Ljuba Slijepčević

Pravosudna akademija

Novi Sad

Privatnost i zaštita podataka o ličnosti kroz domaće i međunarodno pravo s osvrtom na korisnike Fejsbuka i interneta sa krivičnopravnog aspekta

Uvod

Pravo na privatnost je lično pravo svakog pojedinca koje je prisutno u pravnoj nauci od davnina. Pravo na privatnost je s vremenom dobijalo sve veći obim, i sada obuhvata sve aspekte privatnog i porodičnog života, uključujući i zaštitu psihičkog i fizičkog integriteta, zaštitu doma i prepiske, imena i identiteta lica, zaštitu od nedozvoljenog prikupljanja podataka o ličnosti, kao i slobodu da pojedinci žive život po svom nahođenju.

Države imaju obavezu da poštuju ovo lično pravo, koje mogu da ograniče jedino u slučajevima kada je to u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih.

Član 42. stav 2. Ustava Republike Srbije propisuje da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuje zakonom. U Srbiji su podaci o ličnosti definisani Zakonom o zaštiti podataka o ličnosti . Tako u ovom zakonu član 3, tačka 1 stoji:

"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 slično, 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 slično, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i slično ili bez obzira na drugo svojstvo informacije -podatak.

Pravo na poštovanje privatnog i porodičnog života garantovano je brojnim međunarodnim pravnim instrumentima usvojenim pod okriljem Ujedinjenih nacija. Član 12 Univerzalne deklaracije propisuje da niko ne sme biti izložen proizvoljnom mešanju u njegovu privatnost, porodicu, dom ili prepisku, niti napadima na čast ili ugled. Prema članu 8 Evropske konvencije o ljudskim pravima i osnovnim slobodama

"1)Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.

2) Javna vlast se ne meša u uživanje ovog prava, osim ako je takvo mešanje predviđeno zakonom, i ako je to nužna mera u demokratskom društvu, u interesu nacionalne sigurnosti, javne sigurnosti i ekonomske dobrobiti zemlje, sprečavanja nereda ili sprečavanja zločina, zaštite zdravlja i morala, ili zaštite prava i sloboda drugih."

Član 8 štiti privatni život pojedinaca od arbitrarnog mešanja javnih vlasti i privatnih organizacija poput medija. Navedeno pravo pokriva četiri oblasti: privatni život, porodični život, dom i prepisku. Zbirni naziv za zaštitu prava na privatni i porodični život, nepovredivost doma i prepiske, kao i časti i ugleda pojedinca je pravo na privatnost -prava privatnosti. Član 8 nameće dve vrste obaveza državama: "negativnu" obavezu da se uzdrže od mešanja u bilo koja od prava navedenih u članu 8 st 1 osim ako nisu ispunjeni uslovi iz člana 8 st 2, i "pozitivnu" obavezu da se preduzmu koraci u cilju zaštite privatnih života pojedinaca, posebno od mešanja od strane drugih.

Kada je u pitanju zaštita podataka o ličnosti, definicija prava na privatnost je u međunarodnim dokumentima postavljena široko i neophodno je utvrditi konkretnu vezu između privatnosti i zaštite podataka o ličnosti.

Visok nivo zaštite podataka o ličnosti je garant prava na privatnost svakog pojedinca, što je jedno od osnovnih ljudskih prava. Poznavanjem i poštovanjem zakona uspostavljaju se norme funkcionisanja društva u oblastima koje su često vrlo kompleksne, posebno pod uticajem informaciono komunikacionih tehnologija i njihovog brzog razvoja i prodiranja u sve oblasti života.

Zaštita podataka o ličnosti garantuje da će podaci biti sakupljani i čuvani savesno, kao i da neće biti zloupotrebeljni, odnosno da postoji zakonski lek u slučaju nesavesnog, štetnog postupanja sa podacima, kao i njihovom zloupotrebom.

Cilj zakona, međutim, nije sama zaštita podataka o ličnosti, već zaštita pojedinca na koga se ti podaci odnose, a time i dela njegove takozvane informacijske privatnosti.

Rizici zloupotrebe podataka o ličnosti:

Krađa identiteta.

Iako krađa identiteta nije u Srbiji rasprostranjena u istoj meri koliko u zapadnoj Evropi, Australiji ili Americi, i u Srbiji postoji mnogo vrsta prevara, a i prevaranta, koji mogu zloupotrebiti tuđe podatke o ličnosti za sopstvenu korist.

Zloupotreba podataka o ličnosti u komercijalne svrhe: neovlašćena prodaja ili ustupanje podataka o ličnosti i navika na internetu. Neželjeni mejlovi (spam) pripadaju ovoj kategoriji.

Maltretiranje u virtuelnom svetu

U pravu Srbije krivičnopravna zaštita podataka o ličnosti pruža se inkriminisanjem neovlašćenog prikupljanja ličnih podataka, a posredno se štite lični podaci inkriminisanjem određenih dela kao što su proganjanje, neovlašćeno otkrivanje tajne, neovlašćeno prisluškivanje i snimanje, neovlašćeno fotografisanje, neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka. .

Autori naročitu pažnju posvećuju krivičnim delima visokotehnološkog kriminala i opisuju različite vrste zloupotreba podataka o ličnosti i prava na privatnost korišćenjem interneta, sa naglaskom na pravo na zaštitu privatnosti dece.

Visok nivo zaštite podataka o ličnosti je garant prava na privatnost svakog pojedinca, što je jedno od osnovnih ljudskih prava. Poznavanjem i poštovanjem zakona uspostavljaju se norme funkcionisanja društva u oblastima koje su često vrlo kompleksne, posebno pod uticajem informaciono komunikacionih tehnologija i njihovog brzog razvoja i prodiranja u sve oblasti života.

Podaci o ličnosti su svi oni podaci koji se odnose na neko određeno ili odredivo fizičko lice, na osnovu kojih ono može biti identifikovano, a kojima se može ugroziti njegova privatnost. To su, pre svega, podaci kojima se mogu ugroziti život, telesni i fizički integritet, čast, ugled, život porodice, identitet i ime. Ti podaci se odnose na živa, umrla lica, kao i lica proglašena umrlim.

Zaštita podataka o ličnosti je jedan od najznačajnijih i najdelikatnijih problema sa kojima je suočeno moderno društvo. Sve veća dostupnost podataka dovodi do povećanja mogućnosti njihove zloupotrebe. Zloupotreba je korišćenje podataka u nedozvoljene i nelegitimne svrhe, odnosno svaki događaj vezan za podatke zbog kojih je subjekat pretrpeo ili mogao da pretrpi gubitak. Podatci o ličnosti: lično ime i prezime, jedinstveni matični broj građana (poznatiji kao JMBG),kućna adresa,poreski broj,broj zdravstvenog osiguranja,broj telefona (fiksnog i mobilnog),broj lične karte,broj pasoša,broj studentskog indeksa i sl.

