GLOBAL INFORMATION SOCIETY WATCH 2014

Nadzor komunikacija u digitalnom dobu - ODABRANI TEKSTOVI

Association for Progressive Communications (APC)

OneWorld Platform for Southeast Europe Foundation (OWPSEE)

GLOBAL INFORMATION SOCIETY WATCH

2014

ODABRANI TEKSTOVI

APC Hivos

Global Information Society Watch **2014** – IZABRANI TEKSTOVI

Prevod sa engleskog:
Denis Šparavalo

Lektorica:
Aida Mahmutović

Odabir tekstova i adaptacija:
One World Platform for South East Europe Foundation (OWPSEE)

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Association for Progresive Communication (APC)

Global Information Society Watch
Communications surveillance in the digital age
Published by APC and Hivos
2014

ISSN: 2225-4625
ISBN: 978-92-95102-16-3
APC-201408-CIPP-R-EN-DIGITAL-207

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2014.

www.GISWatch.org

ODGOVORNOST POSREDNIKA I DRŽAVNI NADZOR

Elonnai Hickok
Centre for Internet and Society (CIS) India
www.cis-india.org

UVOD

Dana 30. juna 2014. godine objavljen je izvještaj "Pravo na privatnost u digitalnom dobu: Izvještaj Ureda Visokog Povjerenika Ujedinjenih Nacija za Ljudska Prava (OHCHR)"[1] Izvještaj prepoznaje odnos između pružatelja usluga (IP provider) i nadzora te povećanjem trenda privatnog nadzora, ističući:

> Postoje čvrsti dokazi o sve većem oslanjanju vlada na privatni sektor s ciljem provođenja i olakšavanja digitalnog nadzora. Na svim kontinentima, vlade su koristile i formalne i pravne mehanizme te tajne metode kako bi dobile pristup sadržaju kao i metapodacima. Ovaj proces je sve više formaliziran: kako se pružanje telekomunikacijskih usluga prebacuje iz javnog sektora u privatni sektor, tu se pojavila i "delegacija za provedbu zakona" i kvazi-sudskih odgovornosti za Internet posrednike pod krinkom 'samoregulacije' ili '' suradnje"[2].

Ovaj izveštaj će istražiti kako se zakonski uslovi, prakse i politike, koje se odnose na posredničke odgovornosti, hrane ovim rastćim trendom kroz utjelovljavanje zahtjeva za posrednike/ce koji olakšavaju nadzor. Pri tome, ovaj izveštaj će istražiti aspekte politike prodredničkih odgovornosti i praksi, i kako se to odražava te omogućuje državni nadzor. Na kraju, izveštaj će razmotriti praznine koje postoje u politici, a koje se odnose na privatnost, nadzor i posredničku odgovornost.

POSREDNICI I PRIVATNOST

Online komunikacija, interakcija i transakcija su sastavni dio našeg svakodnevnog života. Kao takvi, posrednici - uključujući ali ne ograničavajući se na: tražilice, društvene mreže, cyber kafiće, internet i telekomunikacijske usluge - igraju ključnu ulogu obzirom na privatnost korisnika/ca. Kako pojedinci koriste posredničke platforme na dnevnoj i rutinskoj osnovi, od pretraživanja za informacijama na internetu, objavljivanja i ažuriranja sadržaja na društvenim mrežama, korištenja VoIP usluga (Skype, Viber, Wire i sl.) za povezivanje s prijateljima i kolegama, ili korištenje usluga u internet caffe-u, posrednici i domaćini (host) zadržavaju i imaju pristup ogromnim količinama osobnih podataka svojih korisnika/ca diljem svijeta, bez obzira na nadležnosti. U tom kontekstu, praksa kompanija i zakonski propisi neke zemlje imaju dalekosežne posljedice na prava - konkretno privatnost i slobodu izražavanja - i domaćih i stranih korisnika/ca.

