúciu, ktorá má vo verejnosti vytvárať dojem, že k zneužitiu moci nemôže dôjsť. Právnik a novinár Glenn Greenwald píše:

> „*Táto inštitúcia je v podstate úplne zbytočná a neposkytuje efektívny dohľad nad zneužívaním odpočúvacích metód, keďže nespĺňa ani tie najmenšie predpoklady, všeobecne považované za základné komponenty transparentného justičného systému. Súd sa stretáva za zatvorenými dverami, vyjadriť sa k*

[169] ESLP: Weber a Saravia, op. cit., para. 95.
[170] ESLP: Liberty et al v. UK (App. no. 58243/00) 1. July 2008, para. 63.
[171] Výbor pre súkromie a občianske slobody je nezávislou agentúrou v rámci vlády Spojených štátov, ktorú zriadil Kongres v roku 2004, aby zabezpečila, že ochrana súkromia a občianskych slobôd je primerane zohľadnená pri vytváraní a implementácii zákonov, nariadení a politík súvisiacich s bojom proti terorizmu.
[172] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court January 23, 2014, s. 10
[173] *Ibid*, s. 10

prípadu má právo len jedna strana, konkrétne vláda, a rozhodnutia súdu sa automaticky zaraďujú do kategórie „prísne tajné“[174]

Ďalší argument kritikov je, že napríklad v roku 2012 FISC schválil všetky podané žiadosti o povolenie elektronického sledovania, pričom z celkového počtu 1788 ich pozmenil (zúžil rozsah) len v 40 prípadoch.[175]

Čo sa týka oddielu č. 702 FAA, toto ustanovenie je taktiež problematické. Jedná sa hlavne o fakt, že zmocňuje osoby z exekutívy, aby vydali povolenie na dlhodobé sledovanie neurčitého počtu osôb, bez následnej účasti súdu.[176] Keď už raz NSA získa povolenie od FISC, ktoré je navyše tajné, môže zahájiť sledovanie kohokoľvek z vlastnej iniciatívy a bez dohľadu súdu.[177] Podobnú prax už v minulosti kritizoval aj Výbor.[178]

Na všeobecné vysvetlenie princípu prečo je v prípadoch zásahu do ľudských práv nutná súdna autorizácia alebo aspoň súdny dohľad dobre slúži judikatúra ESLP v prípadoch *Zakharov*[179] a *Szabó*[180]. V prípade *Zakharov* síce Veľký senát ESLP uznal, že „*povolenie odposluchu mimosúdnym orgánom môže byť v súlade s Dohovorom*“[181], no zároveň dodal, že sa musí jednať o orgán „*schopný posúdiť existenciu dôvodného podozrenia voči dotyčnej osobe, hlavne či existujú skutočné indikácie, že táto osoba plánuje, spácha alebo spáchala trestné činy alebo iné činy, ktoré môžu viesť k použitiu opatrení tajného sledovania, napríklad akty ohrozujúce národnú bezpečnosť*.“[182] Túto argumentáciu následne ESLP v rozhodnutí *Szabó* ešte konkretizoval, keď rozhodol, že „*kontrola nezávislým orgánom, zvyčajne sudcom s osobitnými odbornými znalosťami, by mala byť pravidlom a ostatné riešenia výnimkou, ktorá vyžaduje dôkladnú kontrolu“*[183]. ESLP tak vo svojej judikatúre zdôrazňuje riziko zneužitia tejto právomoci ak by bola výhradne v rukách exekutívy a nepovažuje dohľad výlučne v právomoci ministra spravodlivosti za dostatočný.[184] Aj keď dáta získané na území USA sú už mimo jurisdikcie ESLP, súdna autorizácia zásahu do súkromia je štandardnou súčasťou práva ľudských práv, ako konštatoval

[174] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 143.
[175] *Ibid*, s. 144.
[176] Sinha. G. Alex, op.cit., s. 936.
[177] Liberty and Security in a Changing World: The President's Review Group on Intelligence and Communications Technologies (12 December 2013), s. 136.
[178] Concluding Observations on Lesotho, (1999) UN doc. CCPR/C/79/Add. 106, para. 24.
[179] ESLP: Zakharov v. Rusko (App. no. 47143/06) 4 December 2015.
[180] ESLP: Szabó a Vissy v. Maďarsko (App. no. 37138/14) 12. January 2016.
[181] ESLP: Zakharov, op. cit., para. 258.
[182] *Ibid*, para. 260.
[183] ESLP: Szabó, op. cit., para. 77.
[184] ESLP: Szabó, op. cit., para. 77.

aj Vysoký komisár OSN pre ľudské práva vo svojej správe: „*zapojenie súdov, ktoré spĺňa medzinárodné normy týkajúce sa nezávislosti, nestrannosti a transparentnosti, môže pomôcť zvýšiť pravdepodobnosť, že celkový zákonný režim bude spĺňať minimálne štandardy, ktoré vyžaduje medzinárodné právo v oblasti ľudských práv.*“[185] Správa zároveň dodáva, že existencia dohľadu zo strany súdnej moci ešte nemusí sama o sebe znamenať naplnenie potrebných štandardov, nakoľko dohľad musí byť vykonávaný efektívne. Keďže je absencia neefektívneho súdneho dohľadu v rozpore s medzinárodným právom ľudských práv, podľa argumentu *a minori ad maius* musí byť v rozpore s medzinárodným právom aj absencia akéhokoľvek súdneho dohľadu, ako je to v prípade zahraničného sledovania podľa FAA.

Ďalším problémom je miera špecifikácie cieľa sledovania. Čo sa týka zákona RIPA, podľa oddielu č. 8(4) tohto zákona nie je nutné, aby bol v prípade zachycovania tzv. „externej komunikácie“ (komunikácie mimo britské ostrovy)[186], špecifikovaný presný cieľ sledovania. Vyššie spomínané sledovanie podľa oddielu č. 702 FAA navyše nemusí konkretizovať presný cieľ. Opäť sa teda jedná o prosté zmocnenie tajnej služby vybrať si akýkoľvek cieľ. ESLP sa v prípade *Liberty* zaoberal presne otázkou, či je v súlade s Dohovorom, aby mala exekutíva právomoc požiadať o sledovanie na základe neurčitej zákonnej formulácie návrhu typu „*vonkajšie komunikácie, ako sú popísané v príkaze*“[187]. ESLP dospel k názoru, že v takomto prípade došlo k porušeniu článku 8 Dohovoru, nakoľko nepovažoval zákon za dostatočne jasný na to, aby poskytol primeranú ochranu proti zneužitiu moci.[188]

Posledným problematickým aspektom týchto zákonov je, že pre osobu do ktorej práva bolo zasiahnuté je prakticky nemožné dozvedieť sa, kto každý vlastne jej osobné údaje drží. Výbor sa v GC 16 jasne vyjadril, že zákony musia zaistiť, že „*informácie týkajúce sa osobného života osoby sa nedostanú do rúk osôb, ktoré nie sú oprávnené zákonom takéto informácie prijímať, spracúvať a používať, a nikdy sa nepoužívajú na účely nezlučiteľné s Paktom*“[189]. Spomínané zákony však jasne nedefinujú kto a za akých podmienok môže nakladať s už získanými informáciami. Ako judikoval ESLP, poskytnutie

[185] A/HRC/27/37, op. cit., para. 38.
[186] RIPA, oddiel č. 20.
[187] ESLP: Liberty, op. cit., para. 64.
[188] *Ibid*, para. 64-70.
[189] GC 16, para 10.

takýchto údajov iným orgánom a teda rozšírenie okruhu osôb, ktoré majú k daným údajom prístup, je ďalším, separátnym zásahom do práva sledovanej osoby.[190] Aj vzhľadom na spomínanú prax zdieľania informácií v rámci tajných služieb, sú pochybnosti o skutočnom naplnení tejto podmienky na mieste.

