Komentar SHARE Defense – SHARE Fondacije na Nacrt zakona o izmenama i dopunama Zakona elektronskim komunikacijama

1. SHARE Defense zahteva preciziranje odredbi koje se odnose na zadržavanje podataka i predlaže izmenu člana 18. koji se odnosi na član 128, preciziranjem osnova pristupa i međunarodnih tehničkih standarda po kojima operatori ispunjavaju obavezu zadržavanja podataka.

SHARE Defense ukazuje na to da je zadržavanje podataka jako intruzivna mera jer zadire u osnovna ljudska prava i slobode. Zbog toga je neophodno da ta mera, kao ograničenje ljudskih prava, bude tretirana kao izuzetak, a ne kao pravilo, u skladu sa standardima koje je Republika Srbija preuzela svojim članstvom u Savetu Evrope i ratifikacijom Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda.

Zadržavanje podataka, koji otkrivaju gotovo sve o učesnicima komunikacije i o samoj komunikaciji, osim sadržaja, omogućava kreiranje "digitalnih profila" građana, potpuno suprotno dostignutom standardu zaštite ljudskih prava (posebno prava na privatnost). "Profilisanjem" (*profiling*) se mogu otkriti veoma osetljive informacije o pojedincima (npr. pripadnost organizacijama, međuljudski odnosi, zdravstveno stanje...). Treba napomenuti da u ostvarivanju ove mere učestvuju operatori i državni organi, pa se tako povećava rizik od zloupotreba i "curenja" podataka o korisnicima posebno u državama poput naše, gde nikada nisu jasno utvrđene procedure zadržavanja i ustupanja ovih podataka.

Nejasne zakonske odredbe mogu u velikoj meri da dovedu do ugrožavanja privatnosti građana, zbog čega je neophodno precizirati odredbe Nacrta zakona i uskladiti ih sa Ustavom Republike Srbije.

SHARE Defense ukazuje i na postupak koji je pokrenut pred Evropskim sudom pravde, u vezi sa inicijativom za ocenu saglasnosti EU Direktive 24/2006 sa Poveljom Evropske unije o osnovnim pravima i slobodama. Nezavisni advokat *(Advocate General)* Kruz Viljalon je nedavno pružio stručno mišljenje o usaglašenosti ova dva evropska dokumenta, našavši da direktiva predstavlja nesrazmerno zadiranje u fundamentalna ljudska prava (pravo na privatnost), navodeći da nije dovoljno da bude ispunjen formalni zahtev da ograničenje ljudskih prava mora da bude propisano zakonom, nego je bitan i kvalitet tog zakona, odnosno kreiranje garancija da ovlašćenje za zadržavanje podataka neće biti zloupotrebljeno. Između ostalog, naročito je apostrofirana "opštost razloga za pristup podacima", to jest, za korišćenje ove mere za potrebe otkrivanja i procesuiranja krivičnih dela, te zaštite javne i nacionalne bezbednosti, zatim neodređenost roka za zadržavanje (od 6 meseci do 2 godine), koji ostavlja dosta veliki prostor za nejednaku primenu u državama članicama i potencijalne zloupotrebe uz pominjanje da zadržavanje podataka ne obavljaju direktno državni

organi nego telekomunikacioni operatori, što još više povećava rizik neovlašćenog pristupa zadržanim podacima.

Iako je ovo mišljenje pravno neobavezujuće za sud, postoje velike šanse da će Direktiva 24/2006 biti odbačena. Postavlja se pitanje da li je opravdano da Srbija istrajava na obavezi zadržavanja podataka, ako je izvesno da će od toga odustati i Evropska unija.

SHARE Defense predlaže da se u predstojećem procesu Skrininga sa Evropskom komisijom postavi i pitanje obaveze zadržavanja podataka, odnosno da se otkloni svaka nedoumica u pogledu toga da li je Srbija uopšte dužna da transponuje Direktivu 24/2006, ako Evropski sud pravde odluči da je protivna Povelji Evropske unije o osnovnim pravima i slobodama.

