.

# Drˇzava i privatnost(promeniti naslov)

Međutim, privatnost na internetu nije samo lični problem pojedinca, već ima daleko šire razmere koji dostižu i nivo same države. Stoga, kada se govori o privatnosti na internetu, treba pomenuti i odnos drˇzave i drˇzavnih institucija prema privatnosti pojedinca. Kroz istoriju je bio ˇcest sluˇcaj da su drˇzave naruˇsavale privatnost pojedinaca kako bi ostvarile odredene interese, reˇsile određene probleme ili u situacijama ekstremne opasnosti, kao što je na primer borba protiv terorizma. Ovome u prilog ide i činjenica da je sluˇcajeva u kojima su ameriˇcka administracija i sluˇzbe krˇsile privatnost gradana bilo mnogo, od prodaje podataka sluˇzbenika tajnih sluˇzbi novinarima i privatnim detektivima, do ilegalnog prisluˇskivanja ameriˇckih i stranih drˇzavljana od strane FBI-ja. Neki od tih sluˇcajeva su zloupotreba popisnih spiskova od strane ameriˇcke vojske u Prvom i Drugom svetskom ratu, koriˇs´cenje policijskih dronova, kao i televizijske kamere zatvorenog kruga (eng. *closed-circuit television, CCTV*). O ovome svedoči i podatak da prosečan stanovnik Velike Britanije bude uhva´cen na kameri u proseku 300 puta dnevno [[22](#_bookmark40),23[].](#_bookmark41) Ne samo da pojedinac može biti uhvaćen na kameri, već se dešava i da država prisluškuje ono što određeni pojedinci u svakom trenutku govore. Iako je prisluˇskivanje razgovora i postavljanje bubica aktom ameriˇckog kongresa iz 1934. godine zabranjeno, osim u slučajevima kada postoji sudski nalog, to nije sprečilo FBI da nastavi da to da radi ilegalno, ˇcak i tokom Drugog svetskog rada uz dozvolu predsednika Ruzvelta [[28](#_bookmark46)]. Nakon rata, nacionalna sigurnosna agencija (eng. *National Security Agency,* NSA), FBI i druge bezbednosne sluˇzbe nastavile su sa krˇsenjem zakona o privatnosti pojedinaca, ˇsto se kasnije i proˇsirilo na druge vidove komunikacije, i pre svega na internet.

## Legalno naruˇsavanje privatnosti na internetu

Usled pretnje po bezbednost SAD-a, donoˇseni su zakoni koji su bezbednosnim sluˇzbama dali ve´ca ovlaˇs´cenja, koja su automatski dozvoljavala ovim organizacijama upad u privatnost pojedinaca. U narednim odeljcima, bi´ce navedeni neki zakoni kojima američka administracija dozvoljava naruˇsavanje privatnosti na internetu.

### Zakon o nadzoru stranih sluˇzbi

Ameriˇcka administracija je 1978. godine donela zakon o nadzoru stra- nih sluˇzbi (eng. *Foreign Intelligence Surveillance Act*, FISA), kojim se dozvoljava tajni nadzor inostranih vlada i njihovih sluˇzbi. Ovim zako- nom ameriˇcki predsednik je mogao da odobri elektronski nadzor stranih drˇzavljana na jednu godinu, pod uslovom da se time ne krˇsi privatnost drˇzavljana Amerike. U suprotnom, administracija bi morala da dobije sudski nalog za prisluˇskivanje. Međutim, bez obzira na postojanje ovog zakona, postoje mnogi slučajevi kršenja njegovih odredbi. Tako je 2013. godine Edvard Snouden, bivˇsi zaposleni u NSA i FBI, obelodanio na hiljade tajnih dokumenata ameriˇckih tajnih sluˇzbi, medu kojima se naˇsao i projekat PRISM, koji je dozvoljavao NSA-i pristup mnogim serverima pojedinih internet kompanija, kao i velikoj količini privatnih informacija, među kojima su bili i video pozivi ˇ kojima je ovim odredbama dozvoljen pristup čak i bez sudskog naloga [[10](#_bookmark28)]. U odeljku [3.2](#_bookmark8) detaljno ´ce biti detaljno prikazan projekat PRISM.