POSREDNICI, VLADE I NADZOR

"Pravo na privatnost u digitalnom dobu" također zapaža da su internet i pripadajuće tehnologije omogućile vladama da provedu nadzor kao nikada do sada. To je istaknula i objava Edwarda Snowdena, koji je pokazao opseg pristupa koji vlada SAD ima nad podacima u posjedu internetskih tvrtki sa sjedištem u SAD-u. Otkrića također naglašavaju neizvjesnu poziciju u koju su stavljene tvrtke koje nude ove usluge i tehnologije. Iako opseg i količina prikupljenih i zadržanih podataka variraju ovisno o vrsti posrednika, usluga koje nudi i lokaciji infrastrukture, vlade su prepoznale važnu ulogu posrednika - osobito u njihovoj sposobnosti da pomognu državni nadzor omogućavajući pristup ogromnim količinama korisničkih podataka i identifikaciju potencijalno štetnih ili opasnih sadržaja. U sklopu toga, tu je pomak od reaktivnog državnog nadzora koji se temelji na zahtjevu i ovlaštennju, do djelomično

[1] www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[2] Ibid.

privatiziranog nadzora, s tvrtkama koje otkrivaju i prijavljuju potencijalne prijetnje, zadržavaju informacije i olakšavaju pristup policiji. Doista, OHCHR je u svom izvještaju uočio da je Snowdenovo otkrivanje nadzora dijelom olakšan zbog "strateških odnosa između vlade, regulatorne kontrole privatnosti tvrtki i komercijalnih ugovora.[3]"

POSREDNIČKA ODGOVORNOST I DRŽAVNI NADZOR

Kao što je opisano od strane američkog Centra za Demokraciju i Tehnologiju[4], posredničke odgovornosti odnose se na pravne odgovornosti i odgovornosti koje su na posredniku u odnosu na sadržaj koji hostuje i prenosi preko svojih mreža i platformi. Naime, posrednik je odgovoran kompaniji obzirom na sadržaj koji se od strane vlade i/ili privatnih osoba smatra upitnim, nezakonitim ili štetnim. Centar za Demokraciju i Tehnologiju ističe da se, ovisno o nadležnosti, odredbe posredničke odgovornosti mogu koristiti za kontrolu ilegalnih sadržaja na internetu, ali također mogu biti zloupotrijebljene za kontrolu pravnog sadržaja. Kao što je opisano od strane UK-based članka 19., odredbe koje se odnose na posredničku odgovornost mogu se podijeliti u tri osnovna modela: objektivne odgovornosti, gdje su posrednici u potpunosti odgovorni za sadržaj treće strane; sigurna luka (safe harbour), gdje posrednici mogu osigurati imunitet od odgovornosti u slučaju definiranih zahtjeva; i široki imunitet, gdje je posrednicima dat imunitet za sadržaj treće strane[5]. Kao što je istaknuo Frank La Rue u izvještaju specijalnog izvjestitelja o promociji i zaštiti prava na slobodu mišljenja i izražavanja, pravni okviri koji drže posrednika (a ne pojedinca/ku) odgovornim za sadržaj, prijenose ulogu nadzora interneta na posrednike[6]. Neke jurisdikcije nemaju posebne zakonske odredbe koje se odnose na posredničku odgovornost, ali izdaju sudske ili izvršne uredbe kako bi posrednicima ograničili sadržaj, te obvezujući - uključujući tehničke obveze - pružatelje usluga putem licenci operatera.

