Prof. dr Predrag Dimitrijević
Pravni fakultet u Nišu

PRAVO PRIVATNOSTI NA INTERNETU
(pozitivnopravni okvir)

Apstrakt

Internet je globalna kibernetska informaciona mreža u kojoj učestvuju mnogi subjekti kao korisnici različitih informacija. U tom globalnom virtuelnom interaktivnom komunikacijskom prostoru, razmenjiju se različite informacije pa se postavljaja pitanje bezbednosti i integriteta tih podataka, autentičnost, odnosno identitet korisnika, kao i potvrda prijema i slanja podataka. Podaci koji se nalaze u kibernetskom prostoru mogu biti ugroženi od strane raznih pojedinaca ili pravnih lica, institucija ali i državnih organa. Da bi se ti podaci zaštitili države donose razne zakonske i podzakonske akte kojima se pruža zaštita podataka ali istovremeno se legalizuje kontrola podataka, odnosno ničim kontrolisano prikupljanje i obrada podataka na Internetu od strane državnih organa.

Ključne reči: Internet, sajber pravo, pravo privatnosti, podaci o ličnosti.

1. Cyberspace i pravo

Milioni ljudi širom sveta koriste Internet za prikupljanje informacija, razna istraživanja, finansije i korespondenciju a da pri tom i ne pomisle koliko su pravna pitanja povezana i sastavni deo elektronske komunikacije i trgovine. Internet kao produkt novih informacionih tehnologija sustinski menja način rada i komuniciranja u svim oblastima zivota. Prisiljeni smo da nove informacione tehnologije koristimo za uspešnije i kvalitetnije obavaljanje poslova. Internet daje svakome mogućnost da ima svoj website, jednaku mogućnost na objavljivanje teksta, svako može emitovati svoju informaciju, stav ili mišljenje širom sveta, bez potrebe da predhodno ide do izdavača nekog časopisa i slično. S druge strane, mnoge vlade reaguju na informacije sa Interneta tako što kontrolišu i website i one koji pristupaju Internetu.

Internet je mreža kompjuterskih mreža, koalicija svih svetskih mreža (Internet Society).[1] Internet je globalni elektronski komunikacioni sistem međusobno povezanih računarskih mreža i uređaja, namenjen razmeni svih vrsta informacija u skladu sa Internet standardima**.** Internet standardi su dokumenti koji se odnose na koncepte, procedure umrežavanja, protokole, interfejse i metode identifikacije u okviru Interneta.[2] Samo ime Internet dolazi od pojma među mreža ("inter-networking") gde su više kompjuterskih mreža povezane zajedno. Preko Interneta se odvija biznis arena, elektronska pošta (e-

[1] **G. R. Ferrera, S. D. Lichtestein, M. E. K. Reder, R. August, W. T. Schiano**, *Cyberlaw,Your Rights in Cyberspace*, Thomson Learning, Canada, 2001, web: http://www.thomsonrights.com

[2] Internet standarde, pod nazivom *Request For Comments* (RFC) donosi međunarodna organizacija *Internet Engineering Task Force* (IETF).

mail), transfer fajlova i čatovanje (chat rooms), dok se trgovina i pouzdani protok informacija odvija posredsvom globalne svetske mreže (World Wide Web - www). Zajedno oni čine svet kibrernetskog prostora (world of cyberspace) gde pravna pitanja i problemi počinju da enormno rastu, a među njima su privatnost i bezbednost.

Kako Pravo reaguje i odgovara na nove tehnologije? Široko je rasprotranjena povreda autorskih prava od strane onih koji preuzimaju i kopiraju materijale sa drugih websajtova ili nečijih knjiga, članaka i sl. i prezentuju ih kao svoje bez pismene dozvole nosilaca autorskih prava (autora). Regulisanje problema zaštite autorskih prava i pitanja zaštite privatnosti na Internetu predstavljaju samo neke od oblasti koje sajber pravo reguliše.