### Zakon o skladiˇstenoj komunikaciji

Zakon o skladiˇstenoj komunikaciji (eng. *Stored Communication Act*) predstavlja deo zakona o privatnosti pri elektronskoj komunikaciji (eng. *Electronic Communication Privacy Act*) iz 1986. godine i odnosi se na privatnost kolekcija elektronske poˇste. Po ovom zakonu, vlastima nije potreban sudski nalog kako bi od dobavljaˇca internet usluga (eng. *Internet provider*) dobili mejlove starije od 180 dana. Problem sa ovim zakonom se usložnjava činjenicom da od skoro provajderi pružaju klaud usluge, te korisnice više ne čuvaju na ovim serverima samo mejlove, već i veliku količinu drugih privatnih podataka, koje bi inače čuvali na svojim privatnim računarima. Prema tome, odredbe ovog zakona pružaju uvid u podatke koji prevazilaze skladištenu komunikaciju elektronske pošte i dozvoljavaju vlastima uvid i u privatne podatke koji su nekim drugim odredbama suštinski zaštićeni. Usled proˇsirenja skladiˇstenog prostora i funkcija provajderskih servera, skoro pedeset kompanija i organizacija koje smatraju da administracija ne bi smela da dobavlja privatne informacije korisnika sa klauda bez sudskog naloga, udruˇzilo se u organizaciju pod nazivom Digital Due Process, kako bi zahtevali od administracije da unapredi ovaj zakon [[24](#_bookmark42)].

## 3.2 PRISM

Edvard Snouden je u junu 2013. godine obelodanio na hiljade tajnih dokumenata NSA i FBI, čime je otvoren jedan od većih slučajeva narušavanja privatnosti podataka. Među ovim dokumentima su se naˇsli i dokumenti vezani za program PRISM, koji predstvlja tajni program koriˇs´cen za nadzor aktivnosti na internetu. Program je zapoˇcet 2007. godine i u narednih nekoliko godina sve velike kompanije su dale saglasnost za nadzor njihovih servera: Majkro- soft 2007., Jahu 2008., Gugl, Fejsbuk i PalTalk 2009., Jutjub 2010., Skajp i AOL 2011. i Epl 2012. godine [[10](#_bookmark28)].

Prema FISA zakonu, NSA je imala pravo da uz sudski nalog traˇzi podatke o pojedincu od internet kompanije. Medutim, kako su u NSA smatrali da ceo taj proces predugo traje i da su potrebni nalozi za oba uˇcesnika internet konverzacije, program PRISM je bio idealno reˇsenje tog problema. Agencija je imala direktan pristup serverima gorenavedenih kompanija i mnogo ve´cu slobodu u nadzoru i prikupljanju podataka, pa ˇcak i pra´cenju poziva uˇzivo preko interneta. NSA ovo i navodi u svojim dokumentima, gde ovaj program nazivaju "jednim od najvrednijih, jedinstvenih i najproduktivnijih pristupa koji NSA ima"[[10](#_bookmark28)]. Kada se uzme u obzir da je PRISM program omogućio prikupljanje mejlova, razgovora, video poziva, slika, video poziva i istorije pretraživanja korisnika, ne čudi što je za ove organizacije program PRISM bio od tolikog značaja.

Pored problema sudskih naloga, FISA zakon je predstavljao problem za NSA-u jer je sprečavao praćenje komunikacije izmedu dva strana drˇzavljanina ukoliko ona ide preko servera koji se nalaze u SAD-u. Kako je ve´cina servera velikih internet kompanija locirano u SAD-u, ovaj zakon je u velikoj meri ograničavao mogućnost praćenja komunikacije između stranih državljana. Zbog toga je 2007. godine donet zakon o zaˇstiti Amerike (eng. *Protect America Act*, PAA), koji je omogu´cio NSA-i da pokrene program PRISM i da zloupotrebi ovlaˇs´cenja data ovim zakonom kako bi prikupljali i pratili komunikaciju na internetu [[13](#_bookmark31)].