Zakonske odredbe i nalozi koji se odnose na posrednu odgovornost nisu uvijek ograničeni na uklanjanje ili onemogućavanje unaprijed definiranog sadržaja. Zahtjevi za uklanjanje sadržaja mogu biti popraćeni zahtjevima o podacima korisnika/ca - uključujući IP adresu i osnovne podatke pretplatnika. Neka zakonodavstva, kao što je Indija, inkorporirali su zadržavanje mandata za skinuti sadržaj i informacije u vezi s tim, u zakonske odredbe, rješavajući na ovaj način odgovornost posrednika.[7] Druga zakonodavstva, kao što su Kina, traže od provider-a da imaju softver za praćenje instaliran na svojim mrežama, prikupljaju i zadržavaju podatke za identifikaciju korisnika/ca, prate i pohranjuju aktivnosti korisnika/ca, prijave ilegalne aktivnosti, i imaju softver za filtriranje radi ograničavanja pristupa zabranjenim web stranicama.[8]

Neka zakonodavstva također priznaju da je tradicionalni način traženja informacija od posrednika neučinkovit i često spor - osobito ako je posrednik strano pravno lice, a pristup informacijama zahtijeva od vlade da slijede proces Ugovora Uzajamne Pravne Pomoći (MLAT).[9] Možda kao odgovor na izazove nadležnosti, neke vlade su tražile "suradnju" s posrednicima kako bi suzbile nelegalan i uvredljiv govor, kao i identificirale počinitelje/ke. Na primjer, 2007. godine u Indiji (Mumbai) policija je pregovarala s Google-om da uspostavi "izravnu liniju kontakta"[10] s tvrtkom, koja bi, prema vijestima, omogućila pristup IP adresama korisnika/ca koji objavljuju "nepoželjan" sadržaja na

[3] Ibid.

[4] https://cdt.org

[5] Article 19. (2013). *Internet Intermediaries: Dilemma of liability.* London: Article 19. www.article19.org/data/files/Intermediaries_ENGLISH.pdf

[6] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[7] The Information Technology (Intermediaries Guidelines) Rules, 2011, Rule 3(4). deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

[8] Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). *Public Strategies for Internet Co-Regulation in the United States, Europe, and China.* Brussels: Université Libre de Bruxelles. www.philodroit.be/IMG/pdf/BF-LH-GL-WP2007-6.pdf

[9] Mutual Legal Assistance Treaties are formal agreements reached between governments to facilitate cooperation in solving and responding to crimes. A critique of the MLAT process has been that it is slow and inefficient, making it a sub-optimal choice for governments when faced with crimes that demand immediate response. For more information see: Kindle, B. (2012, February 14). MLATS are powerful weapons in financial crime combat, even for private sector. *Association of Certified Financial Crime Specialists.* www.acfcs.org/mlats-are-powerful-weapons-in-counter-financialcrime-combat-even-for-private-sector Some intermediaries, such as Facebook, have specified that foreign governments seeking user account data must do so through the MLAT process or letters of rogatory. For more information see: https://en-gb.facebook.com/safety/groups/law/guidelines

[10] Pahwa, N. (2007, March 14). Updated: Orkut to Share Offender Data With Mumbai Police; Google's Clarification. *Gigaom.* gigaom.com/2007/03/14/419-updated-orkut-to-share-offender-data-withmumbai-police-googles-clarifi

Google-ovoj društvenoj stranici Orkut.[11] Takve suradnje kombiniraju elemente posredne odgovornosti i nadzora, a mogu biti sklone zloupotrebi u slučaju propusta, zakonodavnog utemeljenja ili odgovornosti. U tom kontekstu, posrednička odgovornost nije samo o sadržaju na internetu, već obuhvata prikupljanje i objavljivanje podataka vezanih uz taj sadržaj i korisničke produktivnosti i gledanja takvih sadržaja.

VRSTE SADRŽAJA I NADZORNE MJERE

Određene vrste sadržaja - kao što su dječija pornografija/sadržaji za odrasle, nacionalna/cyber sigurnost i autorska prava – mogu nametnuti veće obaveze posrednicima/cama kako bi proaktivno olakšali nadzor i, u nekim slučajevima preuzeli ulogu policije ili pravosuđa. Stupanj do kojeg su takve obaveze potpomognute zakonskim odredbama varira i može biti u rasponu od zakonskih uvjeta, do političkih inicijativa, pa sve do oblika suradnje između vlada, posrednika i samoregulacijske organizacije. Vrste obveza i mjera također se razlikuju.