Osim ovoga, pod podacima o ličnosti podrazumevaju se i druga obeležja poput starosti, zaposlenja, funkcija koje lice obavlja, položaja i statusa u okvirima određenih subjekata (privrednih, institucionalnih i slično). U podatke o ličnosti spadaju i podaci o DNK, otisci prstiju, otisci ušiju i mrežnjače oka, slika i glas, kao i druge biometrijske odlike po kojima neko može biti identifikovan.

U osetljive podatke o ličnosti spadaju: nacionalna pripadnost,rasa,pol,jezik,veroispovest,pripadnost političkoj stranci,sindikalno članstvo,zdravstveno stanje,primanje socijalne pomoći,status žrtve nasilja,osuda za krivično delo,seksualni život.

Domaći pravni okvir zaštite podataka o ličnosti

Kada je pravo na privatnost i zaštitu podataka o ličnosti u pitanju reguliše ih član 42. Ustava Republike Srbije [1]. U st 1 navodi Član 42 da je Zajemčena zaštita podataka o ličnosti a u st 2 propisuje da se prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuje se zakonom. U Srbiji je je zakonski okvir za zaštitu podataka o ličnosti ustanovljen tek 2008. godine, usvajanjem Zakona o zaštiti podataka o ličnosti (u daljnjem tekstu ZZPL). Pre usvajanja ovog zakona već je postojao Zakon o zaštiti podataka o ličnosti koji je Savezna Republika Jugoslavija usvojila još 1998. godine, koji nikada nije primenjen u praksi. Treba imati u vidu da sam Ustav Republike Srbije jemči zaštitu podataka o ličnosti u članu 42 st 3, koji propisuje da je zabranjena i kažnjiva "upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom", kao i da Ustav u st 4 čl 42

[1] USTAV REPUBLIKE SRBIJE ("Sl. glasnik RS", br. 98/2006 i 115/2021)

navodi “svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti, u skladu sa zakonom, i pravo na sudsku zaštitu zbog njihove zloupotrebe.”

Zakon o zaštiti podataka o ličnosti[2](u daljnjem tekstu ZZPL) uređuje uslove za prikupljanje i obradu podataka o ličnosti, prava lica i zaštitu prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidenciju, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog zakona (član 1. ZZPL-a). Ovaj zakon definiše obradu, rukovaoce podataka, zbirke podataka, korisnike podataka, prava korisnika podataka, obaveze rukovaoca i sl. Cilj ovog zakona, određen u članu 2, je da, u vezi sa obradom podataka o ličnosti, svakom fizičkom licu obezbedi ostvarivanje i zaštitu prava na privatnost i ostalih prava i sloboda.

Republika Srbija je takođe potpisala i ratifikovala Konvenciju Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti u septembru 2005. godine , koja je u odnosu na RS stupila na snagu 1. januara 2006, a u oktobru 2008. potpisala je i ratifikovala Dodatni protokol uz Konvenciju 108 u vezi sa nadzornim organima i prekograničnim protokom podataka

Prema Zakonu o zaštiti podataka o ličnosti, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti nadzire sprovođenje Zakona i ima pravo da ukaže na uočene zloupotrebe kod obrade podataka.

Zakon takođe uspostavlja centralnu ulogu Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti -Poverenik, kao nazavisnog državnog organa, nadležnog da u drugostepenom postupku obezbeđuje zaštitu iz oblasti zaštite podataka o ličnosti, kao i nadležnog za sprovođenje nadzora nad primenom Zakona.

Važno je napomenuti da cilj Zakona „nije sama zaštita podataka o ličnosti, već zaštita pojedinca na koga se ti podaci odnose, a time i dela njegove takozvane informacijske privatnosti. ZZPL ne pokriva čitav spektar prava na privatnost pojedinca, već samo onaj deo prava na privatnost koji se odnosi na njegove podatke o ličnosti.“

Zakon definiše podatak o ličnosti kao svaku informaciju „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.

Prema odredbama o uslovima za obradu podataka iz čl.8-18. Zakona o zaštiti podataka o ličnosti obrada podataka o ličnosti, koja, između ostalog, podrazumeva i prikupljanje i korišćenje podataka, nije dozvoljena bez zakonskog ovlašćenja ili bez izričitog pristanka lica čiji podaci se obrađuju. Takođe, obrada podataka je dozvoljena samo u svrhu određenu

[2] ZAKON O ZAŠTITI PODATAKA O LIČNOSTI ("Sl. glasnik RS", br. 87/2018)

zakonom ili pristankom lica, pri čemu broj i vrsta podataka koji se obrađuju moraju biti srazmerni svrsi obrade. Obrada je nedozvoljena ako je sam način obrade nedozvoljen.

Za obradu naročito osetljivih podataka u smislu čl. 16-17. Zakona, u koje, između ostalih, spada i podatak o nacionalnoj pripadnosti, Zakon zahteva i strožije uslove. Ovi podaci se mogu obrađivati na osnovu slobodno datog pristanka lica, osim kad zakonom nije dozvoljena obrada ni uz pristanak. Uslovi za obradu naročito osetljivih podataka su strožiji i u pogledu forme i sadržine pristanka za obradu, u tom smislu da se pristanak lica daje u pismenom obliku koji sadrži oznaku podatka koji se obrađuje, svrhu obrade i način njegovog korišćenja.

Elektronska komunikacija jeste masovni i umreženi sistem elektronskih komunikacionih odnosa u kome se prenose i obrađuju razne elektronske informacije između, po pravilu, neograničenog broja subjekata. Elektronska komunikacija funkcioniše kao umreženi sistem protoka informacija.

Elektronska komunikacija je sistemski pravno regulisana specijalnim Zakonom o elektronskim komunikacijama. Jedan od važnih ciljeva i načela regulisanja odnosa u oblasti elektronskih komunikacija je i načelo obezbeđivanja visokog nivoa zaštite podataka o ličnosti i privatnosti korisnika, a u skladu sa Zakonom o zaštiti podataka o ličnosti i drugim zakonima. Zakon u delu kojim reguliše dostavljanje podataka i zaštitu tajnosti podataka izričito propisuje da je operater dužan da na zahtev Agencije za elektronske komunikacije, dostavi sve podatke neophodne za obavljanje poslova Agencije, a naročito one koji su potrebni za zaštitu podataka o ličnosti i privatnosti korisnika , podatke za procenu bezbednosti i integriteta ekomunikacione mreže. U tom smislu Agencija je dužna da sarađuje sa organima i organizacijama nadležnim za zaštitu podataka o ličnosti (Poverenik).

