VODIČ KROZ GDPR I ZAŠTITU
PODATAKA O LIČNOSTI

MOJI PODACI, MOJA PRAVA

SHARE
FOUNDATION

IMPRESUM:
SHARE FONDACIJA, JUN 2018.
UREDNICI: DANILO KRIVOKAPIĆ, ANDREJ PETROVSKI
AUTORI: DANILO KRIVOKAPIĆ, ĐORĐE KRIVOKAPIĆ, MILICA JOVANOVIĆ, BOJAN PERKOV, ANDREJ PETROVSKI
OBRADA TEKSTA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ: 200

PROJEKAT PODRŽALA:

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

CIP - Каталогизација у публикацији

Библиотека Матице српске, Нови Сад

004.738.5.056(036)

MOJI podaci, moja prava : Vodič kroz GDPR i zaštitu podataka o ličnosti / [Autori Danilo Krivokapić ... [et al.] ; urednici Danilo Krivokapić, Andrej Petrovski]. - Novi Sad : Share foundation, 2018 (Novi Sad : NS press). - 31 str. ; 16 cm

Tekst štampan dvostubačno. - Tiraž 200.

ISBN 978-86-89487-14-5

1. Кривокапић, Данило [аутор] [уредник] 2. Кривокапић, Ђорђе [аутор] 3. Јовановић, Милица [аутор] 4. Перков, Бојан [аутор] 5. Петровски, Андреј [аутор] [уредник]

а) Интернет - Безбедност - Водичи

COBISS.SR-ID 324300551

UVODNA PITANJA

UVODNA PITANJA

ŠTA SU PODACI O LIČNOSTI?

Svaka informacija o nama koja nas bliže određuje. To mogu biti ime i prezime, adresa, bankovni račun, otisak prsta, zdravstveni karton, opis naših fizičkih ili psiholoških karakteristika, podaci o našem ponašanju na internetu. Praktično, svaka informacija koja se može dovesti u vezu sa konkretnom osobom.

KOJI PODACI SU PODACI O LIČNOSTI NA INTERNETU?

Lozinke i naši nalozi za poruke, mejl ili društvene mreže, istorija aktivnosti koje smo sa tih naloga preduzeli (metapodaci, šerovi, lajkovi, klikovi), istorija pretrage interneta u aplikacijama koje koristimo, IP adresa našeg kompjutera ili smartfona, IMEI broj uređaja kojim pristupamo mreži i slično. Takođe, svi podaci iz fizičkog sveta koje unosimo pri korišćenju usluga (adresa, broj telefona, računa, itd) kao i jedinstvene numeričke vrednosti u kojima su takvi podaci izraženi.

DA LI SU SLIKE I TEKSTOVI OBJAVLJENI NA FEJSBUK PROFILU PODACI O LIČNOSTI?

Snimak pande iz Kine ili citat poznatog pisca, koje smo podelili na svom profilu, nisu lični podaci. Međutim, vreme kada smo objavlili post, geolokacija uređaja koji smo koristili, profili od kojih smo sadržaj preuzeli i koji su dalje delili naš post, mogu se smatrati podacima o ličnosti. Takođe, sama informacija da volimo pande ili određenog pisca predstavlja lični podatak.

DA LI SU PODACI KOJI SE PRIKUPLJAJU PUTEM KOLAČIĆA PODACI O LIČNOSTI?

Sve što nas može identifikovati, direktno ili posredno, jeste podatak o ličnosti. Ako su uređaj ili pretraživač naši, personalizovani, onda i kolačići preuzeti sa sajtova spadaju u naše podatke o ličnosti. Na primer, kolačič za Guglovu analitiku koji registruje posetu i interakcije, danas se nalazi na većini sajtova na svetu. To znači da će Gugl imati podatke o posetiocima tih sajtova, čak i kada posetioci ne koriste nijedan od Guglovih proizvoda.

ZAŠTO LIČNIM PODACIMA TREBA ZAŠTITA, KAD NEKE INFORMACIJE O NAMA SVAKO MOŽE DA ZNA ČIM NAS VIDI, KAO ŠTO SU POL ILI BOJA KOŽE?