Prijavljivanje nezakonitog sadržaja: Neke od tih mjera su usmjerene na prijavljivanje ilegalnog ili nedozvoljenog sadržaja. Na primjer, u SAD-u, po zakonu, davatelji usluga moraju prijaviti policiji sve podatke u vezi s dječjom pornografijom. Na to su ovlašteni Zakonom za zaštitu djece od seksualnih predatora, 1998[12]. Isto tako, u Indiji, u skladu s pravilima koja definiraju proceduralne garancije za posrednička odgovornosti, posrednici moraju prijaviti incidente vezane za cyber sigurnost i podijeliti informacije s Indian Computer Emergency Response Team.[13]

Dobrovoljno otkrivanje nezakonitih sadržaja i aktivnosti: Ostale mjere podupiru dobrovoljno otkrivanje i identificiranje nezakonitog sadržaja, aktivnosti i srodnih informacija policiji. Na primjer, po SAD Zakonu o Jačanju Cyber Sigurnosti iz 2002, provedba zakona može potaknuti pružatelje usluga da otkriju podatke koji se odnose na "hitne stvari". Zakon nadalje daje imunitet davatelju usluga ukoliko je objavljivanje napravljeno s dobrom namjerom i uvjerenjem da je riječ o smrti ili ozbiljnoj fizičkoj povredi.[14]

Baze podataka povratnih prijestupnika: Zahtjevi koje pokušavaju da nametnu na pružatelji usluga mogu također biti u izravnom sukobu s njihovim obvezama prema nacionalnim standardima za zaštitu podataka. Na primjer, u kontekstu predloženih zakonskih uvjeta za identifikaciju i sprečavanje kršitelja autorskih prava na temelju Britanskog Zakona o Digitalnoj Ekonomiji, u izjavi za javnost, pružatelj usluga Talk-Talk napominje da je potrebna kompanija za održavanje baze podataka povratnih prijestupnika - akcija koja bi mogla biti protuzakonita po Britanskom Zakonu o Zaštiti Podataka[15] od Jula 2014. godine, davatelji usluga, nositelji prava i vlada su razvili oblik suradnje u kojoj će nositelji prava "pratiti" IP adrese osumnjičenih prijestupnika/ca. Adrese će se dijeliti s britanskim providerima, koji će zatim korisniku/ci poslati niz obavijesti i upozorenja.[16] Ovaj sistem je potencijalno opasan jer omogućuje proaktivno praćenje IP adrese pojedinaca/ca od strane privatnih osoba (nositelja prava), a onda naknadno djelovanje drugog privatnog subjekta (davatelj usluga). Ni u jednom trenutku ovaj sustav ne definira ili ima u vidu zaštitne mjere, odgovornosti i nadzorne mehanizme.[17]

Mjere koje olakšavaju nadzor: Ostali zahtjevi ne nameću izravno obaveze nadzora providerima, ali mogu olakšati nadzor. Na primjer, u Velikoj Britaniji, davatelji usluga moraju sada ponuditi širokopojasne filtere za "sadržaj za odrasle" automatski uključene. Korisnici/ce koji ne žele imati filter su obvezni "isključiti" filter.[18] Te mjere će olakšati praćenje i utvrditi koji korisnik/ca potencijalno gleda "sadržaj za odrasle".

[11] Chowdhury, S. (2014, July 30). Mumbai Police tie up with Orkut to nail offenders. *The Indian Express*. archive.indianexpress.com/news/mumbai-police-tie-up-with-orkut-to-nail-offenders/25427

[12] Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). Op. cit.

[13] Information Technology (Intermediaries Guidelines) Rules 2011, Rule 9. deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

[14] Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). Op. cit.

[15] Jackson, M. (2014, July 19). Update: UK ISPs Agree Voluntary Internet Piracy Warning Letters Scheme. ISPreview. www.ispreview.co.uk/index.php/2014/07/big-uk-isps-agree-voluntary-internetpiracy-warning-letters-scheme.html

[16] Ibid.