Sajber prostor karakteriše brisnje fizičkih, političkih i socijalnih granica. Nove granice, jedino mogu biti domeni koji su definisani tehničkim karakteristikama. Naziv domena **(**domain name system **- DNS**) koji je uveden 1984**,** je globalno jedinstvena tekstualna oznaka koja povezuje skup računara, uređaja i servisa na Internetu u jedinstvenu administrativno-tehničku celinu. Domeni mogu zauzeti mesto granica u kibernetskom prostoru u tradicionalnom smislu. [3]

Svaka država pokušava da zakonima i podzakonskim aktima reguliše ponačanje na Internetu a koji ne može da se ograniči na državne granice. Nacionalne vlade ne mogu da obuzdaju mogućnosti sajber prostora, baš zbog prirode globalne tehnologija. Kibernetskim prostorom putuju različite informacije a pri tome autori tih različitih sadržaja nemaju mogućnost kontrole nad upotrebom i širenjem svojih dela na Internetu. Zbog neverovatne lakoće kojom se digitalni materijal može kopirati i slati, zakon bi trebalo da zaštiti autore od takvog kopiranja pisanog materijala, muzike, grafičkih dela, softvera. Međutim, postoji i mišljenje da javnost treba da slobodno raspolaže ovakvim sadržajima, na isti način na koji je tradicionalno raspolagala kopijama knjiga, muzike i ostalih autorskih dela.

Korisnicima Interneta[4] je, zbog njegovog multinacionalnog karaktera, omogućeno da izbegnu primenu propisa koji im ne odgovaraju. Ponekad, to znači težnju ka popustljivijim propisima, odnosno izbegavanje propisa; ali ukoliko je to pogodnije, i težnju ka striktnijim propisima. Tačnije, veb-sajt lako može biti smešten van jurisdikcije granica države (nacije) i tako ne bude limitiran njenim zakonima. Ovo off-shore pravosuđe sa minimumom pravnih propisa može pretvoriti Internet u raj za kockanje i ostale radnje koje su zabranjene na drugim mestima.[5]

2. **Zakon o telekomunikacijama**

Sadrži brojne odredbe ali izdvojićemo one koje se tiču privatnosti i bezbednosti

---

[3] Ipak, granice u sajber prostoru su još uvek povezane sa stvarnim efektima u fizički ograničenom stvarnom prostoru. Zato je jedan od najvećih teorijskih izazova sajber prava da prepozna, artikuliše i opiše obim i ulogu ovih prostora. **Ana Marković**, *Zakonska regulativa i Internet* (http://e-trgovina.co.yu/pravo/zakonska_regulativa1.html, stranica poslednji put posećena 08.12.2008.), Beograd, 2008.

[4] *Korisnik Interneta* je fizičko ili pravno lice koje koristi Internet usluge i/ili ostale usluge prenosa podataka po osnovu zaključenog ugovora ili na drugi predviđeni način.

[5] Pitanje je na koji način se donose odluke, u nedostatku kolektivnog internacionalnog tela i da li postoji prostor za konsenzus između strana. Da li će pojedinačni, ili kolektivni postupci potisnuti nacionalnu i internacionalnu regulativu?

informacija a one su smeštene u delu koji propisuje "ostale obaveze javnih telekomunikacionih operatora" (član 54. i 55.). U tom smislu, uzećemo u obzir poslednji stav člana 54. po kome je Javni telekomunikacioni operator dužan da nadležnim državnim organima omogući pristup i analizu podataka o saobraćaju koji se odnose na pojedinačne korisnike i koji se obrađuju radi uspostavljanja veza, a koje inače po zakonu javni telekomunikacioni operator može u čuvati i obrađivati samo u obimu koji je neophodan za ispostavljanje računa korisniku i iste može dostaviti samo pošiljaocu i primaocu poruka.

Drugo, (član 55) Zakon izričito zabranjuje sve aktivnosti ili korišćenje uređaja kojima se *ugrožava* ili *narušava privatnost i poverljivost poruka* koje se prenose telekomunikacionim mrežama, osim kada postoji *saglasnost korisnika*[6] ili ako se ove aktivnosti vrše u *skladu sa zakonom* ili *sudskim nalogom* izdatim u skladu sa zakonom. Pri tome se ne kaže kojim zakon, jer to evidentno nije ZoT. Takođe, zakon obavezuje operatora da kao deo sistema, o sopstvenom trošku, oformi podsisteme, opremu i instalacije za *zakonom ovlašćeni elektronski nadzor* određenih telekomunikacija. Pri tome, tzv. "tehničke uslove" za ove podsisteme, uređaje, opremu i instalacije definiše Agencija (RATEL), u saradnji sa telekomunikacionim operatorima i *državnim organima nadležnim za neposredno sprovođenje elektronskog nadzora*.