Nadzor nad sprovođenjem i izvršavanjem ovog zakona Poverenik vrši preko ovlašćenih lica – inspektora. U vršenju nadzora ovlašćeno lice postupa na osnovu saznanja do kojih je došao po službenoj dužnosti, od strane podnosioca žalbe ili trećeg lica.

Prema odredbama čl.53.Zakona, za iznošenje podataka o ličnosti iz Republike Srbije u državu koja nije članica Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka Saveta Evrope, ili međunarodnu organizaciju u toj državi, potrebna je saglasnost odnosno dozvola Poverenika.

Isto tako, zainteresovana lica mogu podneti žalbu Povereniku. Ako su o nezakonitoj obradi podataka o ličnosti obavestili policiju, policija može sama da inicira prekršajni postupak ili da obavesti Poverenika, te da on pokrene prekršajni postupak. Zakon predviđa novčane kazne .

Krivični zakonik Republike Srbije [3]propisuje krivična dela protiv bezbednosti računarskih podataka .Tužilaštvo za visokotehnološki kriminal je nadležno za krivično gonjenje počinioca dela propisana ovom glavom KZ-a, ali i za gonjenje lica koja su u izvršenju drugih krivičnih dela (npr. protiv polnih sloboda) koristila računarsku mrežu.

Krivičnopravna zaštita podataka o ličnosti u Srbiji započeta je Krivičnim zakonikom iz

[3] KRIVIČNI ZAKONIK ("Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)

2005. godine koji u grupi krivičnih dela protiv sloboda i prava čoveka i građanina predviđa posebno delo neovlašćeno prikupljanje ličnih podataka. Domaće zakonodavstvo nije prepoznalo potrebu za inkriminisanjem radnji neovlašćenog postupanja sa ličnim podacima sve do 2005. godine iako je zaštita ličnih podataka zagarantovana još Ustavom Republike Srbije iz 1990. godine.

Zakonodavac je predvideo dva osnovna oblika krivičnog dela Neovlašćeno prikupljanje ličnih podataka u st. 1. i 2. člana 146. i jedan kvalifikovani oblik u st. 3. ovog člana.

Ovo krivično delo ima blanketni karakter s obzirom na to da je za njegovo potpuno razumevanje neophodno imati u vidu odredbe drugih zakona.. Zakon o zaštiti podataka o ličnost je zakon koji treba imati u vidu prilikom analize ovog krivičnog dela.

Osnovni oblik krivičnog dela Neovlašćeno prikupljanje ličnih podataka postoji kada učinilac podatke o ličnosti, koji se prikupljaju,obrađuju i koriste na osnovu zakona, „neovlašćeno pribavi, saopšti drugom ili upotrebi u svrhu za koju nisu namenjeni" (član 146. stav 1. KZ).

Drugi osnovni (posebni) oblik čini onaj „koprotivno zakonu prikuplja podatke o ličnosti građana ili tako prikupljene podatke koristi"(član 146. stav 2. KZ).

Za oba oblika je propisana novčana kazna ili zatvor do jedne godine. Oba oblika se gone po privatnoj tužbi, a ne po službenoj dužnosti. Ova činjenica ukazuje na to da je krivičnopravnoj zaštiti dat sekundaran značaj.

Krivični zakonik zapravo upućuje na Zakon o zaštiti podataka o ličnosti, s obzirom na to da pomenuti zakon reguliše obradu ličnih podataka na zakonom dozvoljen način. Po ovom zakonu, obrada ličnih podataka je svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima, kao što su prikupljanje,beleženje, razvrstavanje, grupisanje, odnosno strukturisanje, pohranjivanje, upodobljavanje ili menjanje, otkrivanje, uvid, upotreba, otkrivanje prenosom, odnosno dostavljanjem, umnožavanje, širenje ili na drugi način činjenje dostupnim, upoređivanje, ograničavanje, brisanje ili uništavanje.

Zakon o zaštiti podataka o ličnosti propisuje načela koja se moraju poštovati prilikom obrade podataka. Obrada podataka mora biti zakonita, poštena i transparentna, zatim ograničena u odnosu na svrhu koja se njom želi postići, ograničena samo na one podatke koji su zaista neophodni i koji moraju biti zaštićeni i čuvani samo onoliko vremena koliko je to potrebno za ostvarivanje svrhe obrade. Obrada podataka je zakonita, u skladu sa načelom zakonitosti, samo ako je ispunjen jedan od sledećih uslova: ako je lice na koje se podaci o ličnosti odnose pristalo na obradu svojih podataka o ličnosti za jednu ili više posebno određenih svrha, ako je obrada neophodna za izvršenje ugovora zaključenog sa licem na koje se podaci odnose ili za preduzimanje radnji, na zahtev lica na koje se podaci odnose, pre zaključenja ugovora, zatim ako je obrada neophodna u cilju poštovanja pravnih obaveza rukovaoca.

Takođe, obrada je zakonita ako je neophodna u cilju zaštite životno važnih interesa lica nakoje se podaci odnose ili drugog fizičkog lica,zatim ako je neophodna u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca ili ako je neophodna u cilju ostvarivanja legitimnih interesa rukovaoca ili treće strane, osim ako su nad timinteresima pretežniji interesi ili osnovna prava. Objekat krivičnog dela su lični podaci.

Definicija ličnih podataka je data u Zakonu o zaštiti podataka o ličnosti koji propisuje da je lični podatak svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što su ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog,ekonomskog, kulturnog i društvenog identiteta.prava ili slobode lica na koje se podaci odnose koji zahtevaju zaštitu podataka o ličnosti, a posebno ako je lice na koje se podaci odnose maloletno lice. Lični podaci koji su premet obrade moraju biti tačni, jer ukoliko nisu, radilo bi se o nekom drugom krivičnom delu. Zakon o zaštiti podataka o ličnosti[4],

Delo je svršeno preduzimanjem određene radnje izvršenja, pri čemu nije potrebno da su usled toga nastupile i neke štetne posledice za lice o čijim ličnim podacima se radi.

Što se tiče krivice izvršioca, kao subjektivnog elementa dela, potreban je umišljaj.

Analiza krivičnopravnih normi kojima se štiti pravo na zaštitu podataka o ličnosti treba da obuhvati sva relevantna krivična dela,čijom radnjom izvršenja može biti primarno povređeno ovo pravo.