Dok se ova nedoumica ne otkloni, predlažemo jasnije preciziranje odredaba koje se odnose na zadržavanje podataka, naročito članova 18. i 19. Nacrta zakona o izmenama i dopunama Zakona o elektronskim komunikacijama. Naglašavamo da SHARE Defense u potpunosti podržava stavove koje je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti izneo tokom Centralne javne rasprave o ovom dokumentu. Neophodno je otkloniti sve nedoumice u pogledu ovlašćenja za pristup (osnov i razlozi), obaveza operatora, troškova i perioda na koji se podaci zadržavaju. Takođe, SHARE Defense u potpunosti podržava ideju da se poveća transparentnost procesa uvođenjem obaveze vođenja evidencije za operatore i državne organe koji zadržavaju podatke, kao i stav da ta evidencija mora da bude dostupna javnosti, uz uvođenje prekršajne odgovornosti.

Konkretni predlozi za formulisanje članova o zadržavanju podataka

SHARE Defense predlaže izmenu člana 18. koji se odnosi na član 128, preciziranjem osnova pristupa i međunarodnih tehničkih standarda po kojima operatori ispunjavaju obavezu zadržavanja podataka. Predlažemo da član 128. glasi:

„***Obaveza zadržavanja podataka***

Član 128.

(1) Operator je dužan da zadrži podatke o elektronskim komunikacijama iz člana 129. stav 1. ovog zakona (u daljem tekstu: zadržani podaci).

(2) Pristup zadržanim podacima nije dopušten bez pristanka korisnika, osim na određeno vreme i na osnovu odluke suda, ako je to neophodno radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom.

(3) Operator obavezu zadržavanja podataka iz stava 1. ovog člana ispunjava u skladu sa međunarodnim tehničkim standardima Evropskog instituta za standardizaciju u oblasti telekomunikacija koji se se odnose na zadržane podatke (ETSI LI).

(4) Operator iz stava 1. ovog člana je dužan da zadrži podatke u izvornom obliku ili kao podatke obrađene tokom obavljanja delatnosti elektronskih komunikacija.

(5) Operator iz stava 1. ovog člana nije dužan da zadrži podatke koje nije proizveo niti obradio.

(6) Operator iz stava 1. ovog člana dužan je da zadržane podatke čuva **šest** meseci od dana obavljene komunikacije.

(7) Operator je dužan da zadržava podatke tako da im se bez odlaganja može pristupiti, odnosno da se bez odlaganja mogu dostaviti na osnovu odluke suda, za potrebe iz stava 2. ovog člana.

(8) Operator je dužan da na svojoj Internet stranici objavljuje i redovno ažurira informacije o karakteristikama i vrstama podataka u odnosu na konkretnu vrstu komunikacije, koje zadržava kako bi ispunio obavezu iz stava 1. ovog člana.

(9) Nadležni državni organ koji ostvaruje pristup, odnosno kome se dostavljaju zadržani podaci, dužan je da vodi evidenciju o pristupu, odnosno dostavljanju zadržanih podataka, koja naročito sadrži: određenje sudskog akta koji predstavlja pravni osnov za pristup, odnosno dostavljanje zadržanih podataka, datum i vreme pristupanja, odnosno dostavljanja zadržanih podataka, kao i da ovu evidenciju čuva kao tajnu, u skladu sa zakonom kojim se uređuje tajnost podataka.

(10) Kada nadležni državni organ nije u mogućnosti da ostvari pristup zadržanim podacima bez pristupa prostorijama, elektronskoj komunikacionoj mreži, pripadajućim sredstvima ili elektronskoj komunikacionoj opremi operatora, operator iz stava 1. ovog člana dužan je da o primljenim zahtevima za pristup, odnosno dostavljanje zadržanih podataka, vodi evidenciju, koja naročito sadrži identifikaciju ovlašćenog lica koje je pristupilo zadržanim podacima, odnosno kome su dostavljeni zadržani podaci, određenje akta koji predstavlja pravni osnov za pristup, odnosno dostavljanje zadržanih podataka, datum i vreme pristupanja, odnosno dostavljanja zadržanih podataka, kao i da ovu evidenciju čuva kao tajnu, u skladu sa zakonom kojim se uređuje tajnost podataka.“

