Nové formy občianskej neposlušnosti v kyberpriestore

Rudolf Kasinec* – Ján Šurkala**

Abstrakt: Autori svoju pozornosť upriamili na problém kybernetickej neposlušnosti a haktivizmu v súčasnom svete. Najskôr sa pokúsili odlíšiť kybernetickú neposlušnosť od tradičných foriem občianskej neposlušnosti. Hlavné rozdiely nachádzajú najmä vo vyhýbaní sa trestnej zodpovednosti za protiprávne konanie, v realizovaní týchto aktivít v kyberpriestore a v špecifickej forme „nenásilia", ktorá je minimálne diskutabilná. Kladú do vzájomnej korelácie anonymitu pri výkone akcií a následné odmietnutie sankcie, ktorá hrozí za toto protiprávne konanie. Autori ďalej tvrdia, že nastolený status quo – kde sú prakticky všetky činy hacktivizmu považované za nezákonné a zároveň veľmi málo z takýchto činov je reálne potrestaných – si zachovali podivnú rovnováhu. Napriek tomu, význam a aktivity predstaviteľov kybernetickej neposlušnosti budú v nasledujúcich rokoch narastať, čo si bude vyžadovať nevyhnutné zásahy i v právnej oblasti.

Kľúčové slová: protesty, občianska spoločnosť, kyberpriestor, anonymita, haktivizmus, kybernetická neposlušnosť, kybernetický terorizmus, Anonymous, popkultúra

Úvod

Občianska neposlušnosť je považovaná za tradičnú formu politického protestu, ktorý vzniká v rámci občianskej spoločnosti.[1] Vo všeobecnosti sú jej hlavnými črtami porušenie zákona, nenásilná povaha akcie,[2] jej verejný charakter a akceptácia sankcie za porušenie zákona.[3] V posledných dvoch desaťročiach sa stále častejšie objavuje nová forma občianskej neposlušnosti, ktorá je špecifická anonymitou, realizáciou v kyberpriestore a snahou o vyhnutiu sa sankcii za porušenie zákona. Táto nová forma občianskej neposlušnosti sa zvykne v zahraničnej literatúre označovať ako *cyber disobedience*, čo by sme do slovenčiny voľne preložili ako „kybernetická neposlušnosť".

V tomto článku sa pokúsime porovnať tradičný koncept občianskej neposlušnosti s kybernetickou neposlušnosťou. Následne sa sústredíme na analýzu potenciálne budúceho vývoja so špecifickým dôrazom na globalizáciu a postmoderné tendencie podkopávania suverenity a právneho poriadku národných štátov.

* Doc. JUDr. Rudolf Kasinec, PhD., docent, Komenského Univerzita v Bratislave, Právnická fakulta, katedra teórie práva a sociálnych vied. E-mail: rudolf.kasinec@flaw.uniba.sk.

** Mgr. Ján Šurkala, PhD., odborný asistent, Komenského Univerzita v Bratislave, Právnická fakulta, katedra teórie práva a sociálnych vied. E-mail: jan.surkala@flaw.uniba@gmail.com.

1 Pojem občianska neposlušnosť (*civil disobedience*) prvýkrát použil Henry David Thoreau. Porovnaj: THOREAU, H. D. Resistance to Civil Government: A Lecture delivered in 1847. In: PEABODY, E. P. (ed.). *Aesthetic Papers.* Boston – New York: The Editor & G. P. Putnam, 1849, s. 189–211.

2 Problematike nenásilia pri uplatňovaní prejavov občianskej neposlušnosti sa venujú viacerí autori. Napr. MORARO, P. Violent Civil Disobedience and Willingness to Accept Punishment. *Essays in Philosophy – A Biannual Journal.* 2007, Vol. 8, Issue 2, Article 6; MORREALL, J. The justifiability of violent civil disobedience. *Canadian Journal of Philosophy*. 1976, Vol. 6, No. 1, s. 35–47. *„Others consider violent civil disobedience as possible but unjustifiable."* Srov. BAYLES, M. The Justifiability of Civil Disobedience. *Review of Metaphysics*. 1970, Vol. 24, No. 1, s. 17–18; BROWN, S. M. Civil Disobedience. *The Journal of Philosophy*. 1961, Vol. 57, Issue 22, s. 678; MARTIN, R. Civil Disobedience. *Ethics*. 1970, Vol. 80, No. 2, s. 135–137.

3 Porovnaj: BEDAU, H. On civil disobedience. *The Journal of Philosophy.* 1961, Vol. 58, No. 21, s. 656.

1. Nová situácia v kyberpriestore

„Pravidlá kultúrnej a politickej rezistencie sa dramaticky zmenili. Technologická revolúcia – reprezentovaná hlavne počítačovou technikou a videom – vytvorila novú geografiu mocenských vzťahov vo vyspelom svete, ktorá bola ešte pred dvadsiatimi rokmi ťažko predstaviteľná. Ľudia sú zredukovaní na dáta a sledovaní v globálnom merítku. Ich mysle sú rozpustené v obrazovkovej realite a autoritatívne sily vzrastajú ťažiac z nezáujmu ľudí. Nová geografia je virtuálna, a preto ťažisko politickej a kultúrnej rezistencie musí byť tiež v elektronickom priestore.“[4]

Kyberpriestor[5] je zvláštnym teritóriom, kde aj malá skupina aktérov dokáže rýchlo a efektívne ovplyvniť verejnú mienku za použitia relatívne skromných zdrojov. Táto prirodzená vlastnosť virtuálneho priestoru otvára bohaté možnosti pozitívnych občianskych akcií, uľahčuje sieťovanie medzi rozličnými jednotlivcami aj skupinami a prináša zo sebou možnosť kultivácie spoločenskej diskusie a chápanie demokracie ako otvoreného systému vládnutia. S pojmom kyberpiestor sa prvýkrát stretneme nie na poli vedeckom, ale bolo použité v roku 1984 v oceňovanej *science-fiction* novele *Neuromancer* kanadsko-amerického autora Williama Gibsona. Ten popísal kyberpiestor ako: *„konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům […] grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta, vzdalující se […].“*[6] Toto vymedzenie sa stalo základom a inšpiráciou i pre právnu vedu.