Osim dela iz KZ člana 146, to su i: neovlašćeno otkrivanje tajne (član 141);proganjanje (član 138a stav 1. tačka 3), povreda tajnosti pisma (član 142); neovlašćeno prisluškivanje i snimanje (član 143); neovlašćeno fotografisanje (član 144) i neovlašćeno objavljivanje i prikzivanje tuđeg spisa, poretreta i snimka (član 145); pa i krivično delo iznošenja ličnih i porodičnih prilika (član) neovlašćeno prikupljanje ličnih podataka (član 146), prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (član 185), iskorišćavanje računarske mreže ili komunikacije drugim tehničkimsredstvima za izvršenje krivičnog dela protiv polne slobode prema maloletnom licu (član185b), falsifikovanje i zloupotreba platnih kartica (član 243), kao i druga krivična dela gde se koriste računari za izvršenje.

slobode), iako su i ona, u širem smislu, namenjena i zaštiti ličnih podataka.

Krivična dela visokotehnološkog kriminala

Izuzetno brz napredak tehnologije, pored velikih prednosti koje donosi u gotovosvim oblastima života, doneo je i nove oblike krivičnih dela, kao i nove načine izvršenja ranije postojećih krivičnih dela. Reagujući na ovakve pojave u zakonodavstvima definišu se nova krivična dela i preduzimaju različite mere u borbi protiv ove vrste kriminala.

[4] Zakon o zaštiti podataka o ličnosti, („Službeni glasnik RS”, br. 87/18), čl. 3. st. 1. tač. 3).

Lični podaci na internetu mogu se grupisati u tri kategorije:[5]

1.Aktivni digitalni tragovi – podaci (o sebi ili drugima) koje sami korisnici ostavljaju

prilikom korišćenja interneta, obično svesno, mada ne nužno i namerno (npr. prilikom

kupovine nekih proizvoda, preuzimanja nečega sa interneta, postavljanja fotografija, otvaranja profila na nekoj društvenoj mreži);

2.Pasivni digitalni tragovi – podaci koje korisnici ostavljaju na internetu prilikom njegovog korišćenja, uglavnom nesvesno (npr.,putem tzv. kolačića, otisaka prstiju, podataka o lokaciji, korišćenja pametnih stvari i pametnih igračaka);

3.Podaci dobijeni analizom prve dve kategorije podataka pomoću algoritama (kroz proces profilisanja), eventualno u kombinaciji sa drugim izvorima podataka.

Brojne lične informacije mogu biti skrivene u fotografijama ili video-sadržajima koje postavljamo na internet (npr., datum rođenja, broj telefona).

Dela visokotehnološkog kriminala spadaju u nadležnost Posebnog tužilaštva za borbuprotiv visokotehnološkog kriminala i Odeljenja za suzbijanje visokotehnološkog kriminala,specijalizovane jedinice policije unutar Službe za borbu protiv organizovanog kriminala(SBPOK). To su dve glavne institucije koje se bave ovim poslovima i koje su najvažnije u celom tom procesu.

Pregled međunarodnih principa i regulative zaštite podataka o ličnosti i privatnosti ličnosti

Zaštita podataka o ličnosti i privatnosti ličnosti regulisana je sledećim propisima:

Univerzalna deklaracija UN o ljudskim pravima iz 1948. godine je deklaracija Generalne skupštine Ujedinjenih nacija.[6] Iako pravno neobavezujuća, ova deklaracija predstavlja deo običajnog prava i sadrži principe i odredbe koje svaka država treba da garantuje. Pravo na privatnost propisano je u članu 12. koji glasi "Niko se ne sme izložiti proizvoljnom mešanju u privatni život, porodicu, stan ili prepisku, niti napadima na čast i ugled. Svako ima pravo na zaštitu zakona protiv ovakvog mešanja ili napada."

Konvencija o pravima deteta Ujedinjenih nacija[7] u članu 16.kaže da „nijedno dete neće biti izloženo proizvoljnom ili nezakonitom mešanju u njegovu privatnost, porodicu, dom ili prepisku, niti nezakonitim napadima na njegovu čast i ugled"

[5] https://www.mingl.rs/rubrike/informisi-se/495/4937/licni-podaci-na-internetu---kako-da-ih-zastitis.html

[6] Generalna skupština Ujedinjenih nacija je donela i proglasila Opštu deklaraciju o pravima čoveka 10. decembra 1948.

[7] Usvojena i otvorena za potpisivanje i ratifikovanje ili pristupanje rezolucijom Generalne skupštine Ujedinjenih nacija 44/25 od 20. novembra 1989. Stupila na snagu 2. septembra 1990. (Službeni list SFRJ -Međunarodni ugovori br. 15/1990).

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda doneta je u okviru Saveta Evrope , u Rimu, 4. novembra 1950. godine. Pravo na privatnost zagarantovano je članom 8.

"Kako se pravo na privatnost zapravo definše putem zabrane njegova kršenja, mehanizmi za zaštitu ljudskih prava tražili su njegov sadržaj upravo kroz ispitivanja načina i mehanizama za kršenje.Evropski sud za ljudska prava (ESLJP)utvrdio je da se sadržaj prava na privatnost odnosi i na komunikaciju e-poštom, videopozivima i internetskim chatom, a u određenim slučajevima i na metapodatke. Naime sustavi za masovni nadzor često sakupljaju metapodatke (metadata), koji predstavljaju podatke o komunikacijama (npr. podatke o datumu, lokaciju i brojeve, odnosno adrese osoba koje stupaju u kontakt, bez sadržaja same komunikacije), ali ne i sam sadržaj komunikacije. ESLJP je stava da u određenim slučajevima prikupljanje meta podataka samo za sebe ne predstavlja kršenje prava na privatnost s obzirom na to da merenje tih podataka nije isto što i presretanje sadržaja tih podataka, ali da daljnje deljenje i prosleđivanje tih podataka može predstavljati kršenje prava na privatnost zajamčenog članom 8. EKLJP-a." [8]

Međunarodni pakt o građanskim i političkim pravima iz 1966. godine[9] , u članu 17. propisuje da:

"Niko ne može biti predmet samovoljnih ili nezakonitih mešanja u njegov privatni život, u njegovu porodicu, u njegov stan ili njegovu prepisku, niti nezakonitih povreda nanesenih njegovoj časti ili njegovom ugledu. Svako lice ima pravo na zaštitu zakona protiv ovakvih mešanja ili povreda".

Komitet za ljudska prava (Human Rights Committee) je u svom Generalnom komentaru br. 16 o članu 17. Međunarodnog pakta o građanskim i političkim pravima (Pravo na privatnost, porodičan život, dom i prepisku, i zaštitu časti i reputacije) je još 1988. godine uvrstio ovaj pojam kao deo prava na privatnost. Komitet je naveo da "prikupljanje i čuvanje ličnih podataka na kompjuterima, bazama podataka i drugim uređajima, bilo od strane državnih organa ili privatnih lica ili organa, mora biti regulisano zakonom" i da "svaki pojedinac treba biti u mogućnosti da utvrdi koji javni organi, privatna lica ili tela kontrolišu ili mogu kontrolisati njihove podatke. Ako takvi podaci sadrže pogrešne informacije ili su prikupljeni ili obrađeni u suprotnosti sa odredbama zakona, svaki pojedinac treba da ima pravo da traži ispravljanje ili eliminaciju."