Obrazloženje: Predloženim izmenama člana 128. (novi stav 2), preciziraju se razlozi za pristup podacima. Naime, odredbe važećeg člana 128. stav 1. propisuju sledeće razloge za pristup podacima: sprovođenje istrage, otkrivanje krivičnih dela i vođenje krivičnog postupka, kao i zaštita nacionalne i javne bezbednosti Republike Srbije. Ova formulacija je preuzeta iz odgovarajuće evropske direktive, i to Direktive 95/46 koja se odnosi na zaštitu podataka o ličnosti. Način na koji je transponovana u Zakon o elektronskim komunikacijama je prilično sporan. Naime, ova direktiva u članu 13. zaista spominje razloge koji su zapravo izuzeci od garancija u vezi sa zaštitom podataka o ličnosti, koji su ovako opšte formulisani zbog neujednačenosti pravnih sistema država članica u oblasti nacionalne bezbednosti i vođenja krivičnog postupka, pa se svakoj državi članici ostavlja mogućnost da sama formuliše izuzetke od garancija iz direktive. To ne znači da svi ovi razlozi moraju da budu predviđeni konkretnim zakonom, imajući u vidu da citirana odredba direktive ima formulaciju "may" ("može"), a ne "must" ("mora"), što jasno ukazuje da se prilikom transponovanja uzimaju u obzir specifičnosti pravnih sistema država članica. Član 41. stav 2. Ustava Republike Srbije, postavlja uži krug razloga za pristup podacima, i to radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom. Jasno je da naš Ustav ne poznaje institute "otkrivanje krivičnog dela" i ne pravi razliku "javne" i "nacionalne" bezbednosti. Iako se Ustavni sud nije izjašnjavao o ovom pitanju, najsigurnije je prihvatiti sugestiju Poverenika i držati se striktno formulacije iz člana 41. stav 2. Ustava.

Predloženim izmenama člana 128. stava 3. se precizira o kojim se međunarodnim standardima radi. Smatramo da "standardi" koji se pominju u članu mogu biti samo standardi Evropskog instituta za standardizaciju u oblasti telekomunikacija, i to oni iz LI serije (Lawful Interception). Nadležno ministarstvo nije objasnilo koji su standardi u pitanju, pa smatramo da je u interesu pravne sigurnosti neophodno da se navede koji su to tehnički standardi. Takođe, treba imati u vidu da su standardi promenljiva kategorija i da je neophodno da se stalno ažuriraju. Dodatno, ako se odredi obaveza ponašanja po nekom standardu, onda je neophodno da nadležno ministarstvo pokrene proceduru za uvođenje konkretnog standarda u naš pravni sistem (prevođenje na SRPS) u skladu sa propisima koji uređuju standardizaciju.

Predlog za formulaciju novog stava 6. ovog člana predviđa skraćivanje roka u kom su operatori dužni da zadržavaju podatke sa 12 na 6 meseci, imajući u vidu da to omogućava čak i Direktiva 24/2006. Treba napomenuti da zakoni mnogih zemalja u Evropi (EU, EEA, neke zemlje kandidati) predviđaju upravo ovaj rok. Taj rok predviđaju Austrija, Kipar, Litvanija, Luksemburg, Rumunija, Švedska, Lihtenštajn, Norveška i Švajcarska za sve zadržane podatke, odnosno Malta i Holandija za zadržane podatke u vezi sa Internet uslugama. Pitanje ovog roka nije tehničko pitanje nego je upravo u vezi sa procenom srazmernosti mere zadržavanja podataka u odnosu na zaštitu privatnosti korisnika, jer što je duži period zadržavanja, to je veći rizik ugrožavanja privatnosti. Treba napomenuti da je u Litvaniji

postojala zakonska obaveza da operatori zdržavaju podatke koje prenose određeno vreme i čine ih dostupnim bez ikakvih troškova državnim organima. Međutim, Ustavni sud Litvanije je još 2002. godine ovakve odredbe o zadržavanju podataka proglasio neustavnim jer nije bilo vremenskog ograničenja i jer su besplatne. Sud je zato dozvolio operatorima da sami odluče koliko će dugo i u kojem obimu zadržavati podatke.