Bili intimni, privatni ili javno dostupni, podaci o nama su sastavni deo naše ličnosti, a njihova zaštita je deo zaštite našeg prava da slobodno odlučujemo o svom životu. U te slobode spada i odluka šta ćemo i kome reći o sebi, kao i pravo da znamo i ograničimo šta neko može da uradi sa informacijama koje zna o nama.

KO SVE PRIKUPLJA PODATKE O LIČNOSTI?

Svaka državna ili privredna organizacija, udruženje ili institucija, koja je u zakonskoj obavezi da nam utvrdi identitet pre nego što nam isporuči uslugu, bilo da je reč o školi, bolnici, elektrodistribuciji, banci, internet provajderu. S druge strane, prodavci novina ili cipela, na primer, nemaju ovu obavezu, ali im ugovori i dozvole mogu omogućiti da prikupljaju podatke o ličnosti, kako bi nam dostavili robu na kućnu adresu ili poslali reklamnu poruku.

Bez obzira da li podatke uzimaju uz naš pristanak ili po drugom pravnom osnovu, da li postupaju kao državni organi ili privatne organizacije, svi akteri koji obrađuju lične podatke obavezni su da usklade svoje poslovanje sa zakonom o zaštiti podataka o ličnosti.

ŠTA JE ZAKON O ZAŠTITI PODATAKA O LIČNOSTI?

Propis koja jedna država donosi kako bi uredila odnose između građana na koje se podaci odnose, s jedne, i privatnih i javnih organizacija koje prikupljaju i obrađuju te podatke, s druge strane. U Srbiji je zakon usvojen 2008, a na snagu je stupio godinu dana kasnije. Usvajanje novog zakona, usklađenog sa aktuelnim evropskim okvirom, najavljeno je za kraj 2018. godine.

ŠTA JE GDPR?

Opšta uredba Evropske unije o zaštiti ličnih podataka. Usvojena je 2016. kako bi zamenila stari pravni okvir iz 1995. Primena je počela 25. maja 2018.

NA KOGA SE PRIMENJUJE GDPR?

GDPR pre svega štiti prava građana u Evropskoj uniji, te se u potpunosti primenjuje na sve organizacije čije se sedište nalazi na teritoriji EU. Takođe, primenjuje se i na sve organizacije čiji su kupci ili potencijalni klijenti građani koji se nalaze u EU, ili koje prate onlajn ponašanje građana EU.

NOVA PRAVILA

NOVA PRAVILA

Primena novog regulatornog režima zaštite podataka građana u Evropskoj uniji – Opšte uredbe o zaštiti podataka o ličnosti (General Data Protection Regulation, GDPR) i pratećih nacionalnih propisa, počela je 25. maja 2018. S obzirom na potencijalni opseg i dubinu uticaja novog regulatornog okvira, očekuje se da će taj dan označiti početak novog doba na internetu.

Mada je pre svega bila motivisana prevaziđenom regulativom na nivou Unije i različitim nacionalnim zakonima u zemljama-članicama, najznačajnija ambicija GDPR-a jeste regulisanje odnosa u sajber prostoru i jedinstveno uređenje digitalnog tržišta, okruženja gde se poslovanje, ali i druge aktivnosti, u velikoj meri zasnivaju na podacima.

Digitalne tehnologije omogućile su stvaranje i umnožavanje ogromnih količina podataka, čijom se obradom bave državni, komercijalni i neprofitni akteri. Neadekvatna zaštita i zloupotrebe podataka o ličnosti postali su sastavni deo svakodnevice globalnog informacionog društva. Napredni kompjuterski programi koje napajaju podaci, "nafta 21. veka", tzv. veštačka inteligencija (artificial intelligence, AI) ili sistemi mašinskog učenja (machine learning systems), nesumnjivo unapređuju kvalitet života ali, istovremeno, predstavljaju rizik po prava i slobode građana u razmerama bez presedana.

Iako štiti prava građana EU, Opšta uredba o zaštiti podataka o ličnosti predstavlja korak ka novom "društvenom dogovoru" na globalnom nivou. Evropska unija je najveća ekonomija sveta, sa oko 500 miliona potencijalnih potrošača čiju kupovnu moć odražava BDP od oko 30.000 evra po glavi stanovnika. To je više nego dobar motiv da se globalne i nacionalne kompanije sa sedištem izvan EU, a koje se obraćaju evropskim korisnicima, prilagode novoj regulativi. Ako taj motiv ne bude dovoljan, tu je pretnja kaznom u visini i do 20 miliona evra ili 4% godišnjeg obrta u slučaju kršenja prava građana Unije.