3. **Tehnički uslovi za Internet mreže**

Na osnovu *Zakona o telekomunikacijama*[7] i *Statuta Republičke agencije za telekomunikacije*[8], Republička agencija za Telekomunikacije (RATEL),[9] donela je *Tehničke uslove za podsisteme, uređaje, opremu i instalacije internet mreže* (11.07.2008. godine). Ovim se opštim pravnim aktom definišu tehnički uslovi za podsisteme, uređaje, opremu i instalacije za zakonom ovlašćeni nadzor određenih telekomunikacija koje su javni telekomunikacioni operatori (mrežni operatori, pružaoci usluga i pružaoci pristupa) dužni, da kao deo sistema oforme o sopstvenom trošku. Elektronski nadzor se vrši za potrebe nadležnih državnih organa. Da bi se taj nadzor mogao da sprovede *javni telekomunikacioni operatori* se obavezuju da:

- uredno vode i ažuriraju sve baze podataka svih zakupljenih linija i veza,
- omoguće direktan pristup i uvid u baze podataka,
- omogući direktan uvid u evidencije o smetnjama na telekomunikacionom uređajima[10] i prekidima telekomunikacionog saobraćaja,
- da uklone kriptozaštitu pre dostavljanja sadržaja komunikacije nadležnom državnom organu,

---

[6] To je tzv. "obrada sa pristankom" podataka. *Zakon o zaštiti podataka o ličnosti*, Službeni list 97/2008, član 10. Pristanak se može opozvati, pa je u tom slučaju "obrada podataka" *nedozvoljena* posle opoziva pristanka (član 11).

[7] "Službeni glasnik RS" br. 44/03 i 36/06, član 55. stav 3.

[8] "Službeni glasnik RS" broj 78/05, član 18. tačka 7.

[9] **Dejan Šuput**, *Republička agencija za telekomunikacije*, Pravni život, br. 10, Beograd, 2008, str. 807.

[10] Telekomunikacioni podsistemi, uređaji, oprema i računarski sistemi smeštaju se u prostorijama državnog organa (ovlašćenog) za elektronski nadzor i/ili u posebnim prostorijama u okviru telekomunikacionih centara. Ove prostorije obezbeđuju i opremaju javni telekomunikacioni operatori, po zahtevu i tehničkim propisima nadležnog državnog organa.

- da na zahtev nadležnog državnog organa dostavi podatke o svim komunikacionim sredstvima koja su se pojavljivala na određenoj geografskoj, fizičkoj ili logičkoj lokaciji u minimalnom periodu od poslednjih 48 časova, nezavisno od postojanja telekomunikacione aktivnosti.

Pružalac Internet usluga je dužan da nadležnim državnim organima omogući:

- pristup ažurnoj bazi podataka o pretplatnicima i *na zahtev* dostavlja *eksportovanu bazu podataka*.[11]

- pristup ažurnoj bazi podataka o korisnicima elektronske pošte,

- upoznaje ih o načinu zaštite podataka o korisnicima,

- imenuje, uz saglasnost državnih organa osobu za kontakt i komunikaciju sa njima,

- u realnom vremenu potpuno autonomni pasivni monitoring,

- internet aktivnosti proizvoljnog pretplatnika i preusmeravanje dolaznog i odlaznog saobraćaja ka akvizicionom centru nadležnog državnog organa,

- odnosno obezbedi hardver i softver za pasivni monitoring u realnom vremenu, servisa elektronske pošte i preusmeravanje sadržaja pošte ka akvizicionom centru nadležnih državnih organa.

- obezbedi hardver i softver za monitoring saobraćaj između proizvoljnog pretplatnika, preko pružaoca Internet usluga, prema trećem Internet provajderu.

- da ne stvara tehničkih mogućnosti kojima bi svi navedeni podaci postali dostupni trećoj strani.