Jan Kolouch označuje pojem kyberpriestor za ťažko definovateľný a prakticky neobmedzený. Kyberpriestor následne spája s pojmom virtuálna realita: *„Lze říci, že kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného se, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb atd.), adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození, či zániku kyberprostoru jako takového. Kyberprostor je také možné definovat jako prostor kybernetických aktivit, či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.“*[7] Je to svet, ktorý v mnohom kopíruje svet reálny, no je založený na vlastných špecifických pravidlách.

Kyberpriestor sa vyznačuje takmer neobmedzenou mierou slobody. Na druhej strane je však tento priestor veľmi často zneužívaný na manipuláciu s verejnou mienkou a šírenie lží či poloprávd, ktoré sa darí dementovať iba za cenu vysokých časových či finančných nákladov. Nezriedka sme svedkami toho, že nedemokratické štátne aj neštátne štruktúry priamo podnecujú rozvratné tendencie v rámci demokratických štátov a virtuálny priestor im na to slúži viac ako dobre.

---

4 Porovnaj: Critical Art Ensemble. Dostupné na: <http://www.critical-art.net/books/ted/ted1.pdf>, 3. 3. 2017.

5 V česko-slovenskom právnom priestore sa problematike kyberpriestoru venujú: KOLOUCH, J. *Cybercrime.* Praha: CZ.NIC, 2016; GÁBRIŠ, T. Kyberpriestor a nová úprava civilného procesu. In: *21. slovenské dni práva: zborník z konferencie.* Bratislava: Slovenská advokátska komora, 2015, s. 60–77. ŠKOP, M. Hranice práva a kyberprostoru – subverzivita kyberprostoru. *Právník*. 2005, roč. 144, č. 10, s. 1157–1178; POLČÁK, R. Kyberprostor: nové výzvy právní teorii. *Právny obzor*. 2004, roč. 87, č. 3, s. 261–265.

6 GIBSON, W. *Neuromancer.* 4. vydání. Plzeň: Laser-books, 2010, s. 75–76.

7 KOLOUCH, J. *Cybercrime*, s. 43.

V kyberpriestore možno kopírovať i mnohé občianske aktivity, ktorých realizácia je v skutočnom svete zložitá. Napríklad sociálne siete sú skvelým nástrojom na organizovanie rôznych foriem občianskej neposlušnosti a na praktickú realizáciu kybernetickej neposlušnosti. „Internetový dav" môže znefunkčniť webové stránky štátnych orgánov, obchodných spoločností, politických strán a ďalších dôležitých inštitúcií s cieľom vyjadrenia určitých politických a ideologických názorov či osobných presvedčení.

Virtuálny priestor je tiež platformou pre efektívnejšiu realizáciu tradičných foriem občianskej neposlušnosti, kde môže zohrať úlohu štartéra či katalyzátora týchto aktivít. Napríklad cez internet je jednoduchšie zmobilizovať bežný protest či štrajk, sociálne siete uľahčujú komunikáciu medzi protestujúcimi a zefektívňujú ich riadenie. V tomto prípade bude slúžiť kyberpriestor ako nástroj pre organizáciu obrovského počtu osôb.

Rovnako platí, že virtuálny priestor je jedným z najslobodnejších a najmenej regulovaných priestorov vôbec – napriek tomu, že je „len" virtuálny. To by malo na prvý pohľad znižovať jeho dôležitosť, avšak opak je pravdou. Väčšina mladých ľudí tu totiž trávi značné množstvo času – či už v rámci pracovných alebo oddychových aktivít. Preto je nevyhnutné, aby štáty a ostatné verejné autority urobili všetky potrebné opatrenia[8] na to, aby sa z kyberpriestoru nestala zóna bezprávia a neobmedzených kriminálnych či amorálnych aktivít.

Kybernetická neposlušnosť – alebo aj hacktivizmus – operuje v tzv. šedej zóne, pretože jej legalita a legitimita sa môže javiť minimálne pochybná. Hacktivisti zvyčajne bojujú za „slobodu" alebo iné „vyššie hodnoty", pričom sa nerozpakujú porušiť „menej dôležité" pravidlá. Tieto činy však môžu so sebou prinášať aj neočakávané vedľajšie negatívne efekty. Napríklad v prípade znefunkčnenia kľúčových webových stránok verejných inštitúcií, bánk, búrz, nesú negatívne dôsledky tejto operácie nielen samotné inštitúcie, ale aj ich bežní užívatelia. A práve tu leží základný problém s kybernetickou neposlušnosťou – v čom sa principiálne odlišuje od kyberterorizmu? Alebo sú tieto koncepty identické? A ak áno, nemalo by sa k nim právo stavať rovnako?