Konvencija Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti ima za cilj da:

"na teritoriji svake strane ugovornice garantuje svakom fizičkom licu, bez obzira na njegovu nacionalnu pripadnost ili na mesto stanovanja, poštovanje njegovih osnovnih prava i

[8] http://www.bgcentar.org.yu/documents/II9licnod.htm

[9] Međunarodni pakt o građanskim i političkim pravima je potpisan u Njujorku

19.12.1966. godine (Službeni list SFRJ br. 7 od 4. febr. 1971

sloboda, a naročito njegovog prava na privatnost kada je reč o automatskoj obradi njegovih ličnih podataka" (čl. 1).

Ova Konvencija uređuje, između ostalog, i osnovne principe u vezi zaštite ličnih podataka, obaveze ugovornica, bezbednost podataka i izuzetke i ograničenja zaštite podataka. Takođe, u Poglavlju III, uređuje i prekograničnu razmenu informacija, i propisuje da "Jedna strana ugovornica ne može, samo radi zaštite privatnosti, da zabrani ili da uslovi izdavanje nekakve specijalne dozvole, prekogranični protok ličnih podataka na teritoriju neke druge strane ugovornice", osim u slučaju da, zbog karaktera ličnih podataka i zbirki podataka, u njenom zakonodavstvu postoje posebni propisi za te kategorije ličnih podataka ili automatizovanih zbirki sa ličnim podacima, ili ukoliko se prenos podataka vrši sa njene teritorije na teritoriju neke države koja nije potpisnica Konvencije, uz posredstv neke druge strane ugovornice, a radi obezbeđenja da se takav protok vrši mimo zakonodavstva te strane ugovornice.

Dodatni protokol uz Konvenciju 108 u vezi sa nadzornim organima i prekograničnim protokom podataka, potpisan 8. novembra 2001. godine, predstavlja sastavni deo Konvencije i sve odredbe Konvencije primenjuju se u skladu sa ovim Protokolom. Dodatni protokol uz Konvenciju br. 108 (dalje: Protokol) usvojen je 18. maja 2018 godine (CETS, No 223). Konvencija, odnosno prečišćeni tekst Konvencije, koji uključuje i ovaj protokol naziva se Konvencija 108+ ili Modernizovana konvencija.

Osnovni principi na kojima počiva Konvencija 108 se nisu značajno promijenili,već su prilagođeni novim realnostima i zahtjevima sa terena. Dalje, dokument je značajno dopunjen detaljima i delovima koji donekle konkretizuju prilično uopštene odredbe osnovnog teksta

Uredba o zaštiti podataka (GDPR) i Konvencija 108

Evropski parlament je usvojio GDPR 14. aprila 2016. godine, a primenjuje se od 25. maja 2018. godine. Osnovni principi se mogu sažeti na sledeće: zakonitost, pravičnost i transparentnost; ograničavanje svrhe; smanjenje, odnosno minimiziranje količine podataka; tačnost; integritet i poverljivost. Ovo je, s jedne strane, podržano zahtevima za transparentnošću a, s druge strane, zahtevom za odgovornošću .Navedeno ne odudara značajno od osnovnih postulata Konvencije 108, ali se generalno može reći da GDPR više akcentira bezbednost i odgovornost.

UN Rezolucija o privatnosti u digitalnom dobu

Generalna skupština Ujedinjenih nacija,[10] koju čine predstavnici sve 193 svetske države, 20. decembra 2013. godine jednoglasno je usvojila Rezoluciju o pravu na privatnost u digitalnom dobu, što je prvi dokument UN koji se bavi zaštitom privatnosti posle 25 godina. Nemačka i Brazil su pokrenuli inicijativu u Ujedinjenim Nacijama da se ova Rezolucija usvoji zbog masovnog nadgledanja koje su vršile vlade širom sveta. Rezolucija je jednoglasno usvojena pred Trećim komitetom Ujedinjenih nacija, da bi potom, opet jednoglasno bila usvojena i u Generalnoj skupštini.

Rezolucijom je ukazano na to da ubrzan napredak tehnološkog razvoja omogućava pojedincima iz celog sveta da koriste nove IKT, ali i da istovremeno povećava mogućnost da države, kompanije i pojedinaci vrše nadzor, presretanje i prikupljanje podataka, što može da

[10] Usvojena jednoglasno 19-12-2013

dovede do kršenja ljudskih prava, posebno prava na privatnost. Rezolucija je takođe potvrdila ljudsko pravo na privatnost, u skladu sa kojim niko ne može biti podvrgnut arbitrarnom i nezakonitom mešanju u njegovu privatnost, porodičan život, dom i prepisku, kao i pravo na pravnu zaštitu u odnosu na takvo mešanje. Takođe je potvrdila da je pravo na privatnost važno za realizaciju slobode izražavanja i mišljenja, bez ikakvog uznemiravanja.. Rezolucijom se još zahteva da Visoki komesar za ljudska prava UN Generalnoj skupštini podnese izveštaj o zaštiti prava na privatnost u kontekstu nacionalnog i ekstrateritorijalnog nadzora i/ili presretanja digitalnih komunikacija i sakupljanja ličnih podataka, uključujući takvo postupanje i na masovnom nivou. U Rezoluciji se navodi da, iako se prikupljanje i obrada podataka može opravdati zaštitom javne bezbednosti, države moraju da osiguraju poštovanje obaveza koje imaju u skladu sa međunarodnim standardima ljudskih prava. Rezolucija pruža mogućnost da se problem zaštite privatnosti dalje razmatra u Ujedinjenim nacijama. Iako nije pravno obavezujuća za države članice UN, značaj ove Rezolucije je nesporan i predstavlja prvi korak ka usvajanju pravno-obavezujuće zaštite privatnosti u digitalnom dobu. Ovo nije prvi put da se jedna rezolucija UN smatra za deo običajnog prava, koje je jedan od glavnih izvora međunarodnog prava, s obzirom da se glasanjem u Generalnoj skupštini najbolje oslikava praksa država, ali i njihov stav o obavezujućoj prirodi norme koju usvajaju. Imajući ovo u vidu, može se reći da je jednoglasno usvajanje ove Rezolucije dokaz o opštem stavu država članica o neophodnosti zaštite privatnosti u digitalnom dobu.