Vremena za prilagođavanje bilo je na pretek. GDPR je usvojen 2016. a rok od dve godine ostavljen je upravo zato da bi se poslovanje usaglasilo sa izmenama. Očekivano trajanje ove Opšte uredbe je oko 20 godina, pa je već sada izvesno da ćemo se u narednim decenijama dosta susretati sa GDPR-om i njegovim tumačenjima, dok će ekpertiza u ovoj oblasti biti od značaja za praktično svakog profesionalca.

Uredba se odnosi na podatke o ličnosti bez obzira na koji se način oni prikupljaju, obrađuju i čuvaju – na internetu ili na papiru – ali su globalna Mreža i njen digitalni ekosistem u fokusu nove paradigme.

PRIVAT-NOST I PODACI O LIČNOSTI

PRIVATNOST I PODACI O LIČNOSTI

UNIVERZALNA DEKLARACIJA O LJUDSKIM PRAVIMA Ujedinjenih nacija (1948), u članu 12, navodi: ''Niko ne sme biti izložen proizvoljnom mešanju u privatni život, porodicu, stan ili prepisku, niti napadima na čast i ugled. Svako ima pravo na zakonsku zaštitu protiv ovakvog mešanja ili napada.''

EVROPSKA KONVENCIJA ZA ZAŠTITU LJUDSKIH PRAVA I OSNOVNIH SLOBODA (1950) izričito štiti pravo na privatnost u članu 8: ''Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.'' Međunarodni pakt o građanskim i političkim pravima (1966) na sličan način potvrđuje ovu garanciju, u članu 17. Takođe, Povelja o fundamentalnim pravima Evropske unije (2000) garantuje pravo na privatni i porodični život (član 7) i posebno pravo na zaštitu podataka o ličnosti (član 8).

Uopšten koncept privatnosti teško je definisati pravničkim jezikom, a ponekad izmiče i svakodnevnoj komunikaciji. Tako je u svom izveštaju povodom predmeta Van Ostervijk protiv Belgije iz 1979. godine, tadašnja Evropska komisija za ljudska prava (danas Evropski sud) domen privatnog života opisala jednostavnim rečima, kao ''pravo čoveka da živi kako želi, zaštićen od javnosti''. Kako normirati pravo koje toliko zavisi od individualnih želja i potreba, konteksta u kom se ispoljava?

Tokom istorije, kada su prava i slobode ljudi zavisili od naslednog ili stečenog statusa u društvu, zaštita intimnog prostora tretirana je kao luksuz privilegovanih. Na tlu Evrope, ''počev od 16. veka, izraz 'privatan' počeo je da se koristi u kontekstu nezavisnosti i sfere intime, a od 17. veka ovaj pojam označava vrednost mirnog života i poštovanje doma''.[1]

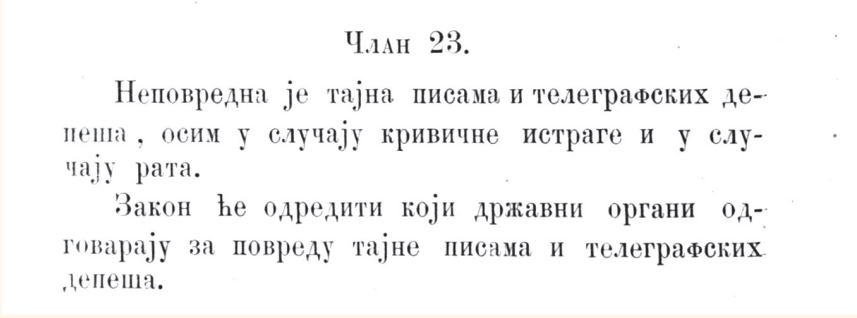
Krajem 19. veka dvojica američkih pravnika, Semjuel Voren i Luis Brendis, objavili su esej o pravu na privatnost, koje su opisali kao ''pravo da se bude ostavljen na miru''.[2] Njihova analiza udarila je temelje čitavom savremenom korupusu zaštite privatnosti, privatne komunikacije, pa i podataka o ličnosti. Istovremeno, predvideli su i neka ograničenja ovog prava, kao što su javni interes ili pristanak na objavljivanje privatne komunikacije, koja važe i danas.