2. Tradičné formy občianskej neposlušnosti

Občianska neposlušnosť bola dôležitým symbolom boja za ľudské práva v 20. storočí. John Rawls považoval občiansku neposlušnosť za akt výsostne politický. Po prvé, je adresovaný väčšine, ktorá drží politickú moc. Po druhé, legitimizuje sa prostredníctvom odkazu na princípy spravodlivosti – čo Rawls opäť považuje za dominantne politickú hodnotu. Osobné presvedčenie protestujúceho subjektu tu zohráva určitú rolu, avšak o občianskej neposlušnosti sa nedá hovoriť v prípade, že jej cieľom je len vlastný záujem jednotlivca či úzkej skupiny.[9] Nič to však nemení na tom, že špecifické skupinové záujmy politických aktérov – ako napr. pracujúcich, černochov, gejov – sú zvyčajným dôvodom občianskej neposlušnosti. Určujúcim faktorom ale je, že sa vždy snažia zmeniť nejakú verejnú politiku.

V Čechách najkomplexnejšie dielo o probléme občianskej neposlušnosti vytvoril Jan Kysela s názvom *Právo na odpor a občanskou neposlušnost*. Zaoberá sa najmä historickým vývojom oboch právnych inštitútov v rozdielnych štátoch. Podľa Kyselu by pri realizácii aktov občianskej neposlušnosti mali byť všetky zákonné možnosti odstránenia bezprávia

8 Pre viac o tomto probléme pozri: DAŇKO, M. The internet in reflection of human rights and fundamental freedoms. In: *Communication as a measure of protection and limitation of human rights. Information in relation to human rights*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2013, s. 658.

9 Viď RAWLS, J. *Theory of justice*. Revised Edition. Cambridge: Harvard University Press, 1999, s. 321.

vyčerpané. Má teda subsidiárny charakter a je krajným prostriedkom po vyčerpaní všetkých ostatných možností (najmä ľudovej iniciatívy a referenda).[10] Pri realizácii aktov kybernetickej neposlušnosti sa táto subsidiarita neuplatňuje. Celý koncept neposlušnosti je širšie koncipovaný a nezameriava sa len na vyjadrenie nespokojnosti s politikou vlády.

Na Slovensku sa pojmu občianska neposlušnosť venoval napr. Radoslav Procházka, podľa ktorého je *„konaním, ktoré nie je spoločensky nebezpečné, naopak, za daných predpokladov je konaním spoločensky užitočným. Preto je v súlade s ústavou a politickou etikou a je legitímnym prostriedkom usilovania o spoločenský konsenzus – je mimoprávnou formou dialógu medzi reprezentantmi jednotlivých sociálnych pozícií.“*[11] Takto je možné vymedziť tradičnú podobu občianskej neposlušnosti. Pri kybernetickej neposlušnosti vystupujú na povrch rozličné ciele a znaky.

Aktivity vykonané v rámci občianskej neposlušnosti sú v rozpore s právom, ale zvyčajne majú nenásilný charakter.[12] Ako poznamenal Lawrence Quill, občianska neposlušnosť začala byť široko akceptovaným nástrojom na dosiahnutie progresu v podmienkach liberálno-demokratických štátov v 60. rokoch minulého storočia.[13] Preto možno konštatovať, že hoci je nedostatok legality občianskej neposlušnosti zjavný, s jej legitimitou to tak nie je. Tá sa podľa nášho názoru odvíja skôr od cieľov politických aktivistov a ich odozve v spoločnosti.

John Rawls definoval občiansku neposlušnosť nasledujúcimi znakmi:

1) Úmyselné porušenie práva;
2) Nenásilná povaha akcie;
3) Verejnosť činu so snahou dosiahnuť čo najväčšiu mediálnu odozvu;
4) Akceptácia právnych následkov protiprávneho konania (sankcie);
5) Zacielenie na zmenu práva alebo nejakej verejnej politiky;
6) Snaha presvedčiť majoritu o oprávnenosti požiadaviek a cieľov;
7) Nasmerovanie na povedomie o spravodlivosti, ktoré je zhmotnené v zákonoch a spoločenských inštitúciách.[14]

Pri občianskej neposlušnosti a jej prejavoch nemožno opomenúť objekt, proti ktorému zvyčajne smeruje. Tradičná podoba občianskej neposlušnosti má vždy politický cieľ. Podľa Jana Pinza *„obecně vzato míří občanská naposlušnost proti celé škále mocenských nepravostí, zejména spočívajících ve zneužívání veřejné moci ve státě, ať už jde o šikanosní výkon veřejnoprávních pravomocí nebo o porušování lidských a občanských práv činností státních organů v jednotlivých veřejnoprávních funkcích, tzn. včetně právotvorby.“*[15] Objekt občianskej neposlušnosti sa však neustále rozširuje a zasahuje i do ekonomickej oblasti, náboženskej, medzinárodnej politiky a mnohých ďalších.

Občianska neposlušnosť podobne ako väčšina spoločenských a právnych inštitúcií podlieha dynamike a zmenám. Aj z tohto dôvodu neexistuje jedna všeobecne prijímaná definícia tohto pojmu, ktorá by bola z časového hľadiska nemenná. Preto nejestvujú ani

10 KYSELA, J. *Právo na odpor a občanskou neposlušnost*. Brno: Doplněk, 2001, s. 105.
11 PROCHÁZKA, R. Občianska neposlušnosť – legitímny disident? *Právny obzor*. 1998, roč. 81, č. 1, s. 42.
12 K problému nenásilia bližšie pozri odkazy v poznámke č. 4.
13 Viď QUILL, L. *Civil Disobedience: (Un)Common Sense in Mass Democracies*. Hampshire: Palgrave Macmillan, 2009, s. 2.
14 Viď RAWLS, J. *Theory of justice*, s. 320–323.
15 PINZ, J. Občanská neposlušnost – demokratické právo občanské společnosti. In: *Scientific papers of the University of Pardubice. Series D Faculty of Economics and Administration*. 1999, Vol. 4, s. 274.

presné hranice, čo sa za občiansku neposlušnosť považovať dá, a čo už nie.[16] V priebehu posledných desaťročí došlo k signifikantnej transformácii tradičného (moderného) konceptu občianskej neposlušnosti. Kybernetická neposlušnosť je teda len jednou z aktuálnych tendencií, ktoré tradičné definície a kategorizácie narúšajú. Vzhľadom na ich intenzitu však nesmú a nemôžu byť prehliadané.