Jedným z ďalších kontroverzných aspektov, konkrétne zákona FAA, je fakt, že vlastne retroaktívne udeľuje imunitu telekomunikačným spoločnostiam, ktoré spolupracujú s NSA a poskytujú im prístup. Podľa zákona FISA by tieto inštitúcie totiž mohli byť cieľom minimálne civilných žalôb. Teoreticky by mohli byť stíhané aj trestne, no ako podotýka Sinha, je nepravdepodobné, že by vláda stíhala telekomunikačné spoločnosti za to, že obchádzali zákon podobne ako vládne inštitúcie samotné.[191] V každom prípade ale takáto retroaktívna imunita vysiela dve dôležité správy. Po prvé, ak nejaká telekomunikačná spoločnosť mala obavy a odmietala spolupracovať práve z dôvodu hroziacich žalôb, už tieto obavy mať nemusí. A za druhé, vláda samotná týmto uznala, že sa jedná prinajmenšom o žalovateľné praktiky.

Podľa môjho názoru teda z vyššie uvedeného vyplýva, že zákony, ktoré sú právnym základom pre sledovacie programy, dostatočne nevyhovujú kritériám legality a sú teda v rozpore s medzinárodným právom.

3.3.2 Legitimita programov NSA a GCHQ

V prípade obhajoby sledovacích programov sa najčastejšie využíva argument národnej bezpečnosti, najmä v súvislosti s bojom proti terorizmu. Boj proti terorizmu je nepochybne legitímny cieľ. Tento cieľ uznáva aj ESLP:

> „*Pre Súd je prirodzeným dôsledkom foriem súčasného terorizmu, že vlády využívajú špičkové technológie na predchádzanie takýmto útokom, vrátane masívneho sledovania komunikácie, u ktorej je náchylnosť na to, že by obsahovala náznaky blížiacich sa incidentov.*“[192]

Zaujímavé na tejto citácii je to, že ESLP sa síce vyjadruje k legitimite „masívneho sledovania komunikácie“, no zároveň nepripúšťa, že je správne sledovať všetku komunikáciu.

[190] ESLP: Weber a Saravia, op. cit., para. 79.
[191] Sinha, G. Alex, op. cit., s. 935.
[192] ESLP: Szabó, op. cit., para. 68.

Formulácia „*komunikácie, u ktorej je náchylnosť na to, že by obsahovala náznaky blížiacich sa incidentov"* jasne vyjadruje požiadavku zúženia rozsahu komunikácie, ktorá je sledovaná, čím sa ESLP dostáva do oblasti cieleného sledovania.

Fakt, že sa aj odborná verejnosť zhoduje na oprávnenosti použitia tajného sledovania za účelom odkrývania teroristických hrozieb, nie je žiadnym prekvapením. Samotný koncept tajných služieb je založený na odhaľovaní potenciálnych bezpečnostných hrozieb zhromažďovaním údajov a informácií takým spôsobom, aby ciele tejto činnosti neboli vopred na monitorovanie upozornení a to prostredníctvom celej škály špeciálnych vyšetrovacích techník, ako je tajné odpočúvanie a monitorovanie (aj elektronickej) komunikácie. Ich opodstatnenie možno vidieť aj v pozitívnej povinnosti štátov prijať preventívne opatrenia na ochranu osôb, ktorých život alebo bezpečnosť sú v potencionálnom ohrození v dôsledku trestnej činnosti.[193]

Metódy sledovania komunikácie sú obzvlášť dôležité pri odkrývaní teroristických hrozieb. Pri tejto forme trestnej činnosti je prevencia častokrát jediná možnosť. Len ťažko očakávať, že štandardné metódy trestného práva ako napríklad sprísnenie trestov ako prostriedku odstrašenia od spáchania trestného činu, bude účinkovať na niekoho kto je v momente páchania trestného činu uzrozumený s vlastnou smrťou.[194]

3.3.3 Proporcionalita programov NSA a GCHQ

Argumentácia bojom proti terorizmu je pochopiteľná a v podstate nesporná, pokiaľ sa jedná o cielené sledovanie osôb podozrivých z teroristických aktivít. Problém ale nastáva pri masívnom sledovaní. Fakt, že má štát na sledovanie legitímny dôvod, ešte neznamená, že rozsah a spôsob zavedenia tohto sledovania je v súlade s medzinárodným právom. Štáty musia pri zásahu do práv osôb dodržiavať zásadu proporcionality: „*Miera a intenzita zásahu musí byť vždy posudzovaná oproti nevyhnutnosti daného opatrenia na dosiahnutie zamýšľaného cieľa a skutočnému prínosu tomuto účelu*"[195]. Tým sa dostávam k otázke, či vyššie spomínané programy masívneho sledovania taktiež vyhovujú kritériu nevyhnutnosti v demokratickej spoločnosti a primeranosti zamýšľanému cieľu.

[193] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, 4 February 2009, A/HRC/10/3, para. 26.
[194] Georgieva, op. cit., s. 123.
[195] A/HRC/27/37, op. cit., para 24.

Martin Scheinin, Zvláštny spravodajca pre ľudské práva v rámci boja proti terorizmu, vo svojej správe uviedol:

> „*Štáty môžu využiť určité preventívne opatrenia, ako je skryté sledovanie alebo odpočúvanie a monitorovanie komunikácie, za predpokladu, že ide o zásahy špecifické pre jednotlivé prípady, na základe príkazu vydaného sudcom po preukázaní legitímneho dôvodu alebo dôvodného podozrenia (probable cause or reasonable grounds); musí existovať nejaký faktický základ súvisiaci so správaním osoby, ktorý odôvodňuje podozrenie, že sa daná osoba môže podieľať na príprave teroristického útoku. Tento preventívny prístup založený na informáciách spravodajských služieb sa snaží skôr predchádzať než obísť súdne konanie a môže byť vhodnou, rozumnou a primeranou metódou na identifikáciu rizík alebo na získanie viac informácií o podozreniach proti podozrivému z terorizmu.*“[196]

ESLP vo svojej judikatúre taktiež uznáva potrebu reagovať na hrozby terorizmu aj sledovaním podozrivých osôb, no zároveň zdôrazňuje, že sa musí jednať o skutočne nutné prípady:

> „*Demokratické spoločnosti sa v súčasnosti ocitli v ohrození vysoko sofistikovanými spôsobmi špionáže a terorizmu, takže štát musí byť schopný v záujme účinného boja proti takýmto hrozbám vykonávať tajné sledovanie podvratných činností pôsobiacich v rámci jeho jurisdikcie. Súd preto musí súhlasiť s tým, že existencia niektorých právnych predpisov, ktorými sa udeľujú právomoci tajného sledovania mailu, pošty a telekomunikácií, je za výnimočných podmienok nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti a / alebo na prevenciu narušenia vereného poriadku alebo trestnej činnosti.*“[197]

Je síce pravda, že aj pri masívnom sledovaní sa v konkrétnom prípade odhalenia teroristickej hrozby bude jednať o primeraný zásah do súkromia potencionálnych páchateľov, vzhľadom na ich trestnú činnosť, no do úvahy je potrebné brať aj vedľajšie škody na právach ostatných, nevinných osôb. Zásah do ich práva by bol proporcionálny len

[196] A/HRC/10/3, op. cit., para. 30.
[197] ESLP: Klass v. Nemecko, (App. no. 5029/71), Series A no. 28, para. 48.

v prípade, že by sa k rovnakému výsledku, nebolo možné dopracovať metódami, ktoré by boli šetrnejšie k ich právam.

3.3.3.1 Sledovanie ako (účinná) zbraň proti terorizmu

Obstojí argumentácia, že je lepšie zhromažďovať čo najviac informácií, pretože je tým väčšia pravdepodobnosť zachytenia potencionálnej hrozby? Štúdie ukazujú, že skôr nie. Samotná „*President Review Group"* prezidenta Obamu pre spravodajské a komunikačné technológie[198] uznala vo svojej správe, že informácie získané použitím telefonických metadát masívne zhromaždených na základe oddielu č. 215, neboli nevyhnutné na predchádzanie teroristickým útokom a mohli byť rovnako získané včasným použitím bežných metód cieleného monitorovania.[199]

Existujú dokonca názory, že masívne sledovanie je kontraproduktívne. Argument je, že zber všetkých informácií v skutočnosti sťažuje efektívnu prácu s informáciami, nakoľko sú tajné služby zahltené zbytočnosťami.[200] Laicky povedané, nájsť ihlu v kope sena je tým ťažšie, čím je kopa sena väčšia.