Već i sama potreba da se bude ''ostavljen na miru'' ukazuje da postoji uznemiravanje koje treba ograničiti i regulisati. Dok s jedne strane raste svest o ličnim pravima svakog pojedinca, izvan telesnih i materijalnih granica, s druge strane, kako se tada govorilo, ''izumi i poslovne metode'' omogućavaju sve dublje i masovnije narušavanje tih prava. U vreme Vorena i Brendisa, to su bili fotoaparati koje je tehnološki razvoj smanjio od glomazne skalamerije do lako prenosivog uređaja, dok su promene na tržištu zatrpale štampana sredstva javnog informisanja trač-rubrikama i klevetanjem u cilju dizanja tiraža. Pravnici su smatrali da zakon mora da odgovori na razvoj tehnologije, svesni da se taj razvoj neće zaustaviti na fotoaparatima.

Danas se pravo na privatnost ceni kao jedno od osnovnih ljudskih prava, a svoj pun razvoj u pravnim tradicijama Amerike, Britanije i kontinentalne Evrope doživljava tokom 20. veka. Ugrađeno je u mnoge ustave, međunarodne konvencije i nacionalne regulative savremenih društava koja su prihvatila dogovorene standarde.

01 Evropsko pravo ljudskih prava, Beograd, 2016. rm.coe.int
02 ''Pravo na privatnost'', Harvard Law Review, 1890. faculty.uml.edu

Najraniji trag prava na privatnost kod nas, u skladu sa tadašnjim evropskim tokovima, zabeležen je u ustavu kraljevine Srbije iz 1888. godine gde se, u članu 15, garantuje nepovredivost stana, dok se članom 23 štiti nepovredivost tajnosti pisama i telegrafskih depeša. Slični instrumenti bili su predviđeni i u ostalim ustavima Srbije kroz istoriju, uključujući i period dve jugoslovenske zajednice.



Члан 23.

Неповредна је тајна писама и телеграфских депеша, осим у случају кривичне истраге и у случају рата.

Закон ће одредити који државни органи одговарају за повреду тајне писама и телеграфских депеша.

U važećem ustavu Srbije iz 2006. pravo na privatnost nije definisano, a izričito se prepoznaje samo u slučaju zaštite potrošača (član 90). Međutim, Ustav detaljno uređuje prava i slobode građana kroz koje se privatnost ostvaruje, kao što su dostojanstvo i integritet ličnosti, nepovredivost stana, tajnost pisama i drugih sredstava komunikacije.

Posebnim članom (42) garantuje se zaštita podataka o ličnosti, zabranjuje se "upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni" i prepoznaje pravo svakog da "bude obavešten o prikupljenim podacima o svojoj ličnosti", kao i pravo na sudsku zaštitu u slučaju njihove zloupotrebe.

Pravnici kažu da je podatak o ličnosti svaka informacija o nekoj osobi koja govori nešto o njenim ličnim karakteristikama, navikama, opredeljenjima, identitetu. Da bi neka informacija stekla "status" podatka o ličnosti, potrebna je mogućnost da se identifikuje ili bliže odredi osoba na koju se podatak odnosi. Šta to u stvari znači?

Ime i prezime, boja očiju, matični broj, adresa, zdravstveni karton, broj pasoša... sve su to informacije koje nedvosmisleno opisuju pojedinu ličnost. Neke od njih su zajedničke mnogim ljudima - kao što su uzrast, krvna grupa ili mesto rođenja - ali kad znamo na koga se odnose, te informacije bliže određuju konkretnu osobu. Drugi podaci o ličnosti su jedinstveni, odnose se samo na jednu jedinu osobu na čitavoj planeti. Takve podatke nazivamo identifikatorima, zato što samostalno mogu odrediti jednu osobu.

Neke informacije su očigledne u prisustvu osobe na koju se odnose, kao što su boja kože ili kose, dok druge možemo saznati samo uz pomoć posebnih alata – recimo, otisak prsta, krvnu grupu ili pojedine karakteristike ličnosti. Bez obzira da li su očigledni svima ili ih utvrđuju samo stručnjaci, rukovanje ličnim podacima se detaljno uređuje kao sastavni deo prava svih ljudi da slobodno odlučuju o svom životu.