3. Fenomén hacktivizmu ako formy kybernetickej neposlušnosti

Kybernetická neposlušnosť sa zvykne stotožňovať s pojmom hacktivizmus. *„Hacktivizmus je zmesou hackovania a aktivizmu, pričom pod hackovaním sa rozumie použitie výpočtovej techniky nezvyčajným alebo ilegálnym spôsobom typicky využívajúc špeciálny software (hackovací nástroj). Hacktivizmus je nástrojom občianskej neposlušnosti, ktorý ju prenáša do kyberpriestoru. […] Nakoľko je hackovanie často zmieňované v médiách, aj hacktivizmus môže generovať značnú publicitu tak pre aktivistov ako aj pre ich ciele.“*[17]

Ako sme sa už zmienili vyššie, v súčasnom svete rapídne rastie dôležitosť kyberpriestoru. Vlády štátov, medzinárodné organizácie aj nadnárodné korporácie sa snažia tento priestor kontrolovať právnymi aj mimoprávnymi prostriedkami. Toto zasahovanie verejných autorít, ktoré „kryjú“ aktivity súkromných korporácií, je v ostrom kontraste so slobodným charakterom internetu.

Kybernetická neposlušnosť a hacktivizmus sa prvýkrát objavili na sklonku 20. storočia. *The Critical Arts Ensemble* (CAE)[18] vydalo už v roku 1996 apel na začatie priamej politickej akcie a občianskej neposlušnosti vo virtuálnom priestore, pretože tento sa stal novým priestorom, v ktorom elity získavajú a znásobujú svoju moc. Prostriedkami tejto akcie sa mali stať taktické blokády zacielené na obeh informácií vo virtuálnom priestore.[19]

V praxi môžeme rozlíšiť viaceré taktiky na dosiahnutie tohto cieľa. Jednou z nich je napríklad on-line sabotáž, ktorá môže mať intenzitu od menej závažného DDoS útoku (*distributed-denial-of-services*) až po tvrdšie ataky na servery, ktoré majú spôsobiť preťaženie zacielených internetových stránok či infiltráciu počítačových systémov. Napokon môžu hackeri prevziať kontrolu nad samotnými webovými stránkami a infiltrovať ich v záujme svojich politických cieľov.[20]

Špecifickým znakom hacktivizmu je verejné demonštrovanie schopnosti narušiť riadne fungovanie „nepriateľských cieľov“. Avšak publicita skutku nie je spôsobená len potrebou zastrašenia tých, ktorí sú pri moci, ale má za cieľ získať súhlas širokých internetových más, ktoré môžu postupne vytvoriť širšiu antisystémovú identitu. Je paradoxom, že táto spoločná identita sa vyznačuje anonymitou.[21] Táto skupina si je na jednej strane dobre vedomá svojich cieľov a prostriedkov na ich dosiahnutie, na strane druhej jej členovia ani v jej vnútri neodhalia svoju skutočnú totožnosť.

Značnú popularitu týmto trendov dodáva aj súčasná popkultúra. Film *V ako Vendetta*[22] bol natočený v roku 2005, teda dva roky potom, ako hackerská skupina *Anonymous* – ktorá

16 Viď MILLIGAN, T. *Civil Disobedience Protest, Justification, and the Law*. London: Bloomsbury Academic, 2013, s. 13.

17 Viď DENNING, D. E. Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In: ARQUILLA, J. – RONFELDT, D. F. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Pittsburgh: RAND, 2001, s. 263.

18 Pre viac informácií o danej skupine pozri: <http://critical-art.net>, 23. 3. 2017.

19 JORDAN, T. *Activism! direct action, hacktivism and the future of society*. London: Reaction Books, 2002, s. 120.

20 Viď SHANTZ, J. – TOMBLIN, J. *Cyber Disobedience: Re://Presenting Online Anarchy*. Washington: Zero Books, 2014, s. 10.

21 Viď MILLIGAN, T. *Civil Disobedience Protest, Justification, and the Law*, s. 4.

22 Pre viac informácií o tomto unikátnom dystopickom filmovom diele pozri: <http://www.imdb.com/title/tt0434409/>, 23. 3. 2017.

sa priamo hlási k ideám hacktivizmu – začala svoju činnosť. Členovia tejto „tajnej" webovej komunity si vybrali za svoj hlavný symbol masku Guya Fawkesa[23] v podobe, v akej bola zobrazená v komixovej predlohe k zmienenému filmu. Hlavný hrdina filmu bojuje proti štátnemu režimu v dystopickej Veľkej Británii, pričom vo svojom boji neváha používať ani násilie (teroristické útoky, atentáty na vedúcich štátnych predstaviteľov a zverejňovanie utajovaných štátnych informácií). Jeho konanie malo veľký vplyv na občanov a veľká skupina opozične naladených ľudí si vybrala nenásilné formy občianskej neposlušnosti.