V prípade teroristických útokov z 11. septembra 2001 sa podľa dostupných informácií nejednalo o problém v nedostatku informácií ale o problém v nedostatočnej schopnosti ich správne vyhodnotiť. Spracovaná správa (ďalej len „správa 9/11")[201] ukazuje, ako sa mesiace pred útokmi vedelo v spravodajskej komunite o možnej hrozbe zo strany Al-Kájdy. Už od jari 2001 sa počet varovaní súvisiacich s možným teroristickým útokom zvyšoval. CIA vydala niekoľko desiatok takýchto varovaní a dokonca padlo podozrenie aj na možný únos lietadla. Federálna letecká správa USA (*Federal Aviation Administration*) upovedomila letecké spoločnosti o tejto hrozbe. Jedna spravodajská správa napríklad varovala, že sa chystá niečo "*veľmi, veľmi, veľmi, veľmi veľké*" a väčšina teroristickej siete Bin Ládina údajne očakávala útok.[202] Aj napriek všetkým týmto indíciám, neboli americké tajné služby schopné zabrániť tomu, čo sa stalo. Dokonca až v 36. prezidentskej

[198] Jej členmi boli okrem iných aj bývalý námestník riaditeľa CIA a poradca Bieleho domu, ktorých preverili preskúmaním prísne tajných dokumentov. Greenwald, op. cit., s. 224.
[199] Liberty and Security in a Changing World: The President's Review Group on Intelligence and Communications Technologies, op.cit., s. 106.
[200] Greenwald, op. cit., s. 226.
[201] Kean, Thomas H, and Lee Hamilton. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004. Celá správa dostupná na odkaze: https://www.9-11commission.gov/report/911Report.pdf
[202] 9/11 Commission Report, op. cit., s. 257.

dennej správne (*Presidential Daily Brief*) z 6. augusta 2001, venujúcej sa hrozbe Bin Ládina, bol spomenutý možný útok na území Spojených štátov:

> *„*[…] *informácie FBI* […] *poukazujú na vzory podozrivých aktivít v tejto krajine naznačujúce prípravu na únosy* (dopravného prostriedku – anglicky „*hijack*“ pozn. aut.) *alebo iné druhy útokov vrátane nedávneho sledovania federálnych budov v New Yorku.“*[203]

Americké tajné služby teda mali všetky dostupné informácie a masívne sledovanie zvyšku obyvateľstva by im v zabránení útokov s najväčšou pravdepodobnosťou nepomohlo. Správa 9/11 taktiež nedošla k záveru, že by problém bol v nedostatku informácií. Osudnou bola práve nedostatočná kooperácia spravodajských služieb a následné podcenenie situácie a neprevedenie niektorých kľúčových opatrení. Správa napríklad uvádza, že niektorí z teroristov priamo zapojených do útokov, boli už spravodajským službám známi členovia Al-Kájdy a aj tak neboli zaradení na tzv. „*watchlist*“. V niekoľkých prípadoch dokonca páchatelia predložili falošné doklady, uviedli odhaliteľne nesprávne údaje (aj voči štátnym orgánom) a pri vstupe na územie Spojených štátov porušili imigračné zákony.[204] Príležitosti k ich zadržaniu teda existovali a žiadna dostupná správa nehovorí o tom, že by sa šance spravodajských služieb zvýšili, keby mali k dispozícii niektorí s programov masívneho sledovania a zberu dát.

3.3.3.2 Priestor pre uváženie a nevyhnutnosť v demokratickej spoločnosti

Ako je popísané v kapitole 1, štáty majú určitý priestor pre uváženie (*margin of appreciation*). Tento priestor však nie je bezbrehý. Jeho hranice sa budú v jednotlivých prípadoch líšiť v závislosti na viacerých faktoroch ako je podstata zásahu, cieľ zásahu, a tak podobne.[205] Výbor v GC č. 31 taktiež argumentuje: „*V žiadnom prípade nesmú byť obmedzenia aplikované alebo vyvolané spôsobom, ktorý by narušil podstatu práva Paktu*“[206].

Aby nebola podstata práva narušená, je nutné správnosť zásahu posudzovať prípad od prípadu.[207] Programy ako získavanie telefónnych záznamov podľa oddielu č. 215,

---

[203] *Ibid*, s. 277.
[204] Kean, Thomas H, and Lee Hamilton. The 9/11 Commission Report Executive Summary. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004, s. 13.
[205] ESLP: Connors v. UK (Application no. 66746/01) 27 May 2004, para. 82.
[206] GC 31, op. cit., para. 6.
[207] GC 16, op. cit., para. 8.

TEMPORA či PRISM, sú však programy, prostredníctvom ktorých získavajú štátne orgány informácie o komunikácií všetkých osôb využívajúcich kyberpriestor pre svoju komunikáciu. Operujú tak na báze zisku informácií „keby niečo“ (*just in case*), čím dochádza k absolútnemu popretiu konceptu posudzovania zásahu prípad od prípadu a k narušeniu samotnej podstaty práva na ochranu súkromia. Ako konštatuje správa Zvláštneho spravodajcu, Bena Emmersona: „*samotná existencia programov masového sledovania predstavuje potenciálne neprimeraný zásah do práva na súkromie*“[208]. Ben Emmerson dokonca prirovnáva takýto zásah k úplnej derogácii práva na ochranu digitálnej komunikácie.[209]

K naplneniu princípu proporcionality neodmysliteľne patrí aj už vyššie spomínané fungovanie efektívneho dohľadu nezávislou autoritou a existencia tzv. „obmedzení využitia“ (*use limitations*). Obmedzenia využitia predstavujú určité limity určujúce kto má k už získaným informáciám prístup a komu ich môže poskytnúť. Podstata spočíva v tom, že aj keď je zásah do súkromia proporcionálny pre naplnenie určitého účelu, už nemusí byť proporcionálny pre účel iný. Aj v súvislosti s vyššie spomínanou praxou zdieľania spravodajských informácií je na mieste pochybovať o naplnení tejto podmienky.

3.3.4 Judikatúra

K problematike legitimity elektronického sledovania existuje judikatúra najmä na regionálnej úrovni ochrany ľudských práv. Jedná sa hlavne o už citované prípady ESLP ako *Klass*, *Liberty*, *Weber*, *Zakharov* a *Szabó*. V týchto prípadoch sa ale nejednalo o reakciu na vyššie spomínané programy NSA a GCHQ.

V Spojených štátoch však v rozhodnutí *American Civil Liberties Union v. Clapper*[210], z roku 2015, súd na národnej úrovni konštatoval, že program na masívne zbieranie telefónnych metadát podľa oddielu č. 215 bol nezákonný a že princípy nevyhnutnosti a proporcionality vyžadujú, aby boli zachytené údaje relevantné pre konkrétne vyšetrovanie a nie len pre boj proti terorizmu vo všeobecnosti.

Čo sa týka ESLP, všetci napäto očakávajú rozhodnutie v prípade *Big Brother Watch*, ktorý je priamou reakciou na Snowdenové odhalenia programov. Sťažovateľmi

[208] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, 23 September 2014, A/69/397, para. 18
[209] A/69/397, op. cit., para. 18.
[210] United States Court of Appeals for the Second Circuit, August Term, 2014 (Argued: September 2, 2014 Decided: May 7, 2015) American Civil Liberties Union, American Civil Liberties Foundation.

sú tri mimovládne organizácie sídliace v Londýne a jedna fyzická osoba, nemecká akademička a expertka na techniky sledovania. Sťažovatelia namietajú, že boli cieľom sledovania zo strany tajných služieb, najmä britskej GCHQ, vzhľadom na náplň ich práce a nakoľko často používajú na vzájomnú komunikáciu e-mail alebo Skype. Poukazujú pritom na programy PRISM, UPSTREAM a TEMPORA a argumentujú, že prístup k ich komunikácií mohla mať ako GCHQ, tak aj NSA, práve prostredníctvom zdieľania získaných informácií medzi týmito agentúrami.[211]

Namietajú, že zásah do ich súkromia nie je ani v súlade so zákonom, konkrétne zákonom RIPA, nakoľko podľa nich tento zákon nevyhovuje potrebným štandardom stanoveným v judikatúre ESLP. Ďalej namietajú, že v britskom národnom práve neexistuje právny základ pre také zdieľanie informácií, aké praktizuje GCHQ, čím dochádza k porušeniu článku 8 Dohovoru. Na záver dodávajú, že masívne sledovanie zahraničnej komunikácie je taktiež v rozpore s článkom 8 Dohovoru a ide podľa nich o neprimeraný zásah do súkromia miliónov ľudí. V momente odovzdávania tejto práce je prípad stále prejednávaný.