Iako su sve kompanije umeˇsane u ovaj program negirale bilo kakvu povezanost, kasnije su izlazile sa izveˇstajima gde navode da je ameriˇcka administracija zahtevala od njih nadzor i pristup podacima svojih korisnika. Tako na primer, u izveˇstaju kompanije Jahu, navodi se da im je administracija pretila i kaznom od 250 hiljada dolara godiˇsnje ukoliko ne budu saradivali [[3](#_bookmark21)

# Zaˇstita privatnosti

## Enkripcija

Internet je otvoren sistem, što znači da se svi podaci kroz viˇse uredaja, deljenih konekcija, ili ˇcak beˇziˇcno ˇsalju kako bi stigli do ˇzeljene destinacije. Ovaj sistem omogu´cava komunikaciju izmedu uredaja koji mogu biti udaljeni viˇse hiljada kilometara, ali zbog kljuˇcnog mehanizma koji to dozvoljava, ovaj sistem pravi i jedan od najve´cih problema. Svaki uredaj koji se nalazi izmedu poˇcetnog i krajnjeg odrediˇsta moˇze videti ˇsta je poslato. Svaka elektron- ska poˇsta, ukucana lozinka i broj kreditne kartice mogu biti proˇcitani od strane nekoga u sredini te se da bi se ovo spreˇcilo koristi enkripcija.

Enkripcija je mehanizam kojim se bilo kakva informacija ˇsifruje, tj. prebacuje iz ˇcitljivog oblika u naizgled nasumiˇcne karaktere, koji se uz pomo´c odgovaraju´ceg kljuˇca mogu vratiti u svoj prvobitan oblik [[14](#_bookmark32)]. Jedan od prvih mehanizama enkripcije je Cezarova ˇsifra (eng. *Caesar’s cipher*) koja je dobila ime po Cezaru koji je slao šifrovane poruke svojoj vojsci koje su samo oni mogli da razumeju. Cezarova šifra je priliˇcno jednostavna i zasniva se na zameni svakog karaktera za karakter koji je pomeren u abecedi za nekoliko mesta. Jedina potrebna informacija za ˇsifrovanje je kljuˇc koji oznaˇcava broj pozicija za koji je karakter pomeren, a za deˇsifrovanje primalac samo treba da isko- risti negativnu vrednost kljuˇca. Ovu enkripciju bi bilo koji ˇcovek mogao da deˇsifruje vrlo brzo, tako da nije primenljiva u domenu raˇcunara, ali daje osnovu za razumevanje kompleksnijih algoritama koji se koriste pri upotrebi veb pregledaˇca, elektronske poˇste ili prilikom onlajn kupovine.

Enkripciju je moguće podeliti na simetričnu i asimetričnu enkripciju, pri čemu je Cezarova ˇsifra primer simetriˇcne enkripcije. Simetriˇcna enkripcija se koristi u situacijama kada ve´c postoji siguran kanal za komunikaciju, te je potreban samo jedan kljuˇc. Joˇs jedan primer ove vrste enkripcije je AES (eng. *Advanced Encryption Standard*), koji se koristi kod virtuelnih privatnih mreˇza (o kojima ´ce biti reˇci u odeljku [5.2](#_bookmark16)), za enkripciju hard diska, kompresiju (WinZip, RAR), kod alata koji se koriste za ˇcuvanje ˇsifara i za enkripciju poruka koje se ˇsalju putem druˇstvenih mreˇza kao ˇsto je Fejsbuk. Do sada nije zabeleˇzen uspeˇsan napad na AES, ali to ne znaˇci da je u potpunosti siguran. Postoje takozvani ˇside-channel"napadi (tajming ili elektromagnetni napadi koji) koji su bazirani na poznava- nju informacija o fiziˇckom naˇcinu implementacije algoritma, okruˇzenju ili samom sistemu na kome se izvrˇsava [[18](#_bookmark36)].