Predlog za formulaciju novog stava 8. ovog člana je posledica nedovoljno preciziranih vrsta zadržanih podataka. Naime, član 129. Zakona o elektronskim komunikacijama nosi naslov Vrste zadržanih podataka, ali se zapravo radi samo o kriterijumima po kojima se mogu prepoznati zadržani podaci. Javnost bi morala da bude informisana o konkretnim vrstama podataka koje operatori zadržavaju da bi ispunili zakonsku obavezu. Ustavni sud je doneo odluku u kojoj je utvrđeno da se zahtevi u vezi sa zadržanim podacima ne mogu regulisati aktom niže pravne snage od zakona, a to se odnosi i na obim (vrste) zadržanih podataka. Direktiva 24/2006 daje iscrpan spisak svih zadržanih podataka, po svakoj konkretnoj vrsti komunikacije, ali je ona, kao što smo već naveli, upravo i zbog toga sporna. To sve onemogućava da se iscrpni spisak vrsta podataka nađe u Zakonu.

Neophodno je da javnost bude informisana o tome koji se podaci zadržavaju, a logično je da to bude obaveza operatora, koji će na svom sajtu redovno objavljivati koje se vrste podataka zadržavaju za potrebe izvršavanja zakonskih obaveza iz člana 128. stav 1. Na primeru telefonskog saobraćaja, operator bi bio obavezan da objavi da zadržava sledeće podatke: vreme početka poziva, trajanje poziva, vreme kada je poziv okončan, broj sa koga se poziva, broj koji se poziva itd. Ova obaveza bi tako pomogla građanima da steknu uvid u to šta su zapravo zadržani podaci, što trenutno nije moguće zbog opšte formulacije člana 129.

2. SHARE Defense predlaže izmenu člana 130. stava 2. važećeg Zakona o elektronskim komunikacijama koji glasi:

“**(2) Operator je dužan da, radi ostvarivanja obaveze iz stava 1. ovog člana, o svom trošku obezbedi neophodne tehničke i organizacione uslove, kao i da dokaze o tome dostavi Agenciji, u skladu sa odredbama ovog zakona.”**

Član treba da se podeli na dva stava koji glase:

(2) Operator je dužan da, radi ostvarivanja obaveze iz stava 1. ovog člana, obezbedi neophodne tehničke i organizacione uslove, **u skladu sa međunarodnim tehničkim standardima iz člana 128. stav 3. ovog Zakona.**

(2a) Troškove obezbeđivanja tehničkih i organizacionih uslova iz stava 2. ovog člana snose državni organi koji su, u skladu sa zakonima koji uređuju krivični postupak i zaštitu bezbednosti Republike Srbije, ovlašćeni da pristupaju zadržanim podacima na određeno vreme, na osnovu odluke suda, a za potrebe vođenja krivičnog postupka i zaštite bezbednosti Republike Srbije.