4. Dôsledky kybernetickej neposlušnosti v súčasnosti

Členovia skupiny *Anonymuous*[24] s pomyselnými „V" maskami na svojich tvárach bojujú proti štátnym politikám, nadnárodným monopolom, bezpečnostným agentúram a ďalším korporáciám, firmám a jednotlivcom. Právna a morálna kvalifikácia ich činnosti je však otázka. Teda buď ide o formu kybernetickej neposlušnosti – teda právne pochybného ale viac-menej legitímneho konania – alebo ide o páchanie trestnej činnosti vo forme kyberterorizmu – pričom by v tomto prípade okrem jednoznačnej nelegálnosti boli tieto skutky aj nelegitímne a nemorálne.

Konanie skupiny *Anonymous* ale aj ďalších hacktivistických skupín sa môže javiť ako hektické, neorganizované, alebo dokonca náhodilé z pohľadu vonkajšieho pozorovateľa. V skutočnosti však vo vnútri týchto skupín prebieha veľké množstvo zložitých a sofistikovaných operácií, ktoré sú pre outsidera neviditeľné.[25] Tento jav je spôsobený absenciou akejkoľvek pevnej hierarchickej štruktúry, ktorú zvyčajne majú konvenčné politické alebo spoločenské zoskupenia. V hactivistických skupinách je rovnako relativizovaná rola vedenia s autoritou a povinným vynucovaním subordinácie vo vzťahu k rádovým členom. Nie je vôbec neobvyklé, že dôležité rozhodnutia sa robia participatívne s účasťou všetkých členov, ktorí navyše majú širokú autonómiu sa do konkrétnej akcie zapojiť alebo nezapojiť v závislosti od svojich vlastných názorov a preferencií. To samozrejme zvyšuje pocit dôvery a vzájomnej spolupráce vo vnútri tých skupín a operatívnych jednotiek.[26]

Rovnako je tenká hranica medzi kybernetickou neposlušnosťou a extrémizmom (zahŕňajúc rozličné formy intolerancie). To demonštrujeme na čerstvom prípade zo Slovenska. Jedna mladá žena vyjadrila svoje politické názory na islam veľmi radikálnym spôsobom – omočila Korán – najsvätejší symbol moslimskej viery – následne knihu roztŕhala na drobné kúsky, poliala benzínom a napokon zapálila. Samozrejme si celú „procedúru" nahrávala na video, ktoré následne zverejnila na internete.[27] Orgány činné v trestnom konaní začali proti nej trestné stíhanie za hneď niekoľko trestných činov, ktorých sa mala v súbehu dopustiť: výroba extrémistických materiálov,[28] násilie proti skupine obyvateľov,[29] hano-

---

23 Guy Fawkes je skutočnou historickou postavou katolíckeho teroristu, ktorý sa neúspešne pokúsil vyhodiť do vzduchu budovu Anglického parlamentu v roku 1605 a tento pokus je nazvaný „Sprisahanie strelného prachu". Viac o tejto osobe sa dozviete: FRASER, A. *The Gunpowder Plot: Terror And Faith In 1605*. London: Hachette, 2010; KENNETH, A. *The Story of Gunpowder*. London: Wayland, 1973.

24 Pozri oficiálnu stránku hnutia Anonymous: <http://anonofficial.com/>, 23. 3. 2017. Moto tejto skupiny znie: *„We are legion. We do not forgive. We do not forget. Expect us."*

25 SQUIRE, J. *Anonymous and the future of hacktivism*. *Socialist Alternative Magazine*. Dostupné na: <http://sa.org.au/node/1177>, 5. 3. 2017.

26 SHANTZ, J. – TOMBLIN, J. *Cyber Disobedience*, s. 14.

27 Pre základné informácie o tomto prípade pozri: <http://metro.co.uk/2017/02/16/woman-films-herself-urinating-on-koran-before-setting-it-on-fire-6451744/>, 23. 3. 2017.

28 Viď § 422a Trestného zákona (T. z., 300/2005 Z. z.).

29 Pozri § 359 T. z.

benie národa, rasy a presvedčenia[30] a podnecovanie k národnostnej, rasovej a etnickej nenávisti.[31] V prípade dokázania viny jej hrozí trest odňatia slobody v rozsahu 3 až 6 rokov. Tento prípad je samozrejme učebnicovým prípadom zneužitia virtuálneho priestoru s chorou snahou upútať pozornosť verejnosti a šíriť idey neznášanlivosti a diskriminácie.

5. Znaky a definícia kybernetickej neposlušnosti

Kybernetická neposlušnosť a hacktivizmus sú pomerne nové koncepty, ktoré vznikli na základoch tradičnej občianskej neposlušnosti. Je však dôležité rozlišovať medzi týmito novými formami neposlušnosti a jej tradičnými podobami. Obe síce v dnešnej spoločnosti pôsobia popri sebe, dôležitosť kybernetickej neposlušnosti však stúpa každým dňom.