[17] Jackson, M. (2013, August 9). UK Government to Finally Repeal ISP Website Blocking Powers. *ISPreview*. www.ispreview.co.uk/index.php/2013/08/uk-government-to-finally-repeal-isp-websiteblocking-powers.html

[18] Miller, J. (2014, July 23). New broadband users shun UK porn filters, Ofcom finds. *BBC*. www.bbc.com/news/technology-28440067

VRSTE POSREDNIKA I MJERE NADZORA

Ovisno o uslugama i nadležnosti, posrednici mogu biti predmet različitih vrste i opsega nadzora. Na primjer:

Internet café: U jurisdikcijama poput Indije[19], cyber kafe-i su suočeni sa zakonskim zahtjevima koji mogu olakšati nadzor - kao što su prikupljanje i zadržavanje identifikacijskih podataka korisnika/ca (osobne karte), pohranjivanje istorije browsera korisnika/ca, i pružanje pomoći u provedbi zakona i drugih tijela kada je potrebno. Cyber kafe-i također strogo podliježu zakonima iz nadležnosti rada.

Davatelji usluga: Na sličan način, davatelji usluga/provideri, čak i kada su multinacionalni, moraju se pridržavati zakona teritorija na kojima rade. Za razliku od posrednika, kao što su multinacionalne društvene mreže ili tražilice, provideri podliježu uslovima licenci koje se odnose na odgovornost posrednika i nadzor. Na primjer, u Indiji, internet i telekomunikacijske usluge su dužne poduzeti "odgovarajuće mjere kako bi se spriječilo da neprihvatljivi, nepristojni, neovlašteni, ili bilo koji drugi sadržaj, poruke ili saopštenja koja povređuju autorska prava, intelektualno vlasništvo i sl. u bilo kojem obliku, budu provedeni na [njihovoj] mreži, u skladu s utvrđenim zakonima zemlje." Osim toga, ukoliko su konkretni primjeri kršenja prijavljeni od strane agencija za provedbu, davatelj usluga mora odmah onemogućiti sadržaj.[20] U slučaju Indije, zahtjevi za pružanje tehničke pomoć u nadzoru i prikupljanju podataka[21] i pretplatničkih informacija također su uključeni u operativne licence za usluge providera.[22]

Društvene mreže: Društvene mreže kao što su LinkedIn, Facebook i Twitter - koje su često multinacionalne kompanije - ne podliježu nužno zakonskim zahtjevima posredničke odgovornost više nadležnosti, ali su često suočene sa zahtjevima i nalozima za podatke o korisniku/ci i zahtjevima za uklanjanje. Za rješavanje tih pritisaka, neke kompanije filtriraju sadržaje u zavisnosti od države. U Junu 2014 LinkedIn je u medijima kritiziran zbog poštivanje naloga iz kineske vlade i filtriranja sadržaja u regionu[23]. Slično tome, Twitter je kritiziran od strane civilnog društva zbog uskraćivanja sadržaja u Rusiji i Pakistanu u maju 2014. godine, iako su u junu 2014. promijenili svoju odluku i vratili obustavljeni sadržaj.[24] 24 Platforme društvenih medija također često i sve više se koriste za provedbu zakona i od strane država za prikupljanje "open source inteligencija".[25]

TEHNOLOGIJA, POSREDNIČKA ODGOVORNOST I DRŽAVNI NADZOR

Kad posrednici provode zakonske uvjete za blokiranje ili filtriranje sadržaja, to čine angažiranjem različitih tehnika i tehnologija, kao što je software za filtriranje ključnih riječi, firewall, skeniranje slika, baze URL podataka, tehnologije koje omogućuju duboku inspekciju data paketa, itd.[26] Na sličan način, poštivanje zakonskih mandata za presretanje ili praćenje komunikacija zahtijeva od posrednika instaliranje i korišćenje tehnologija na svojim mrežama. Kako je istaknuo La Rue, tehnologije korištene za filtriranje također olakšavaju praćenje i nadzor jer imaju sposobnost prepoznavanja i praćenja riječi, slika, web stranica i vrste sadržaja, kao i identificiranje pojedinca/ke koji/a koristi, proizvodi ili je na neki način povezan s istim.[27] Na primjer, YouTube nudi vlasnicima/cama