Obrazloženje: Smatramo da je obaveza zadržavanja podataka nesrazmerni teret za operatora. Obavezu zadržavanja podataka nameće država imperativnom normom, pa se ne čini opravdanim da troškove tih mera snose operatori, već je neophodno prebaciti ih na državu, odnosno organe koji su ovlašćeni za pristup zadržanim podacima (organi unutrašnjih poslova, bezbednosti i odbrane). Treba napomenuti da je praksa da troškove presretanja i zadržavanja podataka snose državni organi zaživela i u nekim državama Evrope na šta ukazuje i vodeća organizacija u svetu koja se bavi problemima presretnja "SS8" u svom II izdanju "Vodič za zakone o presretanju elektronskih komunikacija". U skladu s tim, u Austriji i Estoniji iako operatori kupuju opremu, imaju pravo na povraćaj novca od države. On se procenjuje u svakom pojedinačnom slučaju, dok u Nemačkoj operatori koji imaju ispod 10.000 pretplatnika nemaju obavezu nabavke opreme, već samo pružanja podrške državnim organima u ovom procesu. Takođe, dosadašnja formulacija, koja je predviđala da operator obezbeđuje neophodne tehničke i organizacione uslove, a dokaze o tome dostavlja Agenciji je jako široka pa nije jasno kakav je karakter ove obaveze. Posebno je sporno što je za neispunjavanje ove (nejasne) obaveze, shodno članu 137. Zakona o elektronskim komunikacijama, predviđena kazna za prekršaj, i to ona najviša (raspon od 1.000.000,00 do 2.000.000,00 dinara) za pravno lice, kao i za odgovorno lice u pravnom licu (raspon od 100.000,00 do 150.000,00 dinara). Zbog toga je neophodno ostvarivanje obaveze vezati za ETSI LI standard, a eventualnu prekršajnu odgovornost preformulisati u tom kontekstu.

3. SHARE Defense u potpunosti podržava stav Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti u pogledu redefinisanja člana 19. koji formuliše novi član 130a Zakona o elektronskim komunikacijama.

Neophodno je informisati javnost o razmerama zadržavanja podataka, uz poštovanje razloga zbog kojih određene informacije ne mogu da budu dostupne. Međutim, javnosti ne treba uskraćivati pravo da sazna one podatke koji nisu i koji ne mogu biti tajni, kao i one čija dostupnost ne predstavlja kršenje garancija vezanih za zaštitu podataka o ličnosti.

SHARE Defense je kao deo nevladinog sektora, posebno zainteresovan da informacije o zadržavanju podataka budu dostupne na najoptimalniji mogući način, posebno imajući u vidu razmere zadiranja u privatnost komunikacije korisnika. Podsetićemo na neverovatan podatak koji je Poverenik izneo posle nadzora nad operatorima mobilne telefonije, gde je utvrđeno da je samo kod jednog operatora

zabeleženo 270.000 samostalnih pristupa. Ovo pitanje treba posmatrati i u kontekstu civilne kontrole službi bezbednosti i njihovog otvaranja ka javnosti. Smatramo da na ovom polju treba zaista još mnogo toga da se uradi, posebno u prepoznavanju uloge NVO sektora, u kome država treba da prepozna partnere, a sve u cilju pronalaženja adekvatnog balansa između zaštite dva legitimna interesa: privatnosti na jednoj i bezbednosti na drugoj strani.

Nije na odmet pomenuti ni nedavnu presudu Evropskog suda za ljudska prava u slučaju *Inicijativa mladih za ljudska prava protiv Srbije*, gde je sud nedvosmisleno podržao stanovište da određeni podaci koji se odnose na rad službi bezbednosti moraju da budu dostupni. Konkretno, reč je o broju prisluškivanih lica. Ova odredba ima za cilj da pruži slične statističke podatke o zahtevima za pristup u toku jedne kalendarske godine. Ponavljamo da je ovu odredbu neophodno preformulisati na osnovu sugestija Poverenika, na sledeći način:

- da se obavežu operatori i organi koji zahtevaju pristup zadržanim podacima da sastavljaju evidencije, a potom ih u određenom roku dostavljaju telu nadležnom za zaštitu podataka o ličnosti;

- da te evidencije sadrže sledeće podatke: o broju zahteva za pristup zadržanim podacima, broju ispunjenih zahteva za pristup zadržanim podacima, vremenu koje je proteklo od dana od kada su podaci zadržani do dana kad je ovlašćeni organ zatražio pristup podacima (kako to stoji u članu 130a);

- da se evidencije učine dostupnim javnosti putem objavljivanja na Internet stranicama operatora, državnih organa i Poverenika, kao tela nadležnog za zaštitu podataka o ličnosti;

- da se predvidi odgovornost za prekršaj za operatora/državni organ koji ne ispuni obavezu sastavljanja i dostavljanja Evidencije, i to najvišom novčanom kaznom (od 1.000.000,00 do 2.000.000,00 dinara), imajući u vidu interes koji se ostvaruje ovim normama.