3.3.5 Zhrnutie

Ako z tejto kapitoly vyplynulo, programy NSA a GCHQ vykazujú závažné právne nedostatky a predstavujú tak neprimeraný zásah do práva na ochranu súkromia. Už samotný právny základ týchto programov je pochybný a neposkytuje dostatočné záruky pred zneužitím. Navyše je na mieste pochybovať aj o ich reálnej efektivite v boji proti terorizmu. Aj keď boj proti terorizmu je rozhodne legitímny cieľ na zásah do súkromia osôb, prostriedky, ktoré tieto programy používajú, podľa môjho názoru nevyhovujú kritériám proporcionality a zlyhávajú tak v tomto teste. Bolo by preto žiadúce ich zmeniť alebo vytvoriť nové zákony, ktoré by zavádzali transparentnejší a zároveň efektívnejší systém elektronického sledovania, ktorý by spĺňal svoj účel a zároveň neprimerane nezasahoval do práv iných.

Prameňom pre takúto normotvorbu by mohol byť dokument „Princípy aplikácie ľudských práv na sledovanie komunikácie“[212] (*Principles on the Application of Human Rights to Communications Surveillance)* ktorý vymedzuje základné princípy, ktoré by

[211] ESLP: Big Brother Watch et al v. UK (Statement of facts), (App. no. 58170/13), 7 January 2014.
[212] International Principles on the Application of Human Rights to Communications Surveillance (also called the Necessary and Proportionate Principles) (May 2014), Celý dokument prístupný na adrese: https://www.eff.org/files/necessaryandproportionatefinal.pdf

mali byť dodržané pri elektronickom sledovaní, aby nedošlo k rozporu s medzinárodným právom. Jedná sa o všeobecne uznávaný dokument, citovaný ako Vysokým komisárom OSN, tak aj v správe „*President Review Group*“ prezidenta Obamu pre spravodajské a komunikačné technológie.

Samotné princípy sa v mnohom podobajú už existujúcim zásadám vyjadrených v judikatúre. Pre úplnosť ich uvediem všetky so stručnou charakteristikou:

1. Legalita – vyjadruje už v tejto práci analyzovaný princíp, že každý zásah musí mať svoj právny základ, ktorý je prístupný verejnosti.
2. Legitímny cieľ – taktiež už rozoberaný princíp legitímneho cieľa pričom žiadne opatrenie nesmie byť diskriminačné.
3. Nevyhnutnosť – cieľ musí byť nevyhnutný v demokratickej spoločnosti.
4. Primeranosť – opatrenia musia byť primerané cieľu.
5. Proporcionalita – rozhodnutiam o sledovaní by malo predchádzať dôkladné uváženie možného úžitku oproti škode, ktorá bude sledovaním spôsobená jednotlivcovi.
6. Kvalifikovaná súdna autorita – o povolení by mala rozhodovať nezávislá a nestranná súdna autorita, ktorá nie je akoukoľvek súčasťou inštitúcií vykonávajúcich sledovanie.
7. Spravodlivý proces – každý by mal mať pri zásahu do jeho práva na súkromie možnosť na následné spravodlivé a verejné vypočutie v primeranej dobe.
8. Oznámenie – osobám podliehajúcim sledovaniu by malo byť takéto rozhodnutie oznámené aby mali možnosť právne sa brániť (samozrejme tento princíp zahrňuje výnimku v prípadoch, kedy by oznámenie danej osobe zmarilo účel, pre ktorý bolo rozhodnuté o sledovaní).
9. Transparentnosť – štáty by pri naplnení tohto princípu mali udržiavať istú formu transparentnosti pri vykonávaní elektronického sledovania, napríklad pravidelne informovať verejnosť o počte vykonaných sledovaní.
10. Dohľad verejnosti – verejnosť by mala mať možnosť prostredníctvom nezávislých mechanizmov vykonávať dohľad nad orgánmi vykonávajúcimi elektronické sledovanie, aby zabezpečili, že táto moc nie je zneužívaná.

11. Integrita komunikácií a systémov – štáty by nikdy nemali robiť nátlak na poskytovateľov elektronických služieb aby do svojich produktov zabudovávali prostriedky, ktoré by šlo neskôr využiť na sledovanie užívateľov.
12. Opatrenia pre medzinárodnú spoluprácu – medzinárodné dohody o zdieľaní získaných informácií by mali rešpektovať rovnaké bezpečnostné štandardy ľudských práv na oboch stranách a štáty by nemali tieto dohody využívať na to, aby obišli vlastné zákony.
13. Opatrenia proti nezákonnému prístupu – štáty by mali prijať dostatočné opatrenia vo vlastnej legislatíve aby predišli elektronickému sledovaniu vykonávanému inými osobami.

Tento dokument taktiež uznáva extrateritoriálne záväzky štátov pri ochrane ľudských práv, keď v preambule uvádza: *„Tieto princípy sa vzťahujú rovnako na sledovanie vlastných štátnych príslušníkov vykonávanom na vlastnom území, ako aj na sledovanie ostatných mimo svojho územia.“*[213] Som toho názoru, že zavedenie týchto princípov do zákonov a ich dodržovanie by zabezpečilo to, aby aj taký zásah do súkromia, akým je elektronické sledovanie komunikácie, vyhovoval štandardom medzinárodného práva.

[213] *Ibid*.

4. Špionáž orgánov iného štátu

Pri rozbore vyššie uvedených programov by nebolo správne nespomenúť aj ich druhý účel – špionáž orgánov iných štátov. Jedná sa o sledovanie komunikácie najvyšších predstaviteľov štátu, štátnych úradníkov a diplomatov. Primárne sa už ale nejedná o otázku zásahu do ľudských práv, ale o zásah do suverenity štátu a kompatibilitu takéhoto jednania so základnými pravidlami medzinárodného práva tak, ako ich popisuje Charta Organizácie Spojených národov (ďalej len „Charta"). Ide hlavne o prípady hospodárskej a diplomatickej špionáže.

Hospodárskou špionážou myslím využívanie štátnej sledovacej techniky za účelom sledovania štátnych orgánov ako sú napríklad ministerstvá financií, obchodu a energeticky iných štátov alebo významné súkromné spoločnosti so sídlom v zahraničí, za účelom dosiahnutia zisku. Rozsah tejto špionáže dobre demonštrujú dokumenty odhalené Snowdenom. Jeden dokument napríklad medzi ciele sledovania NSA a GCHQ uvádza brazílsku ropnú spoločnosť Petrobras, ruskú ropnú spoločnosť Gazprom a aerolínie Aeroflot.[214] Fakt, že program BLARNEY nie je určený len na poskytovanie informácií súvisiacich s teroristickými hrozbami je jasný z popisu tohto programu samotnou NSA v jednom z uniknutých dokumentov. NSA uvádza, že program BLARNEY poskytuje svojim zákazníkom[215] aj diplomatické a hospodárske informácie.[216]

Čo sa týka diplomatickej špionáže, asi najmedializovanejším prípadom v Európe bolo odpočúvanie mobilu nemeckej kancelárky Angely Merkelovej.[217] NSA takto údajne monitorovala aj brazílsku prezidentku Dilmu Rousseffovú[218] alebo mexického prezidenta Enriqueho Penu Nieta.[219] Sledovacie metódy NSA sa ale neobmedzili len na predstaviteľov štátov. Terčom boli aj predstavitelia medzinárodných organizácií ako je OSN alebo EU.[220] Jedno hlásenie napríklad dôkladne popisuje, ako BLARNEY poskytoval informá-