Hardver i softver, koji obezbeđuje pružalac Internet usluga, treba da omoguće: pasivni monitoring Internet aktivnosti u realnom vremenu; prikupljanje i analizu statistike Internet aktivnosti; presretanje elektronske pošte, pridruženih sadržaja (attachment) i obradu Web mail-a; presretanje IP telefonskog saobraćaja, faksimila i IP video saobraćaja; presretanje IM (instant messenger) saobraćaja; presretanje saobraćaja na peer-to-peer mrežama, konstrukciju presretnutog saobraćaj do nivoa aplikacije i filtriranje po: korisničkom imenu ili korisničkom telefonskom broju, adresi elektronske pošte, IP adresi i IM (instant messenger) identifikaciji.

Na osnovu iznete regulative može se opravdano koonstatovati da pod maskom navodnih "tehničkih uslova za Internet mreže" u Srbiji se uvodi do sada nezabeleženi masovni i ničim ograničeni *nadzor i arhiviranje* svih oblika elektronskih komunikacija za potrebe službe bezbednosti. Mišljenje je da čak ni u najgora vremena nije se pravila ovakva regulativa. Indikativno je i to da je agencija RATEL kao nezavisno regulatorno telo i donosilac ovog normativnog akta, istom dala retroaktivno dejstvo, odnosno dejstvo pre objavljivanja jer u ovom dokumentu stoji da tzv. "tehnički uslovi" stupaju na snagu narednog dana od dana donošenja, a to znači pre formalnog objavljivanja. Na osnovu svega došlo je i do stavljanja van snage ovog opšeg akta RATEL-a.

4. **Pravilnik o Internetu**

[11] Baza treba da sadrži: lične podatke iz ugovora sa pretplatnikom i vrstu usluga, informaciju o postojanju zaštite prenosa podataka, način pristupa pretplatnika, maksimalnu brzinu prenosa podataka i identifikacione adrese,

Na osnovu *Zakona o telekomunikacijama*[12] Republička agencija za telekomunikacije donela je *Pravilnik o uslovima za pružanje internet usluga i ostalih usluga prenosa podataka i sadržaju odobrenja* (23.09.2008),[13] kojim se utvrđuju tehnički uslovi za pružanje Internet usluga i ostalih usluga prenosa podataka (propisivanje obrazaca, način izdavanja i sadržaj odobrenja i dr.).

"Internet usluge" su javne telekomunikacione usluge prenosa podataka koje se realizuju u skladu sa Internet standardima a za čije ostvarivanje je neophodna upotreba *javnih IP adresa*[14], osim komercijalnih usluga prenosa govora, radio i televizijskih programa u realnom vremenu.[15] Za pružanje Internet usluga moraju biti ispunjeni osnovni tehnički uslovi u skladu sa preporukama i standardima međunarodnih organizacija, a naročito: IETF, ITU, ETSI, IEEE, CEN/CENELEC, ISO, IEC i opštim aktima Agencije.

Agencija izdaje odobrenje za pružanje Internet usluga licu koje je registrovano za telekomunikacionu delatnost, koje je Agenciji podnelo prijavu za registraciju i koje ispunjava zakonom propisane uslove.[16]

Imalac odobrenja je dužan da u skladu sa svojim tehničkim mogućnostima obezbedi Usluge svim zainteresovanim korisnicima, bez bilo kakve diskriminacije (princip jednakosti i nesikriminacije).

Imalac odobrenja je dužan da obezbedi poverljivost i bezbednost svojih usluga, podataka o korisnicima svojih usluga i zabranjeno mu je da koristi ili pruža informacije trećim licima o sadržaju, činjenicama i uslovima prenosa poruka, izuzev minimuma koji je neophodan za pružanje usluga ili u slučajevima predviđenim zakonom.

Imalac odobrenja ne može vršiti bilo kakve ograničenja pristupa uslugama na osnovu nacionalnog, rasnog, verskog, političkog, teritorijalnog ili bilo kojeg drugog kriterijuma, koji bi mogao dovesti do kršenja ljudskih prava i osnovnih sloboda.

Imalac odobrenja ne sme uspostaviti monopol bilo kog oblika, zaključujući ugovore sa drugim pružaocima telekomunikacionih usluga.

On je dužan da obezbedi uređaje, opremu i instalacije koje će u razumnoj meri garantovati zaštitu podataka pretplatnika i onemogućiti zloupotrebu od strane trećih lica.