4. SHARE Defense predlaže brisanje člana 14. Nacrta koji se odnosi na izmenu člana 53. Zakona o elektronskim komunikacijama.

SHARE Defense smatra da je apsolutno nedopustivo i protivno institutu opšteg ovlašćenja da nezavisni regulator iz oblasti elektronskih komunikacija daje prethodnu saglasnost na ugovore o međupovezivanju, budući da nije jasan razlog za uvođenje ove obaveze, a obrazloženje je izostalo. Naime, koja je svrha vođenja registra ugovora o međupovezivanju koji sadrže, između ostalog, i

komercijalne elemente koji su proglašeni poslovnom tajnom? Čini se da je to nesrazmerna obaveza za operatore koja čak ne postoji ni u našem neposrednom okruženju (Crna Gora i Mađarska).

Drugo, obaveza se odnosi na sve ugovore o međupovezivanju, ne samo one o međunarodnom međupovezivanju. Kakav je interes agencije da vodi registar o ugovorima o međupovezivanju i koji javni interes se time štiti? Zaštitne odredbe u odnosu na interkonekciju imaju smisla samo ako dominantni operatori zloupotrebljavaju svoj položaj na tržištu i uskraćuju međupovezivanje tom zloupotrebom. Ipak, to je pitanje zaštite konkurencije, i to ex post regulacije, po Zakonu o zaštiti konkurencije i ex ante, u pogledu pravila o operatoru sa ZTS.

Treba posebno napomenuti da RATEL potpuno protivzakonito, tri godine od usvajanja Zakona o elektronskim komunikacijama, primenjuje **Pravilnik o uslovima i postupku izdavanja odobrenja javnom telekomunikacionom operatoru za povezivanje domaće telekomunikacione mreže sa telekomunikacionom mrežom druge države**, koji uređuje uslove i postupak izdavanja odobrenja za povezivanje domaće telekomunikacione mreže sa telekomunikacionom mrežom druge države. Podsećamo da je kategorija odobrenja ukinuta stupanjem na snagu Zakona o elektronskim komunikacijama i da se od tada sve usluge elektronskih komunikacija pružaju po režimu opšteg ovlašćenja, dok je obaveza pribavljanja dozvole ostala samo u pogledu dozvole za korišćenje radio-frekvencija i dozvole za numeraciju. To su jedine dve situacije u kojima Zakon o elektronskim komunikacijama predviđa prethodnu odluku Agencije u upravnom postupku. Uvođenje instituta “saglasnosti” je vraćanje korak unazad, odnosno pokušaj vraćanja “na mala vrata” odobrenja i licenciranja i to bez jasnih razloga i opravdanja. Naime, međupovezivanje je takođe usluga elektronskih komunikacija (koja se pruža u veleprodaji), koja ni u čemu nije specifična u odnosu na ostale usluge, pa ne postoji opravdanje za drugačiji pravni režim.

Ovaj pokušaj zakonopisca se može tretirati kao legalizacija bespravnog stanja koje je postojalo usled neusklađenosti pomenutog pravilnika i Zakona o elektronskim komunikacijama, s tim što se čak i šire postavlja, jer se odnosi i na usluge domaćeg i na usluge međunarodnog međupovezivanja.

Zbog toga SHARE Defense insistira da se sporna odredba Nacrta zakona o elektronskim komunikacijama izbriše, a da se sporni pravilnik stavi van snage, imajući u vidu da je u suprotnosti sa aktom veće pravne snage – zakonom, što ukazuje i na njegovu potencijalnu neustavnost.