Špecifickými znakmi kybernetickej bezpečnosti sú:

a) *Anonymita*. Pri kybernetickej neposlušnosti je takmer pravidlom, že verejnosť nevie totožnosť osoby, alebo osôb, ktoré za danou aktivitou stoja. Viditeľné sú len masky a symboly, nie skutoční ľudia. Umožňuje to špecifické prostredie – kybernetický priestor – cez ktorý sa môžu tieto virtuálne sily zjednotiť a žiť spoločným životom pri zachovaní utajenia ich skutočnej totožnosti.[32]

b) *Aktivity porušujúce právo*. Skoro všetky aktivity, ktoré spadajú pod kybernetickú neposlušnosť, určitým spôsobom porušujú právo. Tu sú však dôležité dve poznámky. Po prvé, ilegalita kybernetickej neposlušnosti je do značnej miery spôsobená snahou verejných autorít vytlačiť akékoľvek podoby občianskej neposlušnosti z kyberpriestoru. Zatiaľ čo v reálnom priestore sú zaručené práva verejnosti na protest proti vláde a jej prešľapom, vo virtuálnom svete absentuje pozitívne ukotvenie týchto práv.[33] Po druhé, táto „totálna" ilegalita je vyvážená praktickou neschopnosťou orgánov činných v trestnom konaní adekvátne stíhať tieto trestné činy. Korelácia tých dvoch javov je viac ako zjavná. Svetová občianska spoločnosť necíti akútnu potrebu bojovať za pozitívne ukotvenie práva na protest v kyberpriestore v právnych poriadkov štátov či v medzinárodných zmluvách, pretože stíhateľnosť týchto skutkov je dnes minimálna.

c) *Široká škála záujmov*. Prostriedky kybernetickej neposlušnosti môžu byť zamerané na dosiahnutie vskutku rôznorodých cieľov, napr.: politických, ekologických, ekonomických, korporátnych, pracovných, komunálnych, atď.

d) *Špecifická forma nenásilného konania*. Jedným z definičných znakov tradičnej občianskej neposlušnosti je nenásilná forma konania. Pri kybernetickej neposlušnosti je táto črta viac-menej zachovaná pri zohľadnení špecifických prostriedkov, ktoré virtuálny priestor ponúka. Ide napr. o tieto možnosti „nenásilného boja":

   i. *Virtuálne Sit-ins a blokády*. Analogické k okupačným štrajkom. Ich cieľom je znemožniť prístup k stránkam a systémom určitých inštitúcií a tak pritiahnuť pozornosť verejnosti či verejných autorít na sledované ciele a požiadavky.[34]

   ii. *E-mailové bomby*. Aj táto metóda ma charakter blokády s cieľom znemožniť správne fungovanie e-mailov zacielenej inštitúcie, tým že sú jej v krátkej dobe zaslané veľké množstvá e-mailov podobného charakteru, ktorými sa jej e-mailové kontá zahltia.

30 Pozri § 423 T. z.

31 Pozri § 424 T. z.

32 Porovnaj: JORDAN, T. – TAYLOR, P. *Hacktivism and Cyberwars Rebels with a cause?* New York: Routledge, 2004, s. 1.

33 SHANTZ, J. – TOMBLIN, J. *Cyber Disobedience*, s. 22.

34 DENNING, D. E. *Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy*, s. 264.

Obmedzenie práv bežných občanov, ktorí v dôsledku tohto útoku nemajú možnosť využívať služby zacielenej inštitúcie, je hacktivistami ospravedlňované tým, že ich riadne podané protesty a sťažnosti by boli ignorované.[35]

iii. *Hackovanie webových stránok a počítačov (break-ins)*. Týmto typom hackerského útoku je možné meniť obsah zacielených webových stránok alebo presmerovať ich užívateľov na alternatívne stránky.[36] Hlavným cieľom je informovať internetových užívateľov o dôležitom posolstve protestujúcich. Aj keď sa táto forma protestu môže javiť ako pomerne neškodná – nakoľko nevzniká až taká rozsiahla a zásadná škoda – o etickosti danej praxe existujú vážne pochybnosti.[37]

iv. *Počítačové vírusy a červy*. Ide pravdepodobne o najviac invazívnu a istým spôsobom aj násilnú metódu hacktivistického útoku. Jeho zámerom je spôsobiť závažné škody na zacielených počítačoch a webových sídlach cieľom šírenia protestného odkazu.[38]

e) *Realizácia vo virtuálnom priestore*. Všetky aktivity kybernetickej neposlušnosti sa odohrávajú vo virtuálnom priestore, ktorý slúži jednak ako médiu prenosu ideového posolstva, ale poskytuje aj špecifické prostriedky boja. Je možné konštatovať, že všetky špecifiká kybernetickej neposlušnosti, ktoré sme zmienili vyššie, sú podmienené práve osobitým charakterom tohto priestoru.

f) *Snaha vyhnúť sa sankcii za porušenie práva*. Na rozdiel od tradičných foriem občianskej neposlušnosti, pri ktorých sú protestujúci uzrozumení s tým, že sa na ich protiprávne konanie vzťahujú právne sankcie, je pri kybernetickej neposlušnosti očividná snaha subjektov sa týmto sankciám efektívne vyhnúť. Ide to samozrejme ruka v ruke s anonymitou. Hlavní lídri tradičnej občianskej neposlušnosti – ako napr. Mahatma Gandhi, Martin Luther King, Henry David Thoreau či Aung San Suu Kyi[39] – si vo väzení odpykali niekedy aj dlhoročné tresty. Anonymita hacktivistických skupín umožňuje jej členom praktickú beztrestnosť, hoci právna a morálna zodpovednosť ich činov zostáva pochopiteľne nedotknutá bez ohľadu na neefektívnosť vynucovania právnych sankcií.