[214] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 151.
[215] Pojmom „zákazník" sú myslené inštitúcie ako Biely dom, CIA, DIA atď.
[216] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 152.
[217] Council of Europe Parliamentary Assembly, Report on Mass Surveillance, 18 March 2015, Doc. 13734, s. 15.
[218] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 156.
[219] *Ibid*.
[220] Poitras, L., Rosenbach, M., and Stark, H., 'Codename 'Apalachee': How America Spies on Europe and the UN' Der Spiegel (26 August 2013) <http://www.spiegel.de/international/world/secret-nsa-documents-showhow- the-us-spies-on-europe-and-the-un-a-918625.html>

cie o postoji ostatných členov Bezpečnostnej rady OSN pred hlasovaním o uvalení sankcií na Irán.[221] V roku 2003, keď USA a UK chceli v Bezpečnostnej rade OSN presadiť odsúhlasenie invázie do Iraku, unikla na verejnosť komunikácia medzi NSA a GCHQ, popisujúca plány na odpočúvanie pracovných aj domácich telefónov a emailov všetkých zástupcov zvyšných 13 členov Rady bezpečnosti, čim mali USA a UK získať výhodu pri rokovaniach.[222] Sledovaniu sa údajne nevyhli ani organizácie ako UNICEF, Lekári bez hraníc alebo dokonca pápež.[223] Takýto rozsah a výber cieľov sledovania je len ťažko odôvodniteľný bojom proti terorizmu.

4.1 Čo na to medzinárodné právo?

Špionáž ako taká nie je medzinárodným právom upravená, s čiastočnou výnimkou vojnovej špionáže. Logickým odôvodnením toho je, že každý štát určitú formu špionáže vykonáva. To má za následok, že aj keď špionáž nikto nechce uznať otvorene ako samozrejmosť, nikto ju nechce ani absolútne zakázať. Je teda špionáž súčasťou medzinárodného obyčajového práva? K tomu, aby vznikol obyčaj ako prameň medzinárodného práva, je nutné, aby dané jednanie kumulatívne spĺňalo materiálny prvok ustálenej praxe (*usus longaevus*) a subjektívny prvok presvedčenia subjektov o právnej záväznosti danej praxe (*opinio iuris*).[224] Z toho vyplýva, že to, že všetky štáty vykonávajú špionáž, ešte neznamená, že je to súčasťou medzinárodného obyčajového práva, nakoľko v tomto prípade chýba *opinio iuris*.[225]

Určitá úprava naznačujúca zákaz špionáže ale existuje, aj keď sa netýka priamo špionáže elektronickej. Napríklad v článku 19 Dohovoru o morskom práve[226], venujúcemu sa pokojnému prechodu sa píše:

> „*Prechod cudzej lode je považovaný za ohrozenie mieru, verejného poriadku alebo bezpečnosti pobrežného štátu, ak vykonáva v pobrežnom mori niektorú z týchto činností:*

[221] Greenwald, Glenn, Nikto sa neskryje, op. cit., s. 160.
[222] Bright, Martin, Vulliamy, Ed and Beaumont, Peter. Revealed: U.S. Dirty Tricks to Win Vote on Iraq War, The Guardian, Mar. 2, 2003
[223] Buchan Russell, Cyber espionage and international law. In Tsagourias, Nicholas, Buchan, Russell (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Pub, 2015, s. 169
[224] Malenovský, Jiří. *Mezinárodní právo veřejné: jeho obecná část a poměr k jiným právním systémům, zvláště k právu českému*. 5., podstatně upr. a dopl. vyd. Brno: Masarykova univerzita, 2008. s. 188-191.
[225] Buchan Russell, op. cit., s. 185.
[226] Dohovor Organizácie Spojených národov o morskom práve (UNCLOS), Montego Bay 10 december 1982, 16 november 1994 [1833 UNTS 3 / [1994] ATS 31 / 21 ILM 1261 (1982)]

[…]

(c) akúkoľvek činnosť zameranú na zhromažďovanie informácii na ujmu obrany alebo bezpečnosti pobrežného štátu

[…]"

Ďalším príkladom je Viedenský dohovor o diplomatických stykoch[227], ktorý ukladá všetkým osobám požívajúcim výsady a imunity podľa tohto dohovoru povinnosť dbať na zákony a predpisy prijímajúceho štátu, pričom sú povinné nevmiešavať sa do vnútorných záležitostí tohto štátu.[228]

Ak medzinárodné právo nedovoľuje utajené sledovanie z lode v teritoriálnych vodách, z lietadla alebo prostredníctvom diplomatickej misie, prečo by malo dovoľovať sledovanie v rámci kyberpriestoru? Jedným z argumentov je, že všetky vyššie zmienené praktiky sledovania majú svoj teritoriálny prvok, zatiaľ čo kyberpriestor nemá jasne vyznačené hranice a neexistuje niečo ako „nemecký kyberpriestor" alebo „americký kyberpriestor".

Otázkou ale ostáva, či tajné sledovanie predstaviteľov iných štátov aj tak neporušuje zásady medzinárodného práva ako je napríklad zásada nezasahovania do vnútorných záležitostí iného štátu.

4.2 Kybernetická špionáž ako zásah do suverenity?

Jedna zo základných zásad medzinárodného práva, vyjadrená v článku 2(1) Charty OSN, je zásada zvrchovanej rovnosti štátov. S tým sa spája zásada nezasahovania do vnútorných záležitostí iných štátov, ako to v prípade *Nicaragua* formuloval MSD: „*Zásada nezasahovania zahŕňa právo každého zvrchovaného štátu, vykonávať svoje záležitosti bez vonkajšieho zasahovania*"[229]. Aj keď zásada nezasahovania nie je explicitne vyjadrená v Charte, je považovaná za súčasť medzinárodného obyčajového práva.[230] Prvok „nátlaku" (*coercion)* potom predstavuje samotnú podstatu zakázaného zásahu do zvrchovanosti iného štátu.[231] Niektorí argumentujú, že samotné sledovanie a zber informácií nemôže porušovať zásadu nezasahovania, nakoľko práve element nátlaku chýba. Štát,

[227] Viedenský dohovor o diplomatických stykoch, Viedeň, 18 April 1961, 500 UNTS 95 (účinnosť 24. apríl 1964)
[228] *Ibid*. čl. 41(1)
[229] MSD: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, para. 202.
[230] MSD: Nicaragua v. USA, op. cit., para. 202.
[231] *Ibid*, para. 205.

ktorý je sledovaný, častokrát ani netuší, že je cieľom. To má za následok, že na neho nie je v dôsledku tejto činnosti vyvíjaný akýkoľvek nátlak.[232] MSD síce uznáva, že prvok nátlaku je „*obzvlášť zjavný v prípade intervencie, ktorá využíva silu buď v priamej podobe vojenskej akcie, alebo v nepriamej forme podpory podvratných alebo teroristických ozbrojených aktivít v rámci iného štátu*“[233], no to neznamená, že sa zásada nezasahovania aplikuje len na prípady vojenskej intervencie. MSD ďalej argumentuje:

> „*Zakázaný zásah musí mať vplyv na záležitosti, v ktorých má každý štát dovolené, v dôsledku zásady suverenity štátov, sa rozhodnúť slobodne. Jednou z nich je voľba politického, hospodárskeho, sociálneho a kultúrneho systému a formulácia zahraničnej politiky.*“[234]

Fakt, že „*štátna zvrchovanosť a medzinárodné normy a princípy, ktoré vyplývajú zo suverenity, sa vzťahujú na jednanie štátov ohľadom činností súvisiacich s informačno-komunikačnými technológiami a na ich jurisdikciu nad touto infraštruktúrou na ich území*“[235] je dnes už takmer nesporný. V správe Skupiny vládnych expertov na vývoj v oblasti informácií a telekomunikácií v kontexte medzinárodnej bezpečnosti, popísanej v kapitole 2, je medzi kľúčové princípy pri aplikácii medzinárodného práva na informačno-komunikačné technológie výslovne zaradený aj princíp „nezasahovania do vnútorných záležitostí iných štátov“[236].