5. SHARE Defense predlaže da se u ovaj zakon unesu odredbe Direktive 2009/136/EC kojima se uvode izmene i dopune Direktive 2002/58 godine, a u vezi sa zahtevima koji se odnose na pohranjivanje podataka u terminalnoj opremi korisnika i/ili pristupu već pohranjenim podacima (cookies provision), i to dopunama člana 118. Zakona o elektronskim komunikacijama koji se odnosi na nezatražene poruke.

Odredbe člana 5(3) Direktive 2009/136/EC (cookie provision) se odnose na obaveze država članica EU da obezbede da se pohranjivanje informacija ili pristup već pohranjenim informacijama o korisniku uredi na takav način da korisnici za to daju svoj prethodni informisani pristanak u skladu sa zahtevima Direktive 95/46. Ova obaveza se odnosi, između ostalog i na "kolačiće" (cookies), i druge dodatke (tehnologije) koji se koriste za praćenje navika korisnika na Internetu. Internet pretraživači instaliraju bez znanja korisnika takve dodatke, da bi potom ti dodaci beležili informacije o navikama korisnika na Internetu (najčešće se beleže podaci o početku i trajanju sesije, broju poseta određenom sajtu, drugim sajtovima koji se posećuju, IP adresa korisnika itd). Ovi podaci se potom koriste za potrebe targetiranog odnosno personalizovanog marketinga, što je, ako ne postoji pristanak, nedozvoljena obrada podataka o korisniku i posredno ugrožavanje njegove privatnosti.

Zbog toga je neophodno precizirati da korisnici Interneta, pri poseti nekom portalu, moraju biti informisani o postojanju "kolačića" (cookies) ili drugih tehnologija podobnih za praćenje korisnika, njihovim vrstama i nameni, uz pružanje mogućnosti korisniku da pristane na takvu obradu svojih podataka i uz mogućnost da taj pristanak naknadno povuče (*opt-in* i *opt-out*). Ovde se zapravo radi o implementaciji specifičnih pravila u vezi sa zaštitom podataka o ličnosti u oblasti informaciono-komunikacionih tehnologija *(Notice and Consent System)*. Ove obaveze se ne odnose na instaliranje dodataka u svrhu pružanja usluge koju je zahtevao sam korisnik (apsolutno neophodni kolačići), ali čak i tada bi mogla postojati obaveza za pružaoca usluge da informiše korisnika o dodacima koji se instaliraju da bi se usluga normalno pružala (na primer, apsolutno neophodni kolačići bez kojih neki Internet sajt ne bi radio).

Predlažemo da se član 118. Zakona o elektronskim komunikacijama dopuni novim stavovima 4, 4a, 4b i 4c koji glase:

"(4) Lica koja koriste kolačiće (cookies) ili slične tehnologije za praćenje korisnika, radi obrade tih podataka (na primer beleženja, kasnijeg pristupa tim podacima prosleđivanja trećim licima i sl), dužna su da korisnika obaveste najmanje o:

1. postojanju kolačića (cookies) ili sličnih tehnologija za praćenje korisnika;
2. podacima o korisniku koji se obrađuju korišćenjem kolačića ili drugih tehnologija za praćenje korisnika;
3. svrsi obrade podataka o korisniku;
4. licima koji imaju pristup tim podacima.

(4a) Lica iz stava 4. ovog člana, dužna su da korisnicima omoguće da daju prethodni informisani pristanak na obradu podataka iz stava 4. ovog člana *(opt in)* ili da takav pristanak naknadno povuku *(opt out).*

(4b) Ako korisnici ne pristanu na obradu njihovih podataka, ili ga naknadno povuku, lica iz stava 4. ovog člana su dužna da se uzdrže od obrade tih podataka, odnosno dužna su da prestanu sa obradom već prikupljenih podataka, a da do tada prikupljene podatke su dužni da izbrišu, odnosno učine neprepoznatljivim.