6. Hranica medzi kybernetickou neposlušnosťou a kybernetickou kriminalitou

Oba pojmy sú pomerne nové v právnom poriadku Slovenskej republiky. Do oblasti tzv. počítačovej kriminality zasiahla novela aktuálne platného Trestného zákona 300/2005 Z. z. zo dňa 1. 1. 2016, kedy boli precizované a rozšírené trestné činy úzko súvisiace s počítačovými systémami: § 247 Neoprávnený prístup do počítačového systému; § 247a Neoprávnený zásah do počítačového systému; § 247b Neoprávnený zásah do počítačového údaja; § 247c Neoprávnené zachytávanie počítačových údajov; § 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov a § 360a Nebezpečné prenasledovanie. Skupina týchto ustanovení Trestného zákona jasne zadefinovala, ktoré aktivity sú v kyberpriestore považované za protiprávne, a aká hrozí sankcia za ich realizáciu.

35 Ibidem, s. 268.

36 Ibidem, s. 272–273.

37 Porovnaj napr. SPAFFORD, E. H. Are Computer Hacker Break-ins Ethical? *Journal of Systems and Software*. 1992, Vol. 17, No. 1, s. 41–47.

38 DENNING, D. E. *Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy*, s. 278.

39 Politická aktivistka z Barmy, ktorá bola umiestnená v domácom väzení takmer 15 z 21 rokov od 1989 do 2010, stala sa tak jednou zo svetovo najznámejších politických väzňov vo svete. Viac informácií o tejto pozoruhodnej žene sa môžeme dozvedieť z filmu Luca Bessona *Dáma* (*The Lady*), alebo z kníh: *Freedom from Fear: And Other Writings* (2010), *Letters from Burma* (2010), *Aung San Suu Kyi, Voice of Hope: Conversations with Alan Clements* (2008).

§ 247 a nasledujúce sú súčasťou štvrtej hlavy Trestného zákona – trestné činy proti majetku. Predpokladá sa preto ich finančné pozadie, kde sa predpokladá, že trestne zodpovedná osoba plánuje uskutočnením týchto nelegálnych aktivít dosiahnuť majetkový prospech, prípadne poškodiť finančné záujmy iných osôb.

Kybernetická neposlušnosť ako právne i teoreticky málo zmapovaný fenomén sa vyznačuje znakmi, ktorým sme sa už bližšie venovali. Nesmieme opomenúť ani primárne rozdiely medzi počítačovou kriminalitou a kybernetickou neposlušnosťou. Podľa nášho názoru je zásadným rozdielom sledovaný cieľ, ktorý chcú realizátori kybernetickej neposlušnosti a kyberzločinci dosiahnuť. *„Pod kybernetickou kriminalitou, alebo taktiež kyberkriminalitou, rozumieme takú činnosť, ktorou je porušovaný zákon alebo je v rozpore s morálnymi pravidlami spoločnosti. Táto kriminalita môže byť namierená priamo proti počítačom, ich hardwaru, softwaru, dátam, sieťam a pod., alebo v nej vystupuje počítač len ako nástroj pre páchanie trestného činu, prípadne počítačová sieť a k nej pripojené zariadenia sú prostredím, v ktorom sa taká činnosť odohráva.“*[40]

Kyberzločinci svojimi činmi dosahujú majetkový alebo iný ekonomický prospech, prípadne šíria prostredníctvom svojich útokov strach (kyberterorizmus) a útočia tak na demokratické hodnoty súčasných slobodných štátnych režimov. Vykonávatelia kybernetickej neposlušnosti majú vopred stanovený cieľ – poukázanie na lokálny alebo globálny spoločenský problém (ekologický, politický, ekonomický a pod.). Svojimi aktivitami nechcú vyvolať strach, ale chcú informovať čo najväčší počet adresátov o probléme a vyvolať tak búrlivú spoločenskú reakciu prípadne efektívny politický nátlak na kompetentné orgány verejnej moci. Kybernetická neposlušnosť sa následne môže spojiť s tradičnou civilnou neposlušnosťou[41] a tým sa zosilní tlak na príslušné orgány, ktoré budú nútené konať.

Čo sa legitímnosti prejavov kybernetickej neposlušnosti týka, tak tu môžeme postupovať podobne ako v prípade tradičnej civilnej neposlušnosti. Oba inštitúty sa pohybujú na hrane zákona, no ich nelegálne prejavy nesmerujú proti ohrozeniu demokratických hodnôt a princípov právneho štátu. Ich účelom je poukázať na komplexné (migrácia, obchodovanie s ľuďmi, znečisťovanie životného prostredia) či parciálne problémy (korupcia v štáte, zlé postavenie LGBTI osôb, zlé postavenie zamestnancov v školstve a pod.) a vyvolať celospoločenskú odozvu.

Spoločným znakom kybernetickej neposlušnosti a kyberzločinu je ich principiálna protiprávnosť. V zmysle zachovania zásad právneho štátu a právnej istoty je teda prípustné a podľa nášho názoru aj osožné, že sa sankcie aplikujú aj na prípady kybernetickej neposlušnosti. Na strane druhej je ale pri kybernetickej neposlušnosti dôležité zobrať do úvahy verejnoprávny charakter – teda motiváciu „narušovateľov právneho poriadku“ zlepšiť svet okolo seba – a premietnuť to do zmiernenia trestov. V odôvodnených prípadoch si vieme predstaviť aj úplnú exkulpáciu. Hranice však musí stanoviť aplikačná prax, ktorá by v tomto mohla pokojne vychádzať z princípov a zásad ako pri klasickej občianskej neposlušnosti.

---

40 JIROVSKÝ, V. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 19. K tomu ďalej pozri: MÉSZÁROS, T. Kyberkriminalita a právne možnosti jej postihu – realita a perspektíva vývoja. In: *Míľniky práva v stredoeurópskom priestore. 2012. 2. časť.* Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2012, s. 988–994.