V prípade elektronickej špionáže sa teda síce nejedná o fyzický zásah do územia štátu, no ak štát vykonáva zvrchovanosť nad informáciami a dátami nachádzajúcimi sa v kyberpriestore, tajné sledovanie alebo zber takýchto dát inou mocou by sa, podľa môjho názoru, malo považovať za zasahovanie do jeho zvrchovanosti. Zložitosť tejto problematiky otvára priestor pre ďalšie skúmanie.

[232] Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013, s. 433.
[233] MSD: Nicaragua v. USA, op. cit., para. 205.
[234] *Ibid*, para 205.
[235] UN GA, A/70/174, op. cit., para. 27.
[236] *Ibid*, para. 26(e).

Záver

„Oveľa radšej sa budem zodpovedať za masívne sledovanie, ako sa snažiť vysvetľovať, prečo sme nedokázali zabrániť ďalšiemu 11. septembru.“

Takýmito slovami začal generál Keith Alexander, bývalý riaditeľ NSA, svoje vystúpenie pred vyšetrovacou komisiou amerického kongresu.

V prvej otázke, ktorú som si v úvode položil pre túto prácu, týkajúcej sa aplikovateľnosti medzinárodnoprávnych dokumentov v kontexte elektronického sledovania, som dospel k názoru, vychádzajúc aj z argumentov uvedených v druhej kapitole, že by jednoznačne aplikovateľné v tomto kontexte mali byť.

Druhá otázka, či je vôbec niekedy prípustné masívne sledovanie, je už náročnejšia. Myslím si, že masívne elektronické sledovanie je tak obrovský zásah do samotnej podstaty práva na súkromie, že asi neexistuje situácia, v ktorej by takéto opatrenie mohlo byť legitímne. Som ochotný pripustiť, že môžu nastať určité okolnosti, kedy bude treba právo na súkromie dočasne významnejšie obmedziť pre účely bezpečnosti obyvateľstva, no svojvoľné masívne sledovanie všetkých osôb predstavuje absolútnu derogáciu tohto práva. Od autoritárskych režimov, ktoré sa neštítia svojvoľných zásahov do ľudských práv, nás predsa odlišuje práve systém ochrany ľudských práv, ktorý nastavuje určité neprekročiteľné mantinely pre štát samotný. Podstata tohto systému je práve v tom, že máme určité práva, ktoré obmedziť za žiadnych okolností nemožno a zároveň máme práva, ktoré je možné obmedziť len za predpokladu, že sú dodržané pravidlá, ktoré sme si určili. Masívne sledovanie obyvateľstva teda podľa môjho názoru nie je v súlade s medzinárodným právom a neviem si predstaviť situáciu, kedy by to prípustné za súčasného štandardu ochrany ľudských práv bolo.

Nepochybujem ale o tom, že pre potreby národnej bezpečnosti, či už sa jedná o boj proti terorizmu, boj proti organizovanému zločinu alebo o odvracanie iných vážnych hrozieb, je istá forma elektronického sledovania potrebná. Je vysoká pravdepodobnosť, že teroristi budú komunikovať a regrutovať nových členov do svojich radov hlavne prostredníctvom internetu a iných digitálnych technológií. Organizovaný zločin dnes tiež svoju činnosť neobmedzuje na hranice jedného štátu, práve naopak, menšiu efektivitu cezhraničnej spolupráce, či už tajných služieb, alebo polície, využíva vo svoj prospech. Ak je sledovanie, aj zahraničné, vykonávané efektívne a so súhlasom a pomocou druhého

štátu, tak sa jedná o veľmi účinnú metódu boja proti zločinu a rozhodne nezastávam názor, že by do určitej miery nebol legitímny.

Je preto nutné nájsť rovnováhu medzi intenzitou zásahu do súkromia osôb za účelom ich ochrany a úrovňou rešpektovania a ochrany ich práva na súkromie. K tomu, aby to bolo možné, je podľa môjho názoru nutné zmeniť a doplniť niektoré kľúčové aspekty ochrany súkromia, zvlášť princípov pre jeho obmedzenie. Za dobrý príklad takýchto princípov považujem vyššie spomínaný dokument „Princípy aplikácie ľudských práv na sledovanie komunikácie", ktorý prináša prehľadný, stručný a zrozumiteľný súhrn najdôležitejších štandardov, ktoré by mali štáty pri monitorovaní komunikácie dodržiavať.

Uvedomujem si, že zavedenie takýchto princípov a ich všeobecné dodržiavanie je z pohľadu medzinárodného práva beh na dlhu trať, no značne by k tomu mohla prispieť napríklad reforma Všeobecného komentára (GC) č. 16 k článku 17 Paktu, ktorý už nevyhovuje dnešným podmienkam. Krokom vpred by taktiež bolo, keby ESLP v prípade *Big Brother Watch* rozhodol v prospech navrhovateľov. Čo sa týka budúcnosti samotného oddielu č. 702 FAA, na konci roku 2017 končí jeho platnosť a momentálne nie je jasné, či bude predĺžená. Posledné správy z Bieleho Domu naznačujú skôr to, že administratíva prezidenta Donalda J. Trumpa nemá v úmysle podporiť akékoľvek reformy k oddielu č. 702. Dan Coats, americký senátor a nominant prezidenta Trumpa na pozíciu šéfa tajných služieb (*Director of National Intelligence*), sa vyjadril, že oddiel č. 702 patrí medzi „kráľovské klenoty" (*crown jewels*) tajnej služby.[237] Definitívne rozhodnutie však k dátumu odovzdania tejto práce nepadlo. Ostáva len dúfať, že systém bude prinajmenšom zreformovaný a to takým spôsobom, aby neumožňoval ďalšie zneužitie zo strany tajných služieb.

Nakoľko sú teda slová generála K. Alexandra opodstatnené? Myslím si, že by namiesto získavania miliónov zbytočných informácií, bolo efektívnejšie bojovať proti terorizmu zdokonaľovaním už existujúcich metód cieleného sledovania a to najmä v oblasti vyhodnocovania hrozieb a lepšej kooperácie jednotlivých agentúr medzi sebou. Rešpektovanie ľudských práv neodmysliteľne patrí k našej modernej a demokratickej spoločnosti a nemyslím si, že by sme sa tohto výdobytku mali vzdať na úkor falošného pocitu bezpečnosti.

---

[237] http://www.reuters.com/article/us-usa-trump-fisa/white-house-supports-renewal-of-spy-law-without-reforms-official-idUSKBN16855P

Zoznam skratiek

MSD	Medzinárodný súdny dvor
ESLP	Európsky súd pre ľudské práva
Výbor	Výbor pre ľudské práva
Charta	Charta Organizácie Spojených národov
Dohovor	Európsky Dohovor o ochrane ľudských práv a základných slobôd
Pakt	Medzinárodný pakt o občianskych a politických právach
Deklarácia	Všeobecná deklarácia ľudských práv
GC	Všeobecné stanovisko Výboru (*General Comment*)
VDZP	Viedenský dohovor o zmluvnom práve
OSN	Organizácia Spojených národov
NATO	Organizácia Severoatlantickej zmluvy
NSA	Národná bezpečnostná agentúra
GCHQ	Vládne komunikačné ústredie
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FAA	FISA Amendments Act
RIPA	Regulation of Investigatory Powers Act
IPT	Investigatory Powers Tribunal
správa 9/11	The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States

Zoznam literatúry

Medzinárodné zmluvy

- Americký dohovor o ľudských právach, 22. november 1969, OAS Treaty Series No. 36, (účinnosť 18. júl 1978)
- British U.S. Communication Intelligence Agreement (5 March 1946)
- Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907
- Dohovor Organizácie Spojených národov o morskom práve (UNCLOS), Montego Bay 10 december 1982, 16 november 1994 [1833 UNTS 3 / [1994] ATS 31 / 21 ILM 1261 (1982)]
- Európsky Dohovor o ochrane ľudských práv a základných slobôd, 4. november 1950, ETS No. 5, (účinnosť 3. september 1953)
- Medzinárodný pakt o občianskych a politických právach, 16. december 1966, 999 UNTS 171 (účinnosť 23. marec 1976)
- UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4
- Dohovor o zabránení a trestaní zločinu genocídia., 9. december 1948, UNTS, vol. 78, p. 277
- Viedenský dohovor o zmluvnom práve, 23 máj 1969, UNTS, vol. 1155 (účinnosť
- Viedenský dohovor o diplomatických stykoch, 18. apríl 1961, 500 UNTS 95 (účinnosť 24. apríl 1964)
- Všeobecná deklarácia ľudských práv, 10 december 1948, 217 A (III)