Nadležni organ vrši kontrolu nedozvoljenog sadržaja. Ukoliko nadležni organ konačnom odlukom naloži imaocu odobrenja, da ukloni sadržaj za koji je ustanovljeno da je nedopušten, uvredljiv, štetan, ili da krši zaštićena autorska prava, imalac odobrenja je dužan da bez odlaganja postupi prema takvoj odluci.

Imalac odobrenja za pružanje Internet usluga je obavezan da u granicama svojih tehničkih mogućnosti korisniku omogući zaštitu od neželjene elektronske pošte i/ili štetnih sadržaja.

---

[12] "Službeni glasnik RS", br. 44/03 i 36/06, član 38. st. 5, 6. i 9.

[13] Republička agencije za telekomunikacije (RATEL) je ovim posebnim opštim aktom (pravilnikom) regulisala komercijalno pružanje usluge prenosa govora, radio i televizijskih programa u realnom vremenu. Danom stupanja na snagu ovog pravilnika prestao je da važi *Pravilnik o uslovima za pružanje Internet usluga i sadržaju odobrenja* („Službeni glasnik RS", broj 60/06").

[14] *Javna IP adresa* je numerički identifikator, koji jednoznačno identifikuje mrežu ili pristupnu tačku u sklopu Interneta, a za čij e je dodeljivanje na svetskom nivou nadležna organizacija Internet Assigned Numbers Authority (IANA).

[15] "Ostale usluge" prenosa podataka su javne telekomunikacione usluge koje se realizuju pomoću uređaja za prenos podataka koji su priključeni na javnu telekomunikacionu mrežu, i za čije ostvarivanje se ne koriste javne IP adrese.

[16] *Zakon o telekomunikacijama*, "Službeni glasnik RS", br. 44/03 i 36/06.

On je dužan da ugovorom odnosno opštim uslovima obaveže korisnike na zabranu slanja neželjene pošte i štetnih sadržaja. U slučajevima slanja neželjene pošte ili štetnih sadržaja, povrede prava intelektualne svojine, imalac odobrenja je u obavezi da uputi pisano upozorenje korisniku. Ukoliko korisnik nastavi sa slanjem neželjene pošte, štetnog sadržaja ili povrede prava intelektualne svojine imalac odobrenja može da prestane sa pružanjem usluge tom korisniku.

Agencija ne snosi odgovornost za nastanak bilo kakve materijalne ili druge vrste štete nanete pretplatniku odnosno korisniku, prouzrokovane korišćenjem usluga imaoca odobrenja (npr. neželjena pošta - „spam", virusi, „phishing", i dr).

5. Zakon o zaštiti podataka o ličnosti[17]

Ovim zakonom se uređuju uslovi za prikupljanje i obradu podataka o ličnosti[18], prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka i nadzor nad izvršavanjem zakona.

1. Zaštita podataka o ličnosti obezbeđuje se svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva. Poslove zaštite podataka o ličnosti obavlja *Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti*, kao samostalan državni organ, nezavisan u vršenju svoje nadležnosti. On je uspostavljen sa ciljem da, u vezi sa obradom podataka o ličnosti,[19] svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda.

Međutim, ***zakon ne primenjuje na obradu svih podataka.*** Odredbe ovog zakona ne primenjuju se na obradu određene grupe podataka sem ukoliko "očigledno pretežu suprotni interesi lica". To su sledeće grupe podataka: podaci dostupni svakome (javna glasilia i publikacije, arhive, muzeji), porodični i lični podaci koji nisu dostupni trećim licima, zatim, podaci o članovima političkih stranaka i drugih oblika udruživanja, koji se obrađuju od tih organizacija, ali dok traje članstvo, i podataka koje je lice samo objavilo o sebi, a ono je sposobno da se samo stara o svojim interesima.

Svi drugi podaci koji se prikupljaju i obrađuju u druge svrhe mogu da se obrađuju

---

[17] Službeni list 97/2008. Odredbe ovog zakona primenjuju se na svaku automatizovanu obradu, kao i na obradu sadržanu u zbirci podatka koja se ne vodi automatizovano.