Pregled EU principa i regulative

- Povelja Evropske unije o osnovnim pravima (07. decembra 2000. godine);

- Direktiva Evropskog parlamenta i Saveta o zaštiti građana u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka (95/46 od 24. 10. 1995. godine);

- Direktiva Evropskog parlamenta i Saveta u vezi obrade ličnih podataka i zaštite privatnosti u elektronskim komunikacionim sektorima (2002/58 FC od 12. 07. 2002. godine);

- Direktiva Evropskog parlamenta i Saveta o zadržavanju generisanih ili obrađenih podataka u vezi sa odredbom u javnosti raspoloživih elektronskih komunikacionih servisa ili javne komunikacine mreže i dopune Direktive 2002/58/ec i (2006/24) EU od 15. 03. 2006. godine;

- Evropska Konvencijom o zaštiti lica u pogledu automatske obrade ličnih podataka Saveta Evrope (ETSNo 108) i dodatnim protokolom uz Konvenciju o zaštiti u odnosu na automatsku obradu ličnih podataka;

- Direktiva 2009/136/EZ Evropskog parlamenta i Saveta (od 25. 11. 2009. godine) o univerzalnoj usluzi i pravima korisnika u vezi sa mrežama i uslugama elektronskih komunikacija;

Primena Direktiva bi trebalo da dovede do harmonizovanijeg pravnog okvira u kontekstu razmene informacija između organa unutrašnjih poslova u EU i, konačno, doprinese smanjenju troškova i stope kriminaliteta.

Direktiva Evropskog parlamenta i Saveta Evropske unije 95/46/EZ od 24.10.1995. o zaštiti građana u vezi sa obradom podataka o ličnosti i o slobodnom kretanju takvih podataka obavezuje države članice da štite osnovna prava i slobode fizičkih lica, a posebno njihovo

pravo na privatnost u pogledu obrade podataka o ličnosti. Ova Direktiva uređuje osnovna načela u pogledu zaštite ličnih podataka, zatim obaveze rukovalaca i prava lica na koje se podaci odnose, postupanje sa osetljivim podacima, prekogranični prenos podataka i drugo..

Direktiva Evropskog parlamenta i Saveta Evropske unije u vezi sa obradom ličnih podataka i zaštite privatnosti u elektronskom komunikacionom sektoru (2002/58EC od 12.jula 2002)navodi da je poverljivost komunikacija zagarantovana u skladu sa međunarodnim instrumentima koji se odnose na ljudska prava, naročito Evropskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda i ustavima Država članica EU. Ova Direktiva usklađuje odredbe Država članica koje se traže za obezbeđenje nekog ekvivalentnog nivoa zaštite osnovnih prava i sloboda, naročito prava na privatnost, u odnosu na obradu ličnih podataka u sektoru elektronske komunikacije i za obezbeđenje slobodnog kretanja takvih podataka i podataka o opremi za elektronsku komunikaciju i usluge u Zajednici, i uređuje pitanja poput poverljivosti komunikacije, bezbednosti, podacima o saobraćaju podacima o lokaciji mimo podataka o sabraćaju i druga relevantna pitanja za elektronsko komunikacioni sektor, kao što su kolačići ("cookies"), zatim uvođenje naplate računa po stavkama, upotreba spyware opreme i opreme za prisluškivanje i drugo.

"14. aprila 2016. godine su usvojena nova pravila o zaštiti ličih podataka na nivou Evropske unije („EU").Paket reformi uključuje Opštu uredbu o zaštiti podataka (General Data Protection Regulation; „Uredba") i Direktivu o zaštiti podataka za policiju i sektor krivičnog pravosuđa (Data Protection Directive for Police and Criminal Justice Authorities; „Direktiva"), koje će zameniti dosadašnji centralni propis evropske legislative u oblasti zaštite podataka, Direktivu o zaštiti podataka iz 1995. godine (Data Protection Directive – Directive 95/46/EC), kao i Okvirnu odluku za policiju i sektor krivičnog pravosuđa iz 2008. godine. Novi pravni okvir će stupiti na snagu nakon isteka prelaznog perioda u trajanju od dve godine, što bi trebalo da omogući odgovarajuća prilagođavanja." [11]

Društvene mreže s osvrtom na Fejsbuk (engl. Facebook)

Čovekova želja za druženjem pronalazi uvek nove načine interakcije koji u sprezi s brzim razvojem novih tehnologija,definišu društvenost na posve novi način.

Fejsbuk je najpopularnija društvena mreža i broji više od pola milijarde korisnika.Fejsbuk (engl. Facebook) je internet stranica koja služi kao servis za socijalnu mrežu. Počeo je sa radom 4. februara 2004. Ova internet stranica, na koju se svako može učlaniti, nalazi se u vlasništvu istoimenog preduzeća (Facebook, Inc.) koje i upravlja njime. Njegovi korisnici se mogu pridruživati u mreže koje su organizovane, kako bi se povezali i komunicirali sa drugim ljudima. Takođe, ljudi mogu dodavati prijatelje, slati im poruke, a mogu i postavljati nove podatke u svoje profile kako bi obavestili prijatelje o sebi.Stvorio ga je Mark Zakerberg dok je bio student na univerzitetu Harvard.

U početku članstvo na ovoj društvenoj mreži bilo je dozvoljeno samo studentima sa Harvarda, da bi se kasnije proširilo na studente sa svih koledža koji su članovi „Ajvi lige" (engl. Ivy League).

[11] https://geciclaw.com/sr/eu-usvojila-reformu-politike-zastite-podataka-o-licnosti/

U nekim zemljama, kao što su Sirija, Kina, Vijetnam, i Iran, pristup ovoj internet stranici je povremeno blokiran, a isto je učinjeno i na brojnim radnim mestima, kako zaposleni ne bi trošili vreme na posetu sajta. Jedan od problema je predstavljalo poštovanje privatnosti korisnika, koje je nekoliko puta dovedeno u pitanje.

U današnje vremenu napredne tehnologije, milioni ljudi su uključeni u društvene mreže.Putem društvenih mreža Kompanije nisu angažovane samo da posmatraju šta posećujete na internetu, već da infiltriraju informacije i šalju reklame zasnovane na vašoj istoriji pretraživanja.