Medzinárodné dokumenty

- Council of Europe Parliamentary Assembly, Report on Mass Surveillance, 18 March 2015, Doc. 13734
- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, 23 September 2014, A/69/397

- Summary Record of the Hundred and Thirty-Eighth Meeting, U.N. ESCOR Hum. Rts. Comm., 6th Sess., 138th mtg at 10, para 34, U.N. Doc. E/CN.4/SR.138 (1950)
- The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37
- UN GA, A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015.
- UN GA Resolution. 68/167, "The right to privacy in the digital age," U.N. Doc. A/RES/68/167 (Jan. 21, 2014)
- UN General Assembly, Res. 40/144, 13 December 1985, UN Doc. A/RES/40/144
- UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 28 December 2009, A/HRC/13/37
- UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, 4 February 2009, A/HRC/10/3
- UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40

Judikatúra a iné rozhodnutia

Medzinárodný súdny dvor:

- Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, International Court of Justice (ICJ), 9 July 2004
- Corfu Chanel Case (UK v Albania) (Separate Opinion of Judge Alvarez) [1949] ICJ Rep 43.
- Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)
- Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, Advisory Opinion, ICJ Reports 1951, 15

Európsky súd pre ľudské práva:

- Al-Skeini et al v. UK, (App no 55721/07) 7 July 2011
- Banković et al v. Belgium et al, (App. no. 52207/99) 12 December 2001
- Big Brother Watch et al v. UK (Statement of facts), (App. no. 58170/13), 7 January 2014
- Campbell v. UK, (App. no. 13590/88), Series A no. 233
- Connors v. UK (Application no. 66746/01) 27 May 2004
- Costello-Roberts v. UK (App. no. 13134/87), 19 EHRR 112
- Dubská a Krejzová v. Czech Republic (App. no. 28859/11 and 28473/12)
- Gillan and Quinton v. UK, (App. no. 4158/05)
- Jaloud v. the Netherlands (Application no. 47708/08) 20 November 2014
- Khan v. UK, (App. no. 35394/97)
- Klass and Others v. Germany, (App. no. 5029/71) Series A no. 28
- Liberty et al v. UK (App. no. 58243/00) 1. July 2008
- Loizidou v. Turkey (App no. 15318/89) (ECtHR (GC), 23 March 1995)
- Malone (James) v. UK, Judgment (Merits), (App no. 8691/79) (A/82), [1984] ECHR 10, (1984) 7 EHRR 14, IHRL 47 (ECHR 1984)
- Niemietz v Germany, Merits and Just Satisfaction, (App no. 13710/88), A/251-B, [1992] ECHR 80, (1993) 16 EHRR 97, IHRL 2979 (ECHR 1992), 16th December 1992
- Pad et al. v. Turkey (App no. 60167/00) 28 June 2007
- S. and Marper v. UK, (App. no. 30562/04 and 30566/04), 4 December 2008
- Silver and Others judgment, (App. no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75), Series A no. 61, judgment of 25 March 1983 813
- Soering v. UK (App. No. 14038/88) 7 July 1989
- Szabó and Vissy v. Hungary (App. no. 37138/14) 12. January 2016
- Von Hannover v. Germany, (App. no. 59320/00), ECHR 2004-VI.
- Weber and Saravia v. Germany (App no. 54934/00), ECHR 2006-XI.
- X and Y v. Netherlands, Judgment (Merits and Just Satisfaction), Case No 16/1983/72/110, App. no. 8978/80 (A/91), [1985] ECHR 4, (1986) 8 EHRR 235, IHRL 51 (ECHR 1985), 26th March 1985

- Zakharov v. Russia (App. no. 47143/06) 4 December 2015

Inter-americký súd pre ľudské práva:

- The Effect of Reservations on the Entry Into Force of the American Convention on Human Rights (Arts. 74 and 75), Advisory Opinion OC-2/82, September 24, 1982, Inter-Am. Ct. H.R. (Ser. A) No. 2 (1982)

Výbor pre ľudské práva:

- Coeriel et al. v. The Netherlands, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994)
- Concluding Observations on Lesotho, (1999) UN doc. CCPR/C/79/Add. 106
- Lopez Burgos v. Uruguay, Communication No. R.12/52, Supp. No. 40, 176, UN Doc. A/36/40 (1981)
- Rafael Armando Rojas García v. Kolumbia, Communication No. 687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).
- Toonen v. Austrália, Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994).
- UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988
- UN Human Rights Committee (HRC), CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency, 31 August 2001
- UN Human Rights Committee (HRC), General comment No. 33, Obligations of States parties under the Optional Protocol to the International Covenant on Civil and Political Rights, 25 June 2009
- UN Human Rights Committee (HRC), General Comment No. 24 (52), General comment on issues relating to reservations made upon ratification or accession to the Covenant or the Optional Protocols thereto, or in relation to declarations under article 41 of the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.6 (1994)
- UN Human Rights Committee (HRC) General Comment No. 31, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (26 May 2004)

Vnútroštátna judikatúra:

- United States Court of Appeals for the Second Circuit, August Term, 2014 (Argued: September 2, 2014 Decided: May 7, 2015) American Civil Liberties Union, American Civil Liberties Foundation.

Vnútroštátne zákony

- An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.
- An Act to authorize electronic surveillance to obtain foreign intelligence information, October 25, 1978.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

Knihy

- Čepelka, Č., Šturma, P., Mezinárodní právo veřejné. Praha: Beck, 2008
- Da Costa, Karen. The Extraterritorial Application of Selected Human Rights Treaties. Leiden; Boston, Martinus Nijhoff Publishers, 2013
- Evropská úmluva o lidských právech: komentář. Praha: C.H. Beck, 2012
- Goodman, Marc. „Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It.“First edition, Doubleday, 2015.
- Johnson, R. David, and Post, G. David, Law and borders: The rise of law in cyberspace, 48 Stanford L Rev 1367, 1996. Contra Goldsmith, L. Jack, 'Against cyberanarchy', 65 U Chi L Rev 1199, 1998.
- Kälin, W., & Künzli, J. The law of international human rights protection. Oxford: Oxford University Press., 2009.
- Lord Lester and D. Pannick (eds.). Human Rights Law and Practice. London, Butterworth, 2004
- Malenovský, Jiří. Mezinárodní právo veřejné: jeho obecná část a poměr k jiným právním systémům, zvláště k právu českému. 5., podstatně upr. a dopl. vyd. Brno: Masarykova univerzita, 2008.
- Nowak, Manfred. U. N. Covenant on Civil and Political Rights : CCPR Commentary. Kehl [Etc.], Engel, 1993

- Potočný, Miroslav a Jan Ondřej. Mezinárodní právo veřejné: zvláštní část. 6., doplněné a rozšířené vydání. Praha: C.H. Beck, 2011
- Rule, James. Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience, OUP, 2009
- Savin, Andrej, and Edward Elgar Publishing. EU Internet Law. Northampton, Mass., E. Elgar, 2013
- Tsagourias, Nicholas, and Buchan, Russell, Research Handbook on International Law and Cyberspace. Edward Elgar M.U.A., 2015
- Ziolkowski, Katharina (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013
- Zureik, E., Stalker, L., & Smith, E. Surveillance, Privacy, and the Globalization of Personal Information International Comparisons. Montreal: McGill-Queen's University Press, 2014