[18] *Podatak o ličnosti* je svaka informacija koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i sl), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije (neposredno, putem slušanja, gledanja i sl, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl), ili bez obzira na drugo svojstvo informacije

[19] *Obrada podataka* je svaka radnja preduzeta u vezi sa podacima kao što su: prikupljanje, beleženje, prepisivanje, umnožavanje, kopiranje, prenošenje, pretraživanje, razvrstavanje, pohranjivanje, razdvajanje, ukrštanje, objedinjavanje, upodobljavanje, menjanje, obezbeđivanje, korišćenje, stavljanje na uvid, otkrivanje, objavljivanje, širenje, snimanje, organizovanje, čuvanje, prilagođavanje, otkrivanje putem prenosa ili na drugi način činjenje dostupnim, prikrivanje, izmeštanje i na drugi način činjenje nedostupnim, kao i sprovođenje drugih radnji u vezi sa navedenim podacima, bez obzira da li se vrši automatski, poluautomatski ili na drugi način .

isključivo u istorijske, statističke ili naučnoistraživačke svrhe, ako ne služe donošenju odluka ili preduzimanju mera prema određenom licu uz obezbeđivanje odgovarajućih mera zaštite.[20]

2. Zakon navodi izričito situacije u kojima *obrada podataka* (ali ne i prikupljanje) nije dozvoljena, i to ako:

1) fizičko lice nije dalo pristanak za obradu ili se obrada vrši bez zakonskog ovlašćenja;

2) se vrši u svrhu različitu od one za koju je određena, bez obzira da li se vrši na osnovu pristanka ili zakonskog ovlašćenja;

3) svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili je već ostvarena;

4) je lice na koje se podaci odnose, određeno ili odredivo i nakon što se ostvari svrha obrade;

5) je način obrade nedozvoljen;

6) je podatak koji se obrađuje nepotreban ili nepodesan za ostvarenje svrhe obrade;

7) su broj ili vrsta podataka koji se obrađuju nesrazmerni svrsi obrade;

8) je podatak neistinit i nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili je zastareo.

Postoji izričita *zabrana automatske obrade* određene vrste podataka. Tako, odluka koja proizvodi pravne posledice ili pogoršava njegov položaj nekog lica, ne može biti isključivo zasnovana na podacima koji se obrađuju automatizovano i koji služe oceni nekog njegovog svojstva (radne sposobnosti, pouzdanosti, kreditne sposobnosti i sl), sem kada je to zakonom izričito određeno, odnosno kada se usvaja zahtev lica u vezi sa zaključenjem ili ispunjenjem ugovora, uz sprovođenje odgovarajućih mera zaštite. U tom slučaju lice mora biti upoznato sa postupkom automatizovane obrade i načinom donošenja odluke.

Ono što je posebno interesantno je taksativno navođenje situacija kada je obrada podataka dopuštena *ex lege* iako nema pristanka, tzv "***obrada bez pristanka***". Obrada bez pristanka je dozvoljena:

1) da bi se ostvarili ili zaštitili životno važni interesi lica (život, zdravlje i fizički integritet);

2) u cilju izvršenja zakonskih obaveza ili obaveza određenih aktom donetim u skladu sa zakonom;

3) u drugim (pod) zakonskim slučajevima, radi ostvarenja pretežnog opravdanog interesa lica, rukovaoca ili korisnika.

Obrada podatke bez pristanka lica od strane organa vlasti vrši se ako je obrada neophodna u cilju ostvarivanja interesa nacionalne ili javne bezbednosti, odbrane zemlje, sprečavanja, otkrivanja, istrage i gonjenja za krivična dela, ekonomskih, odnosno finansijskih interesa države, zaštite zdravlja i morala, zaštite prava i sloboda i drugog

[20] Mere zaštite podataka koji se arhiviraju u isključivo istorijske, statističke ili naučnoistraživačke svrhe uređuju se posebnim propisom.

javnog interesa, a u drugim slučajevima na osnovu pismenog pristanka lica.

3. Zakon pravi razliku između "obrade" podataka i "prikupljanja" podataka. U tom smislu što kaže da se podaci prikupljaju od *lica na koje se odnose*,[21] od *organa uprave* koji su ovlašćeni za prikupljanje i od *drugog lica* ako:

1) je to predviđeno *ugovorom* zaključenim sa licem na koje se podaci odnose;

2) je to propisano *zakonom* ili drugim propisom;

3) je to neophodno s obzirom na *prirodu posla*;

4) prikupljanje podataka od samog lica zahteva prekomerni utrošak vremena i sredstava;

5) se prikupljaju podaci radi ostvarenja ili zaštite životno važnih interesa lica na koje se odnose, posebno života, zdravlja i fizičkog integriteta.