[19] Information Technology (Guidelines for Cyber Cafe) Rules 2011, Rule 4, Rule 5, Rule 7. ddpolice.gov.in/downloads/miscelleneous/cyber-cafe-rules.pdf

[20] Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 40.3. www.auspi.in/policies/UASL.pdf

[21] Call record details consist of information about a subscriber's use of mobile and broadband networks and can include: called numbers, subscriber name and address, date and time of the start and end of a communication, type of service used (SMS, etc.), international mobile subscriber identity, international mobile equipment identity, location details. For more information see: Afentis Forensics, "Telephone Evidence: Mobile telephone forensic examinations, Billing Records, Cell Site Analysis". afentis.com/telephone-evidence

[22] Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 41.10. www.auspi.in/policies/UASL.pdf

[23] Mozur, P. (2014, June 4). LinkedIn Said it Would Censor in China. Now That It Is, Some Users are Unhappy. *The Wall Street Journal.* blogs.wsj.com/chinarealtime/2014/06/04/linkedin-said-it-wouldcensor-in-china-now-it-is-and-some-users-are-unhappy

[24] Galperin, E., & York, J. (2014, June 23). Twitter Reverses Decision to Censor Content in Pakistan. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/06/twitter-reversesdecision-censor-content-pakistan

[25] Open source intelligence has been widely recognised as an essential tool for law enforcement and security agencies. Open source intelligence is derived from information that is publicly available from sources such as the internet, traditional media, journals, photos, and geospatial information. For more information see: Central Intelligence Agency. (2010, July 23). INTellingence: Open Source Intelligence. *Central Intelligence Agency.* https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[26] Bloxx. (n/d). *Whitepaper: Understanding Web Filtering Technologies.* www.bloxx.com/downloads/US/bloxx_whitepaper_webfilter_us.pdf

[27] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

autorskih prava mogućnost YouTube "identifikacije sadržaja", sistema za upravljanje i identificiranje njihovog sadržaja na platformi. Akcije koje vlasnici/ce autorskih prava mogu odabrati su uključivanje i isključivanje zvuka koji odgovara zaštiti muzičkog/audio sadržaja, blokiranje pregleda videa, pojavljivanje oglasa protiv videa, i praćenje statistike videa. Ove opcije mogu se provoditi na nivou specifičnom za svaku državu.[28]

UKLANJANJE PROVIDER USLUGA IZ NADZORA

Dok neke vlade obavezuju posrednika da pomogne s nadzorom, druge vlade uklanjaju takve obveze sa providera kroz mjere nadzora koje nastoje zaobići same providere i omogućavaju vladi i sigurnosnim agencijama izravno presretanje i pristup informacijama o komunikacijskim mrežama, odnosno mjere koje zahtijevaju od providera da dozvole sigurnosnim agencijama izravnu liniju u svoje mreže. Na primjer, Indija je u procesu implementacija sistema centralnog praćenja koji je predviđen da omogući sigurnosnim agencijama da direktno presreću komunikacije bez pomoći pružatelja usluga. Iako ovaj sistem uklanja obveze sa pružatelja usluga da pomaže i bude uključen u slučajevima nadzora, također otklanja potencijalnu garanciju - gdje davatelji usluga mogu osporiti ili zatražiti izvanzakonski ili neformalni zahtjev za nadzor. U izvještaju o provedbi zakona Vodafona 2014, kompanija bilježi da je u određenim državama, provedba zakona i vlasti imaju izravan pristup komunikacijama pohranjenim na mrežama.[29]