(4c) Stavovi 4-4a ovog člana se ne primenjuju na kolačiće ili druge slične tehnologije koje su neophodne za pružanje usluge koju je korisnik sam zahtevao (apsolutno neophodni kolačići i slične tenologije), ali su lica iz stava 4. ovog člana dužna da korisnika obaveste o postojanju ovakvih kolačića i sličnih tehnologija za praćenje korisnika.“

6. SHARE Defense predlaže da se jasno definiše šta se podrazumeva pod obavezom operatora iz člana 37. stav 2. tačka 15)

Ova odredba zakona govori o obavezi operatora da primenjuje mere za sprečavanje i suzbijanje zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga. Zakon ne definiše na koje se ovo zloupotrebe i prevare odnosi, a to ne precizira ni Pravilnik o opštim uslovima za obavljanje delatnosti elektronskih komunikacija po režimu opšteg ovlašćenja, koji predviđa da je operator dužan da, u skladu sa propisima, primeni odgovarajuće tehničke i druge mere, u cilju sprečavanja zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga. Smatramo da su citirane odredbe Zakona i Pravilnika nejasne i preširoke i da daju mogućnost arbitrarnog tumačenja šta se podrazumeva pod zloupotrebom i prevarom.

Naime, radi se naime o pravnim kategorijama, čije tumačenje ne može biti prepušteno nezavisnom regulatoru iz oblasti elektronskih komunikacija, nego sudu. Još spornija je definicija iz pravilnika koji neodređeno upućuje na „propise“. Smatramo da smisao Direktive 2002/20 o autorizaciji mreža i usluga elektronskih komunikacija, sa kojom je ovaj zakon usklađen, nije bio da se upušta u pravne kvalifikacije zloupotreba i prevara, nego da utvrdi odgovarajući tehnički standard koji će omogućiti najveći mogući stepen zaštite elektronske komunikacione mreže od prevara i zloupotreba koje se odnose na elektronsku komunikacionu uslugu a ne na sadržaj komunikacije. Nažalost, u praksi se upravo dešavalo da su se razni državni i nedržavni entiteti obraćali operatorima sa zahtevom za filtriranje/blokiranje sadržaja. Najpoznatiji je primer Uprave za igre na sreću koja je pre par godina zahtevala od pružalaca usluga Interneta da blokiraju pristup listi sajtova za onlajn klađenje, pozivanjem na odredbe Zakona o igrama na sreću koji propisuje da se igre na sreću mogu organizovati samo na osnovu prethodno pribavljene dozvole. Međutim, taj zakon nije imao odredbu koja daje ovlašćenje za blokiranje/filtriranje, pa zahtev nije bio osnovan. U toj situaciji je moglo da se desi da neki operatori, zbog nejasne odredbe Zakona o elektronskim komunikacijama, poslušaju Državnu lutriju Srbije, što bi predstavljalo zapravo nesrazmerno zadiranje u pravo na slobodu izražavanja, i to zbog nejasnog regulatornog okvira. Podsećamo da za blokiranje sadržaja mora da

postoji jasno ovlašćenje u zakonu, da je mera srazmerna cilju koji treba da postigne i neophodna u demokratskom društvu.

Predlažemo da se član 37. stav 2. tačka 15) isključivo odnosi na prevare i zloupotrebe u vezi sa pružanjem usluga elektronskih komunikacija (na primer Bypass), bez ikakvog ulaženja u sadržaj koji se prenosi elektronskim signalom (što bi moralo da bude predmet drugih zakona, na primer Zakona o elektronskoj trgovini, budućeg Zakona o informacionoj bezbednosti i sl), tako da glasi:

“**15) primene tehničke standarde u cilju sprečavanja i suzbijanja zloupotreba i prevara u vezi sa korišćenjem elektronskih komunikacionih mreža i usluga, bez ulaženja u sadržaj koji se korišćenjem tih mreža/usluga prenosi;”**

Vladan Joler

SHARE Defense – SHARE Fondacija

U Novom Sadu,

20. 12. 2013.

ADDRESS: ZARKA ZRENJANINA 10/7 **PHONE:** +381648236421 **MAIL:** INFO@SHARECONFERENCE.NET **WEB:** WWW.SHARECONFERENCE.NET
PIB: 1074657125 / **MATICNI BROJ:** 28825323