Zakon uvodi posebnu kategoriju podataka koji se zovu "***naročito osetljivi podaci***" u koju spadaju: podaci koji se odnose na nacionalnu pripadnost, rasu, pol, jezik, veroispovest, pripadnost političkoj stranci, sindikalno članstvo, zdravstveno stanje, primanje socijalne pomoći, žrtvu nasilja, osudu za krivično delo i seksualni život. Ovi podaci imaju poseban zakonski režim prikupljanja i obrade. Ovi "naročito osetljivi podaci" su posebno zakonom zaštićeni jer se mogu obrađivati isključivo *na osnovu* ***slobodno datog pristanka*** *lica*. Zakon ih posebno štiti jer uvodi još jedan stepen zaštite kada propisuje da se zakonom može *zabraniti* obrada ovih naročito osetljivih podataka iako je i dat pristanak.[22]

Izuzetno, podaci o političkoj pripadnosti, zdravstvenom stanju i socijalnoj pomoći, mogu se obrađivati i bez pristanka lica, ako je to zakonom dopušteno.

6. Umesto zaključka

Ova sumarna analiza pozitvnopravnih rešenja otvara brojna pitanja. Pitanje je, koji su to državni organi nadležni da vrše elektronski nadzor privatnih podataka, koji su to slučajevi kada zakon dopušta elektronsku kontrolu, kako mogu pojedinci zaštititi svoju privatnost od e-nadzora ili monitoringa u "zakonom dopuštenim sistuacijama". U tom kontekstu, da li je zakon o zaštiti privatnosti u Srbiji i podzakonska regulativa RATELA-a doneta upravo u suprotnom cilju da legalizuju administrativnu kontrolu privatnosti. To je osetljivo pitanje granica državne kontrole i prava privatnosti u virtuelnoj stvarnosti.

---

[21] Rukovalac koji podatke prikuplja od *lica na koje se odnose*, odnosno od *drugog lica*, pre prikupljanja, upoznaće lice na koje se podaci odnose, odnosno drugo lice o svom identitetu, svrsi prikupljanja i dalje obrade, načinu korišćenja podataka, obaveznosti i pravnom osnovu, odnosno dobrovoljnosti davanja podataka i obrade i dr. *Obaveza obaveštavanje o obradi* ne postoji kada takvo upoznavanje, s obzirom na okolnosti slučaja, nije moguće ili je očigledno nepotrebno, odnosno neprimereno, a naročito ako je lice na koje se odnose podaci, odnosno drugo lice već upoznato sa time ili ako lice na koje se podaci odnose nije dostupno.

[22] Zakon poznaje instituciju "opoziva pristanka" za obradu naročito osetljivih podataka, u kom slučaju, lice koje je dalo pristanak dužno je da rukovaocu naknadi opravdane troškove i štetu, u skladu sa propisima o odgovornosti za štetu, osim ako je drukčije određeno u izjavi o pristanku.

Prof. dr Predrag Dimitrijević

RIGHT TO PRIVACY ON THE INTERNET

Abstract

Internet is a global cybernetic information network in which many subjects participate as users of different information. In that global virtual communication space different information are exchanged and that creates a question of security and integrity of the data, authenticity, user's identity, as well as confirmation of receipt and sending of data. Data found in the cybernetic space can be endangered by various individuals or legal entities, institutions and government bodies. To protect the data, states make various laws and legislation that provides data protection, but at the same time they legalize control of data, and not controlled collection and processing of data on Internet by state authorities. The question is, which authorities can control private data, which are cases when the law allows electronic control, how individuals can protect their privacy from e-surveillance or monitoring in the "situations allowed by law". In particular, the question is whether the laws on the protection of privacy bring in the opposite order to legalize the administrative control of privacy. It is a sensitive issue of boundaries of state control and privacy in virtual reality.

Keywords: Internet, cyber law, the right to privacy, personal data.