PITANJE NADLEŽNOSTI

Nadležnost i primjenjivost lokalnih zakona je tenzija koja se javlja u kontekstu posredničke odgovornosti i nadzora. Neki aspekti ove napetosti uključuju: U kojoj mjeri se zakonska ograničenja o sadržaju primjenjuju na multinacionalnim platformama koje posluju u zemlji? U kojoj mjeri države mogu pristupiti komunikacijama koje prolaze ili se pohranjuju na njihovom području? I do koje mjere se domaća zaštita osnovnih prava - uključujući i slobodu izražavanja i privatnosti - primjenjuje kako na strance tako i na državljane? OHCHR je u izvještaju Pravo na Privatnost u Digitalnom Dobu bacio novo svjetlo na ova pitanja, oslanjajući se na brojne međunarodne instrumente i čvrsto tvrdeći da svako miješanje u pravo na privatnost mora biti u skladu s načelima zakonitosti, proporcionalnosti i neophodnosti, bez obzira na nacionalnost ili lokaciju pojedinca/.[30] Tenzije oko masovnog nadzora stranih državljana/ki i političkih vođa, i nedostatak pravne konstrukcije u zemlji i inostranstvu za rješavanje tih napetosti, doveli su do pitanja pravca i budućnosti upravljanja Internetom – o kojima se raspravlja na forumima poput NETmundial, gdje su pokrenuta načela koja se odnose na nadzor i posredničku odgovornost.[31] Slično tome, u martu 2014, SAD je saopštila da planira da se odrekne odgovornosti da nadgleda tijelo čiji će zadatak biti regulisanje internet kodova i numeracije sistema. Ovaj potez izazvao je zabrinutost zbog negativne reakcije koja bi mogla dovesti do podjele i odvajanja interneta, olakšavanja masovnog nadzora i kontrole sadržaja.[32]

DRŽAVNI NADZOR I POSREDNIČKA ODGOVORNOST: UTICAJ NA KORISNIKA I ULOGA KOMPANIJE

Vlade su inicirale ograničenja sadržaja i nadzor online komunikacije pojedinaca/ki, a transakcije i interakcije, široko je priznato, imaju negativan uticaj na korisnička prava na privatnost i slobodu govora. U zavisnosti od cilja i razloga, takvi potezi vlada mogu imati dublje implikacije na ljudska prava – ako su, na primjer, meta izdvojena mišljenja, aktivisti i novinari. Težina i jasan uticaj na ljudska prava akcija vezanih za posredničke odgovornosti i nadzor ukazuju na kompleksnost ovih pitanja. Postoje brojni slučajevi pojedinaca/ki koji su bili/e identificirani i proganjani zbog govora online, a identifikaciju tih pojedinaca/ki su olakšale

28 YouTube, "How Content ID Works". https://support.google.com/youtube/answer/2797370?hl=en

29 www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

30 Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age, 30 June 2014. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

31 Powles, J. (2014, April 28). Big Business was the winner at NETmundial. *wired.co.uk*. www.wired.co.uk/news/archive/2014-04/28/internet-diplomacy-netmundial

32 Kelion, L. (2014, April 23). Future of the Internet Debated at NetMundial in Brazil. *BBC*. www.bbc.com/news/technology-27108869