Na internetu se uglavnom koristi asimetriˇcna enkripcija. Ona podra- zumeva da svako ko uˇcestvuje u komunikaciji ima svoj javni i privatni kljuˇc, tako da postoje dva različita ključa, za razliku od simetriˇcne u kojoj postoji samo jedan. Javni kljuˇc pojedinca je poznat svima, a privatni kljuˇc zna i koristi samo osoba koja ga poseduje. Pri slanju poruke, poˇsiljalac je najpre ˇsifruje sa javnim kljuˇcem primaoca, a zatim svojim privatnim kljuˇcem. Kada primalac do- bije poruku, on je deˇsifruje uz pomo´c javnog kljuˇca poˇsiljaoca i nakon toga sopstvenim privatnim kljuˇcem. Ovim je obezbedena komunikacija tako da niko sa strane ne moˇze da proˇcita niti promeni prosledenu poruku, a da se to ne detektuje. Par kljuˇceva kod asimetriˇcne enkripcije se generiˇse po matematiˇckim principima, tako da ako se neˇsto ˇsifruje uz pomo´c javnog kljuˇca, moˇze se deˇsifrovati privatnim i obrnuto. Najpopularniji primer asimetriˇcne enkripcije je RSA (eng. *Rivest–Shamir–Adleman*) [[12](#_bookmark30)]. Ona se obiˇcno ne koristi za enkripciju ˇcitavih poruka ili fajlova, ve´c se koristi u kombinaciji sa drugim ˇsemama enkripcije ili kao digitalni potpis za dokazivanje autentiˇcnosti i integriteta

poruke. Fajlovi se obiˇcno enkriptuju nekom simetriˇcnom enkripcijom, a zatim se njihovi kljuˇcevi enkriptuju pomo´cu RSA. Poˇsto za razliku od AES, RSA moˇze biti razbijena faktorizacijom celih brojeva, kljuˇcevi mo- raju biti duˇzi. Nacionalni Institut za Standarde i Tehnologiju predlaˇze koriˇs´cenje kljuˇca duˇzine 2048 bitova. RSA je prisutna kod pretraˇzivaˇca veba, imejlova, VPN usluga, ˇcetova i drugih komunikacionih kanala.

## Virtuelne privatne mreˇze (VPN)

Virtuelne privatne mreˇze (eng. *virtual private network*) nastale su usled potrebe da se biznisi, organizacije, vlade i sliˇcni subjekti koji poseduju ose- tljive informacije zaˇstite od hakovanja i gubitka podataka u sluˇcajevima kada je potrebno da im udaljeni korisnici ili satelitske kancelarije pristupe, kao i radi smanjenja telekomunikacionih troˇskova efikasnijim koriˇs´cenjem infrastrukture. VPN su privatne mreˇze koje rade preko deljene javne infrastrukture kao ˇsto je internet [[26](#_bookmark44)]. Virtuelna je zato ˇsto ne postoji odvojena fiziˇcka infrastruktura za datu mreˇzu, ve´c koristi ve´c postoje´cu javnu infrastrukturu. Privatna je zato ˇsto omogu´cava bezbednu upotrebu uz garanciju da ´ce samo ˇclanovi mreˇze mo´ci da vide poslate informa- cije [[17](#_bookmark35)]. VPN omogu´cavaju privatnost podataka koriˇs´cenjem sigurnosnih procedura(enkripcija) i protokola tuneliranja (IPsec, PPTP, L2TP). Pod tuneliranjem se podrazumeva da VPN pravi "tunel"izmedu korsinika pri ˇcemu se podaci enkriptuju na strani poˇsiljaoca, ˇsalju kroz tunel i zatim dekriptuju na strani primaoca. Pored podataka mogu se kriptovati i polazna i zavrˇsna adresa radi ve´ce sigurnosti [[11](#_bookmark29)].