Postoje četiri osnovna razloga zbog čega dolazi do mogućnosti kršenja prava na privatnost na društvenim mrežama:

1. nesavršenost korisnika društvene mreže – odnose se uglavnom na nesavršenosti čoveka kao ljudskog bića i na njegovu potrebu da svoju privatnost deli sa drugim ljudima; svest o sopstvenoj i tuđoj privatnosti ne postoji u operativnoj memoriji čoveka pa korisnik tako „oda" osetljivu informaciju da i nije toga svestan;

2. mane u programima (softverima) koji se koriste na društvenim mrežama – dovode do toga da su na društvenim mrežama mehanizmi za kontrolu privatnosti veoma slabi i nezaštićeni od svih direktnih zlonamernih napada, poput krađe ličnih podataka,stvaranja lažnih profila i sl.;

3. nenamerno odavanje ličnih podataka – do ličnih podataka na društvenoj mreži se može doći i metodom isključivosti (npr.kada na osnovu godine diplomiranja možemo zaključiti koje je korisnik godište iako to nije napisao u profilu); nažalost, protiv ovakvog "curenja" podataka korisnik se najteže bori jer na društvenim mrežama postoji nebrojeno mnogo informacija i podataka od kojih korisnik ne može da se sačuva niti pripazi;

4. sukob interesa – većina društvenih mreža se finansira od oglasa koje reklamne agencije postavljaju, pa ova činjenica dovodi do sukoba interesa kada je reč o ličnim podacima korisnika koje društvene mreže mogu da ustupaju reklamnim agencijama; korisnici žele da njihovi podaci nedostupni ljudima koje nisu označili kao „prijatelje" dok reklamne agencije žele da dođu u posed što većeg broja ličnih informacija kako bi bolje i lakše plasirali svoje proizvode ili usluge.

Imajući u vidu da deca nisu u dovoljnoj meri svesna rizika, posledica, zaštite i prava u vezi sa prikupljanjem i obradom ličnih podataka, deca zaslužuju posebnu zaštitu privatnosti na internetu. Među zemljama članicama Evropske unije u kojima se primenjuje GDPR uredba trenutno ne postoji konsenzus u vezi sa donjom uzrasnom granicom ispod koje je neophodno tražiti saglasnost roditelja ili staratelja za detetovo korišćenje servisa na internetu. Ovaj raspon se kreće od 13 do 16 godina. Neke zemlje kao razlog za podizanje uzrasne granice navode nameru da podrže aktivno uključivanje roditelja u život njihove dece.

Zemlje koje su spustile uzrasnu granicu na 13 godina smatraju da je to način da se podstaknu internet provajderi da kreiraju zaštitne alate i preuzmu odgovornost za bezbednost dece na internetu, pošto je odgovornost za dečju zaštitu prebačena sa roditelja na industriju. Prema američkom Zakonu o zaštiti privatnosti dece na internetu nijedna organizacija niti osoba koja koristi usluge na internetu (uključujući i vlasnike društvenih mreža) ne sme da prikuplja lične podatke osoba mlađih od 13 godina bez odobrenja njihovih roditelja ili staratelja.

Da bi se izbeglo dobijanje roditeljske saglasnosti za mlađe od propisanog uzrasta, većina servisa postavila je uzrasno ograničenje za korišćenje njihovih usluga. Ono je jasno navedeno u tzv. „uslovima korišćenja", a od korisnika se traži da se pre početka korišćenja saglasi sa ovim uslovima.

Važno je istaći da i roditelji,često nesvesno, ugrožavaju pravo na privatnost

Pitanje nije samo pravne prirode. Socijalna dimenzija problema ukazuje na nepostojanje svesti građana kada su u pitanju posledice ponašanja u digitalnom okruženju. I dalje postoji uverenje da je onlajn ponašanje odvojeno od realnog života. Međutim, očigledno je da se posledice neodgovornog ponašanja onlajn osećaju u realnom životu i obratno.

Zaštita podataka o ličnosti je deo korpusa zagarantovanih ljudskih prava i predstavlja neodvojivi deo ljudskog prava na privatnost, čija je zaštita propisana kako međunarodnim, tako i domaćim i regionalnim propisima.

Pojedinac u većini slučajeva ne može da izbegne davanje podataka o ličnosti (koji u stvari predstavljaju svojevrstan način plaćanja na Internet stranicama poput Facebook-a i Instagram-a, koje su naizgled besplatne, ali je pristup njima uslovljen davanjem podataka o ličnosti korisnika, pod njihovim uslovima poslovanja) , a Internet platforme i biznis-modeli zasnovani na prikupljanju podataka o ličnosti su dužni da omoguće da oni budu bezbedni i zaštite građane od svake zloupotrebe i nedozvoljene obrade.

Još jedna opasnost koja preti kršenju prava na privatnost i zaštiti podataka o ličnosti jeste stvaranje velikih "banaka podataka" u svim oblastima. Pristup informacijama na osnovu kojih je utvrđen ili se može utvrditi identitet neke osobe može se iskoristiti i na način da ovi podaci budu zloupotrebljeni za nadgledanje te osobe, za stvaranje čitavih baza podataka o pojedincima, za razmenu i trgovinu ovim podacima, kao i za krađu identiteta i mnoge druge oblike zloupotreba. Ukoliko se obrada podataka ne vrši na pravno dozvoljen način, stvara se mogućnost za ozbiljno narušavanje prava na privatnost, ali i uticaj na društvo u celini i raznovrsne etičke probleme, uključujući i nadzor na komunikacijama, prodaju podataka o ličnosti i krađu identiteta. Društveno odgovorno poslovanje kompanija u digitalnoj eri teži da uspostavi ravnotežu između zaštite korisnika i bezbednosti njihovih podataka, uz istovremeno neometano poslovanje i inovaciju. Stoga bi konstantni dijalog, edukacija i saradnja različitih aktera trebalo da dovedu do zaštite podataka o ličnosti u skladu sa najvišim standardima, a da pritom ne utiču negativno na razvoj tržišta, slobodnu komunikaciju na Internetu i razvoj.

Korisnici fejsbuka nemaju pravo na digitalni zaborav tj. deaktivacija profila znači privremeno ukidanje profila , ali ne i trajno., tj Fejsbuk i dalje drži podatke korisnika za slučaj da se vrati a taj način zadržavanja podataka je suprotan modernim propisima o zaštiti podataka.

Ukoliko dođe do zloupotrebe na Fejsbuku policija mora da upotrebi mere „digitalne forenzike" kako bi identifikovala administratora sporne Fejsbuk strane. Mora postojati pravni osnov po kome bi Fejsbuk, kao pružalac internet usluge (provajder) bio primoran da dostavi

logove sa svojih servera kao i informacije kojima bi se omogućilo identifikovanje ovih lica. U praksi, ovo se može pokazati kao težak zadatak.

Ukoliko se identifikuje administrator sporne Fejsbuk strane na teritoriji Republike Srbije, to lice je dužno da inspektoru Poverenika omogući nesmetano vršenje nadzora i stavi mu na uvid i raspolaganje potrebnu dokumentaciju. Ako se prilikom obavljanja nadzora utvrdi da su povređene odredbe zakona kojima se uređuje obrada, Poverenik će upozoriti rukovaoca na nepravilnosti u obradi i nakon toga može:

narediti da se nepravilnosti otklone u određenom roku; privremeno zabraniti obradu koja se obavlja suprotno odredbama zakona; narediti brisanje podataka prikupljenih bez pravnog osnova.