internet kompanije. Na primjer, Yahoo je uveliko kritikovan u međunarodnim medijima za pružanje kineskoj vladi u 2006. godini korisničkih detalja sa nalozima i sadržajem komunikacija političkog disidenta i novinara Shi Tao – omogućavajući policiji da identifikuje i locira Shi, a potom ga i zatvori na deset godina.[33] Slučajevi kao što je slučaj Shi Tao pokazuju složenost pitanja vezanih za posredničke odgovornosti i nadzor i postavljaju pitanje razumnih očekivanja o praksama Internet kompanije i odgovora (posebno multinacionalnih kompanija), adekvatnog nacionalnog zakonodavstva, međunarodnih smjernica, i odgovarajućeg odgovora javnosti. Kako je navedeno u "Pravo na Privatnost u Digitalnom Dobu", "Vodeći principi o privrednim i ljudskim pravima, koja je prihvatio Savjet za Ljudska Prava u 2011. godini, daju globalni standard za sprječavanje i rješavanje negativnih efekata na ljudska prava vezana za poslovne aktivnosti. Odgovornost da se poštuju ljudska prava se primenjuje tokom globalnog poslovanja kompanija, bez obzira na to gdje se korisnici/ce nalaze, i postoji nezavisno od toga da li država ispunjava svoje obaveze u pogledu ljudskih prava." Ovo je visoki standard kojeg se posrednici moraju pridržavati. Neke kompanije kao što su Google[34], Facebook[35], Twitter[36], Vodafone[37], Microsoft[38], Yahoo[39] i Verizon[40] su počeli da rasvjetljavaju količinu zahtjeva za nadzor i kontrolu sadržaja koji su predmet u izvještajima transparentnosti. Kompanije kao što su Vodafone[41], Facebook[42] i Twitter[43] takođe imaju politiku za rješavanje zahtjeva od strane zakonskih nalogodavaca.

ZAKLJUČAK

Kao što je pokazano gore, postoji značajno preklapanje između posredničke odgovornosti, privatnosti i nadzora. Ipak pravni sustavi koji se bave ovim pitanjem odvojeno - često imaju nezavisno zakonodavstvo za zaštitu podataka/privatnosti, posredničke odgovornosti i nadzora. Rezultat je da su sadašnji pravni okviri za posredničke odgovornosti, privatnost i nadzor regulisane modelima koji neobavezno "govore jedni s drugima". Kada su zahtjevi koji olakšavaju nadzor ugrađeni u odredbe koje se odnose na praksu i posredničku odgovornost, postoji rizik da zahtjevi mogu izostaviti ključne zaštitne mjere koje su priznate kao kritične na međunarodnom nivou, uključujući neophodnost, proporcionalnost, zakonitost i legitimni cilj. Kako je La Rue naglasio, i kao što je naglašeno i u drugim međunarodnim izvještajima i forumima, postoji potreba da se vlade preispitaju, ažuriraju i ojačaju zakone i pravne standarde koji se odnose na državni nadzor. Idealno takva obnova će obuhvatiti pravne standarde za posredničke odgovornosti.

Dok su dijalozi više zainteresovanih strana[44] i multilateralnih[45] pregovora rezultirali otezanjem i sporim napretkom, neke odluke Suda Pravde Evropske Unije i Evropskog parlamenta pozivaju na pažnju i napore po ovom pitanju[46].

[33] MacKinnon, R. (2007). *Shi Tao, Yahoo!, and the lessons for corporate social responsibility.* rconversation.blogs.com/YahooShiTaoLessons.pdf

[34] Google Transparency Report. www.google.com/transparencyreport

[35] Facebook Global Government Requests Report. https://www.facebook.com/about/government_requests

[36] Twitter Transparency Report. https://transparency.twitter.com

[37] Vodafone Disclosure to Law Enforcement Report. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

[38] Microsoft's Law Enforcement Request Report. www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency

[39] Yahoo Transparency Report. https://transparency.yahoo.com

[40] Verizon's Transparency Report for the first half of 2014.transparency.verizon.com

[41] Vodafone, Human Rights and Law Enforcement: An Overview of Vodafone's policy on privacy, human rights, and law enforcement assistance. www.vodafone.com/content/index/about/about-us/privacy/human_rights.html

[42] Facebook, Information for Law Enforcement. https://www.facebook.com/safety/groups/law/guidelines/

[43] Twitter Guidelines for Law Enforcement. https://support.twitter.com/articles/41949-guidelines-for-law-enforcement

[44] Powles, J. (2014, April 28). Op. cit.

[45] RT. (2013, October 26). Germany, Brazil enlist 19 more countries for anti-NSA UN resolution. RT. rt.com/news/nsa-un-resolutiontalks-788

[46] Powles, J. (2014, April 28). Op. cit.