Jedan od poznatijih tipova VPN-a je VPN "od lokacije do lokacije"(eng. *site-to-site*) je tip mreˇze koja omogu´cava uspostavljanje bezbedne komunikacije izmedu viˇse poslovnica na razliˇcitim lokacijama preko javne infrastrukture, i time se podaci sa jedne lokacije stavljaju na koriˇs´cenje zaposlenima na drugoj. Drugi osnovni tip ovih mreˇza je VPN za udaljen pristup (eng. *remote access VPN*), koja omogu´cava pojedincima da uspostave bezbednu vezu sa udaljenom mreˇzom i pristupe njenim resursima kao da su direktno povezani na dati server.

Iako prvobitno nisu bile namenjene za to, usled skoraˇsnjih otkri´ca o velikim projektima za nadzor i ograniˇcenja koje odredene vlade name´cu svojim gradanima, sve viˇse raste upotreba VPN usluga za zaˇstitu privat- nosti pojedinaca, zaˇstitu od cenzurisanja kao i za pristup sadrˇzaju koji je geografski ograniˇcen [[21](#_bookmark39)]. Joˇs jedan od razloga za pove´cano koriˇs´cenje je porast upotrebe javnih mreˇza koje je prouzrokovano ˇsirenjem mobilne industrije. Ovo je dovelo do stvaranja uslova za napade kao ˇsto su krada akreditiva, presretanje paketa i krada sesija, ˇsto vodi do toga da neki korisnici koriste VPN za zaˇstitu svojih interakcija. Mnoge VPN usluge nude mogu´cnost izbora izlaznih taˇcaka tako da korisnici mogu da dobiju IP adrese u razliˇcitim drˇzavama.

Iako do nekog stepena VPN provajderi pruˇzaju navedene usluge, do- vodi se u pitanje njihova sposobnost da oˇcuvaju anonimnost i privatnost. Privatnost se kod ovih mreˇza ne odnosi na privatnost krajnjih korisnika ve´c na povezivanje viˇse privatnih mreˇza. Zbog lako´ce koriˇs´cenja, veli- kih performansi i jakog marketinga postoji velika privlaˇcnost prema ovim mreˇzama, iako neinformisanost korisnika dovodi do problema.

### Rizici za korisnike VPN

Iako veliki broj pruˇzalaca VPN usluga tvrde da pruˇzaju robusne i si- gurne infrastrukture uz obezbedivanje bezbedonsti korisnika tako ˇsto ne

loguju podatke, ne postoje alati i istraˇzivanja koji te tvrdnje provera- vaju. Pored toga neki provajderi su poznati po tome ˇsto prodaju podatke korisnika i manipuliˇsu saobra´cajem. Takmiˇcenje izmedu provajdera za- jedno sa nedostatkom objektivnih mera kvaliteta dovodi do manipulacije i prikrivanja informacija koje bi bile od značaja za klijenata. Usled nedostatka nezavisnih ocena VPN usluga korisnici su primorani da se o tome informiˇsu sa blogova ili veb sajtova. Ti sajtovi su ve´cinom podrˇzani od strane VPN partnerskog marketinga i usluga, pa se od njihovih ocena ne moˇze oˇcekivati nepristrasnost. To se odnosi na neke od najbolje rankiranih sajtova za ocenjivanje VPN usluga. Pored curenja saobra´caja zbog loˇse bezbednosti oko 10% VPN servisa presre´cu i/ili ma- nipuliˇsu saobra´cajem s tim ˇsto su mogu´ci naˇcini za nadziranje saobra´caja koji su teˇski da se otkriju. Takode, VPN servisi obiˇcno obe´cavaju veliki broj razliˇcitih geografskih lokacija koje korisnici mogu da izaberu kao iz- lazne ˇcvorove, ali oko 10% njih daje netaˇcne informacije. Izmedu 5 i 30 procenata tih ˇcvorova nalazi se na potpuno drugim lokacijama od onih koje su predstavljene. Cˇak postoje provajderi koji tvrde da imaju lokacije u preko 190 drˇzava, a u stvarnosti se serveri nalaze u ne viˇse od 10 centara podataka [[21](#_bookmark39)].