41 Ako príklad môžeme uviesť protikorupčné protesty v Slovenskej republike, ktoré majú svoj základ v aktivitách v kyberpriestore. Na začiatku sa zverejňovali videá, otvárali sa politické (korupčné) kauzy. Následne bola na sociálnej sieti vytvorená udalosť s názvom Veľký protikorupčný pochod, ktorú podporilo viac ako 21 tisíc užívateľov a viac ako 12 tisíc sa plánovalo udalosti i fyzicky zúčastniť. Udalosť sa uskutočnila 18. apríla 2017 na Hviezdoslavovom námestí v Bratislave a podľa odhadov sa jej zúčastnilo viac ako 8 tisíc osôb.

Záver

Ak máme vôbec pripustiť, že existuje rozdiel medzi kyberterorizmom, kybernetickou kriminalitou a kybernetickou neposlušnosťou, tak musíme hneď zdôrazniť, že medzi nimi existuje v skutku tenká hranica.

Subjekty kybernetickej neposlušnosti majú zväčša šľachetné a vysoké ciele, pre ktoré chcú získať pozornosť ostatných ľudí, občianskej spoločnosti, vybraných spoločenských skupín či verejných autorít. Môžu byť však tieto vznešené ašpirácie jediným ospravedlnením niekedy značne závažných zásahov do práv iných subjektov a ohrození dôležitých verejných hodnôt?

Zastávame názor, že kybernetická neposlušnosť je novou formou občianskej neposlušnosti vyjadrujúcej zmenu spoločenskej klímy, ktorú priniesli nové informačno-technické prostriedky. Túto zmenenú situáciu však dosiaľ nereflektovalo právo. Ako sme už poznamenali vyššie, represívne prístupy verejných autorít vyznievajú tragicky bezzubo, nakoľko bojujú proti „nepriateľovi" prostriedkami, ktorými ho v priestore bez hraníc nemôžu poraziť. Navyše je vysoko spochybniteľná ale legitimita týchto politík a snáh.

Preto navrhujeme, aby táto disparita medzi ambíciami národných kriminálnych orgánov a ich reálnymi možnosťami efektívne zakročiť proti týmto javom, bola zmiernená buď efektívnejšou spoluprácou medzi štátmi ako aj medzinárodnými organizáciami s cieľom potlačenia ilegálnych kriminálnych aktivít definovaných tak, ako sú v súčasnosti, alebo aby sa prikročilo k ich redefinícii s cieľom legalizovania menej závažných činov tak, aby sa vytvoril legálny priestor pre výkon kybernetickej neposlušnosti.

Podľa nášho názoru je druhá alternatíva lepším riešením. V tomto sa stotožňujeme s J. Squireom – bývalým členom hackerskej skupiny *LulzSec* – ktorý ešte v roku 2013 konštatoval:

„Online aktivizmus a hacktivizmus budú v budúcnosti nepochybne rásť. Sčasti to bude dôsledkom prebehajúcich snáh vlád a korporácií podrobiť si bežných internetových užívateľov, čo vyvolá zákonitú odvetnú reakciu a snahu internetových užívateľov o udržanie si svojich slobôd. Sčasti však k tomu dôjde aj preto, lebo virtuálny priestor sa stáva stále dôležitejším pre organizovanie protestných aktivít. Hacktivizmus bude dôležitejší aj preto, lebo tak vlády ako aj korporácie – ktoré sú častým objektov útokov ľavicových a protestných hnutí – operujú stále viac a viac vo virtuálnom priestore, čím sa stávajú zraniteľnejšími voči online aktivizmu."[42]

Je paradoxom, že napriek extrémne frekventovaným správam o hacktivizme, stojí tento fenomén na okraji záujmu verejnosti, a to aj odbornej aj laickej. Boj za partikulárne politické záujmy sa tak ticho presúva na iné – doteraz neprebádané – teritórium. Z ulíc a námestí, titulných stránok novín a politických vyhlásení či transparentov rozzúreného davu sa politický protest presúva do virtuálneho priestoru internetu. Nakoľko ide o priestor nový – bez zaužívaných konvencií, možnosti fyzického násilia a vo veľkej miere aj bez normatívnych pravidiel ako takých. Na strane druhej sa tento priestor vyznačuje novými možnosťami aktivizácie širokých más globálnej populácie a dobrovoľne zdieľanej publicity. V dnešnej dobe majú informácie snáď tú najvyššiu hodnotu – preto je virtuálny priestor azda najdôležitejším teritóriom na tejto planéte. Preto niet divu, že prebieha tichý boj o jeho kontrolu.

42 SQUIRE, J. *Anonymous and the future of hacktivism*. Dostupné na: <http://sa.org.au/node/1177>.

New Forms of Civil Disobedience in Cyberspace

Rudolf Kasinec – Ján Šurkala

Abstract: The authors address the problem of cyber disobedience and hacktivism in contemporary world. Firstly, they try to distinguish cyber disobedience from the traditional forms of civil disobedience. The main differences they see in avoidance of punishment for illegal conduct, exercising these activities in the cyber space and specific nature of "non-violence", which is at least disputable. They put to the correlation the anonymity of the actions and avoidance to accept the punishment for criminal deeds. They argue that the status quo – where virtually all acts of hacktivism are considered illegal and in the same time very little of such acts are punished – conserved the strange equilibrium. However, they prognose that the importance of cyber disobedience will grow in the near future and this movement should be followed by proper changes of the law in action.

Key words: protests, civil society, cyber space, anonymity, hacktivism, cyber disobedience, cyber terrorism, the Anonymous, pop-culture