Články

- ACLU of Northern California, Location-Based Services: Time for a Privacy Check-In 5, http://aclunc-tech.org/files/lbs-privacy-checkin.pdf
- Buchan Russell, Cyber espionage and international law. In Tsagourias, Nicholas, Buchan, Russell (eds.). *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Pub, 2015
- Carolyn Y. Johnson, Project 'Gaydar', BOSTON.COM, Sep. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/
- Cohen, Julie E. "What Privacy Is for.(Privacy Self-Management and the Consent Dilemma)." *Harvard Law Review*, vol. 126, no. 7, 2013, pp. 1904–1933
- Conley, Chris, Metadata: Piecing together a privacy solution, ACLU of Northern California, Inkworks Press, 2014
- Deeks, Ashley S. "An International Legal Framework for Surveillance." *Virginia Journal of International Law* 55.2, 2015, 291-368
- De Montjoye, Yves-alexandre, et al. "Unique in the Crowd: The Privacy Bounds of Human Mobility." *Scientific Reports* (Nature Publisher Group), vol. 3, 2013

- Georgieva, Ilina. The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR. *Utrecht Journal of International and European Law* 31.80, 2015
- Margulies, Peter. "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism." *Fordham Law Review* 82.5 (2014): 2137-1677
- Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age." *Harvard International Law Journal*, vol. 56, no. 1, 2015, pp. 81–146
- Sinha. G. Alex, NSA SURVEILLANCE SINCE 9/11 AND THE HUMAN RIGHT TO PRIVACY. *Loyola Law Review* 59, 2013: 861-1049
- Wilde, Ralph. "Human Rights Beyond Borders at the World Court: The Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties." *Chinese Journal of International Law* 12.4 (2013): 639-777

Online a spravodajské zdroje

- Bright, Martin, Vulliamy, Ed and Beaumont, Peter. Revealed: U.S. Dirty Tricks to Win Vote on Iraq War, The Guardian, (2 March 2003): https://www.theguardian.com/world/2003/mar/02/usa.iraq
- Ewen McAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' The Guardian (21 June 2013): http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
- Glenn Greenwald and Ewen McAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' The Guardian (June 7 2013): http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni-Article:in /2body%/20ink
- Horwitz, Sari, Asokan, Shyamantha and Tate, Julie, Trade in surveillance technology raises worries, Washington Post, 1 December, 2011: https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-
- Jane Mayer, What's the Matter with Metadata?, NEW YORKER, (June 6 2013): http://www.newyorker.com/online/blogs/newsdesk/2013/06/verizon-nsa-metadata-surveillance-problem.html.

- Nick Hopkins and others, 'GCHQ: inside the top secretworld of Britain's biggest spy agency' The Guardian (1 August 2013): http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden
- Poitras, L., Rosenbach, M., and Stark, H., 'Codename 'Apalachee': How America Spies on Europe and the UN' Der Spiegel (26 August 2013): http://www.spiegel.de/international/world/secret-nsa-documents-showhow- the-us-spies-on-europe-and-the-un-a-918625.html
- Walker, Shaun and Grytsenko, Oksana, "Text messages warn Ukraine protesters they are 'participants in mass riot'", The Guardian, (21 January 2014): https://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

Iné

- International Telecommunication Union: Series X: Data networks, open system communications and security: overview of cybersecurity, 2008
- Kean, Thomas H, and Lee Hamilton. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004.
- Liberty and Security in a Changing World: The President's Review Group on Intelligence and Communications Technologies (12 December 2013): https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
- PEN American Center, "*Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*", (12 November, 2013): https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf
- Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23 January, 2014
- U.S. Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12(R) (Washington, DC: U.S. Joint Chiefs of Staff, 5 February 2013)

Abstrakt ČJ

Za poslední desetiletí překonaly digitální technologie nevídaný vývoj. Internet, který původně sloužil jako prostředek komunikace mezi akademiky, se přetransformoval na hlavní komunikační prostředek používaný na celém světě. Způsob, jakým lidé mohou spolu komunikovat, se tak značně zjednodušil. V důsledku toho, se na kyberprostor zaměřila i pozornost vlád a tajných služeb, s cílem ho co nejvíc kontrolovat. Po Snowdenových odhaleních v roce 2013 se na mezinárodní scéně rozpoutala debata o přípustnosti masivního sledování jako prostředku boje proti terorismu. Od událostí z 11. září se rozšířily pravomoci tajných služeb v oblasti monitorování komunikace osob. Tato praxe s sebou přinesla několik zajímavých a dosud nevyřešených problémů. Je takové jednání vůbec přípustné? Pokud je, za jakých podmínek? Diplomová práce analyzuje legitimitu masivního elektronického sledování a sběru dat v mezinárodním právu v kontextu ochrany lidských práv, zejména práva na ochranu soukromí. Zaměřuje se přitom na elektronické sledování prováděné prostřednictvím sledovacích programů americké Národní bezpečnostní agentury (NSA) a britského Vládního komunikačního ústředí (GCHQ). Jelikož se jedná o programy zahraničního sledování, práce věnuje důkladnou analýzu také sporné otázce extrateritoriální aplikovatelnosti mezinárodních smluv o ochraně lidských práv v kontextu kyberprostoru. Do konfliktu se tak dostávají na jedné straně pozitivní závazky států chránit své občany před hrozbou terorismu a na druhé straně závazek chránit a respektovat právo na soukromí. Práce rozebírá nejdůležitější kritéria, které je nutné splnit k tomu, aby byl zásah do soukromí osob v souladu s mezinárodním právem. Práce nejprve charakterizuje systém ochrany lidských práv podle Mezinárodního paktu o občanských a politických právech a Evropské úmluvy o ochraně lidských práv a základních svobod s důrazem na rozhodování Výboru pro lidská práva a judikaturu Evropského soudu pro lidská práva. Dále přibližuje problematiku kyberprostoru jako místa regulovaného právem a charakteristiku sledování jako takového. Je také vznesen argument, proč by výše zmíněné instrumenty k ochraně lidských práv měly být aplikovatelné i extrateritoriálně a v rámci kyberprostoru. Následně jsou tyto principy aplikovány na sledovací programy NSA a GCHQ, přičemž je posouzena jejich legalita, legitimita a proporcionalita. Na závěr je stručně představen i problém související s kybernetickou špionáží jako zásahem do suverenity států.

Abstrakt AJ

Over the past decade, digital technology has undergone unprecedented development. The Internet, which originally served as a mean of communication among academics, has become the main communication mechanism used throughout the world. The way people can communicate with each other is much easier now. As a result, the attention of governments and secret agencies has also been focused on cyberspace, with the aim of controlling it as much as possible. Following the Snowden revelations in 2013, the debate on the international scene regarding the feasibility of mass surveillance as a tool in the fight against terrorism began. Since the events of September 11, the powers of the secret services in the field of communication of persons have been extended. This practice has brought up some interesting and unresolved issues. Are such activities permissible at all? If so, under what conditions? This diploma thesis analyzes the legitimacy of massive electronic surveillance and data collection in international law in the context of the protection of human rights, especially the right to privacy. It focuses on electronic surveillance conducted by the American National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ). Since these are foreign monitoring programs, the work devotes a thorough analysis to the controversial issue of the extra-territorial applicability of international human rights treaties in the context of cyberspace. The conflicts thus come between the positive obligation of states to protect their citizens from the threat of terrorism and the obligation to protect and respect the right to privacy. Thesis deals with the most important criteria that need to be met to ensure that this invasion of privacy is in accordance with international law. The thesis firstly describes the system of human rights protection under the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms with emphasis on the decision-making process of the Human Rights Committee and the case law of the European Court of Human Rights. It also deals with the issue of cyberspace as a place regulated by law and surveillance characteristics as such. It is also argued, that the above-mentioned human rights instruments should be applicable extra-territorially and within cyberspace. Subsequently, these principles are applied to NSA and GCHQ surveillance programs with the assessment of their legality, legitimacy and proportionality. Another issue that is also briefly presented in the end of the thesis, is the issue regarding electronic espionage as an interference with state sovereignty.

Název práce v českém jazyce:

Legitimita masivního sledování a sběru dat v mezinárodním právu

Název práce v anglickém jazyce:

Legitimacy of mass surveillance and data collection in international law

Klíčová slova:

Masivní sledování, kyberprostor, právo na soukromí

Key words:

Mass surveillance, cyberspace, right to privacy