Ukoliko se počini neko krivično delo reaguje tužilaštvo za visokotehnološki kriminal.

Zaštita podataka na internetu

WHOIS baza podataka

“WHOIS je servis nivoa aplikacije OSI modela računarske mreže. Ovaj mrežni protokol koristi TCP port 43. Njegova osnovna primena je dobijanje podataka o registraciji vlasništva internet domena, IP-adrese i autonomnih sistema traženog domena.

Protokol podrazumeva arhitekturu "klijent-server" i koristi se za pristup bazama javnih servera koji sadrže zapise o IP adresama i registrantima domena. Trenutna verzija protokola je opisana je u RFC 3912. Najčešće, WHOIS klijent je implementiran kao konzolni servis. Međutim, pošto mnogim korisnicima komandna linija nije nedostupna ili je komlipkovana za rad, na mnogim sajtovima na internetu postoje onlajn servis. Pored toga, postoje i WHOIS klijent GUI.

U početku, WHOIS servis je da omogućio administratorima da traže kontakt informacije o drugim administratorima, IP-adresama ili imenima domena.” [12]

Whois zaštita / whois guard predstavlja zaštitu podataka vlasnika domena i omogućava da privatne informacije ne budu izložene i dostupne, odnosno da budu skrivene prilikom WHOIS upita. One se čuvaju u tajnosti i zaštićene su od strane Domain Privacy Protection Servisa, čije se kontakt informacije prikazuju, pružajući na taj način najviši nivo zaštite od spamera i zloupotreba identiteta.Za svaki internet domen postoji javno dostupna WHOIS baza podataka u kojoj se nalaze podaci o vlasniku, administratoru i tehničkom kontaktu za

[12] https://sr.wikipedia.org/sr-el/WHOIS

svaki domen. Podaci se unose prilikom registracije domena i moraju biti ažurni jer registri domena zadržavaju pravo da otkažu registraciju domena ako zaključe da su podaci netačni ili zastareli.Podatke koji se nalaze u WHOIS bazi podataka zaštićuju se poručivanjem dodatne usluge za domen zaštita WHOIS podataka . U tom slučaju javno dostupna WHOIS baza podataka neće prikazivati podatke sve dok postoji aktivirana opciju zaštite podataka za određeni internet domen.

Usluga zaštite WHOIS podataka se aktivira za određeni domen na period od jedne ili više godina. Zaštitu privatnosti možete poručiti: Prilikom registracije novog domena, tako što obeležite dodatnu opciju "zaštita privatnosti"

Treba imati u vidu da dodavanje whois zaštite, na domen koji je već neko vreme postojao bez whois zaštite, možda neće biti potpuno efektivno, jer na internetu postoje razni nezavisni sajtovi koji prikupljaju i u svojim bazama čak i zauvek čuvaju podatke i pored trenutno "zaštićenih" podataka nude i prikaz tih starih podataka i nakon kasnije aktivirane whois zaštite. Zbog toga je jedina potpuna zaštita identiteta da se whois zaštita zakupi prilikom prve registracije domena.

Zaključak:

Krivičnopravna zaštita jeste ultima ratio, ali imajući u vidu objekt zaštite, a to je pravo na privatnost i pravo na zaštitu podataka o ličnosti kao njegov segment, spadajući u osnovna ljudska prava, zavređuju najviši nivo zaštite. Ostaje na nama koji se bavimo pravom da posredno i neposredno utičemo na javnost i zakonodavca da proširi nivo krivičnopravne zaštite podataka o ličnosti i time stane na put u najvećoj mogućoj meri rastućim vidovima zloupotrebe ličnih podataka.

Cilj domaćih i međunarodnih propisa nije sama zaštita podataka o ličnosti, već zaštita pojedinca na koga se ti podaci odnose, a time i dela njegove takozvane informacijske privatnosti.

Literatura:

1. Milan Škulić: Kompjuterski kriminalitet

2.L.Komlen Nikolić :Suzbijanje visokotehnološkog kriminala,; Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd;2010

3.Mirjana Drakulić:Osnovi kompjuterskog prava, Beograd, 1996. Godina

4. Vida M. Vilić POVREDA PRAVA NA PRIVATNOST ZLOUPOTREBOM DRUŠTVENIH MREŽA KAO OBLIK KOMPJUTERSKOG KRIMINALITETA doktorska disertacija Pravni fakultet Niš

5. ZAKON O ZAŠTITI PODATAKA O LIČNOSTI („Službeni glasnik RS", br. 87/18);

6.Krivični zakonik („Službeni glasnik RS", broj 85/05, 88/05, 107/05, 72/09, 111/09, 121/12,

104/13, 108/14, 94/16, 35/19);

7.Ustav Republike Srbije („Službeni glasnik RS”, br. 98/06, 16/22 (Odluka o proglašenju Ustavnog zakona za sprovođenje Akta o promeni Ustava Republike Srbije – Amandmani I–XXIX – „Sl.glasnik RS”, br. 115/21)

8.Zakon o organizaciji nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS”, br. 61/05, 104/09, 10/23, 10/23 (drugi zakon));

9.Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka („Službeni list SRJ – Međunarodni ugovori”, broj 1/92 i „Službeni list SCG – Međunarodni ugovori”, broj 11/05);

10. https://www.rnids.rs/lat/podaci-o-registrovanom-domenu/whois-servis

11. http://www.geciclaw.com/sr/eu-usvojila-reformu-politike-zastite-podataka-o-licnosti/

12. http://www.prafak.ni.ac.rs/files/nast_mat/PRAVO_PRIVATNOSTI.pdf

13. http://www.europarl.europa.eu/news/hr/top-stories/20130901TST18405/za%C5%A1tita-podataka-za%C5%A1tita-va%C5%A1e-privatnosti

14. https://www.rnids.rs/lat/podaci-o-registrovanom-domenu/whois-servis

15. http://www.geciclaw.com/sr/eu-usvojila-reformu-politike-zastite-podataka-o-licnosti/

16. http://www.prafak.ni.ac.rs/files/nast_mat/PRAVO_PRIVATNOSTI.pdf

17. https://sr.wikipedia.org/sr-el/WHOIS

Objavljen tekst Privatnost i zaštita podataka o ličnosti kroz domaće i međunarodno pravo s osvrtom na korisnike Fejsbuka i internet sa krivično pravnog aspekta - Radno pravni savetnik br 1/2024