PRIVATNOST I PODACI O LIČNOSTI NA INTERNETU

Čini se da je u fizičkom prostoru lakše održati svest o privatnoj sferi. Svesni smo da slobodno odlučujemo s kim ćemo stupati u odnose: poslovne, prijateljske ili ljubavne; s kim ćemo podeliti detalje iz svog života, kome ćemo dozvoliti da nam priđe - a koga ćemo držati na distanci.

Konačno, privatnost nije nekakva zona tajni kojih se stidimo, već dragocenost koju s drugima delimo štedljivo i s pažnjom. Svakodnevno štitimo i svoju, ali i privatnost ljudi koji pripadaju našem ličnom društvenom krugu - privatnost svoje dece, partnera, porodice, prijatelja...

... ili je bar tako bilo sve do eksplozije komunikacije na društvenim mrežama, gde iz sata u sat izveštavamo čitav svet o tome šta smo jeli, gledali, slušali, gde smo putovali, s kim smo u vezi i da li je komplikovano.

Ako ove statuse i objavljujemo uz punu svest o potencijalno ogromnoj publici koja tako stiče uvid u našu privatnu svakodnevicu, mnoge aktivnosti na internetu izmiču našoj pažnji mada su takođe čvrsta svedočanstva o intimi. Neke od tih aktivnosti vidljive su prijateljima na mreži – šta delimo, šta nam se sviđa, gde se krećemo, s kim smo se povezali, sa kim smo u učestaloj interakciji, kom događaju smo prisustvovali.

Najčešće, međutim, uopšte nismo svesni jednog dubljeg nivoa, na kom kompjuteri, pametni telefoni i računarska infrastruktura svake sekunde proizvode podatke bez kojih kretanje između digitalnog i fizičkog sveta ne bi bilo moguće. Lokacija sa koje se povezujemo na internet, uređaji i usluge koje koristimo, sajtovi koje posećujemo – drugim rečima, naše ponašanje na internetu zabeleženo je detaljno, u autentičnom obliku. Uz pomoć jedinstvenog identifikatora uređaja koji koristimo i njegove IP adrese na internetu, svaki lajk predstavlja podatak koji otkriva deo naše intime.

Možda je privatnost izgubila društvenu i ličnu vrednost koju je imala u 20. veku, ali red je da znamo čega smo se i zašto odrekli - makar zbog prilike da razmotrimo moguće posledice života u okruženju u kom svako može znati sve o nama, pratiti svaki naš korak i umesto nas birati stvari i ljude koji bi trebalo da nam se sviđaju.

Podaci koje ostavljamo za sobom na internetu nisu bezvredni. Uostalom, tržišna vrednost Fejsbuka, najpopularnije besplatne platforme za druženje, prošle godine je prešla granicu od 500 milijardi dolara. Pokrenuta je pre samo 14 godina iz studentske sobe, a njen poslovni model je gotovo u potpunosti zasnovan na preprodaji podataka o ponašanju korisnika na tržištu gde korisnici postaju roba.

GDPR - PRINCIPI I PRAVA

GDPR - PRINCIPI I PRAVA

Internet je moguć upravo zahvaljujući automatskoj razmeni i obradi velikih količina podataka, od kojih su mnogi prepoznati kao **podaci o ličnosti – informacije ili delovi informacija na osnovu kojih je moguće identifikovati osobu kojoj ti podaci pripadaju.** To više nisu samo ime i prezime, adresa, zdravstveni karton ili bankovni račun, već i IP adresa uređaja sa kog se povezujemo na internet, metapodaci koje uređaj generiše tokom rada, digitalni tragovi koje ostavljamo za sobom svakodnevno.

Budući da je reč o oblasti koja zadire u temelje društva, privrede, državne uprave i ličnih prava, GDPR je dugačak i složen pravni dokument. Visok nivo opštosti omogućava da se svi procesi obrade podataka o ličnosti urede jednoobrazno, bez obzira na pojedinačne sektore, razlike među ljudima čiji se podaci obrađuju ili karakteristike same obrade. Shodno tome, mnogi koncepti koji su ovim propisom uspostavljeni ne mogu se brzo i jednostavno razjasniti ni primeniti. Upravo se po ovom pitanju evropski regulatorni okvir značajno razlikuje od američkog, koji pojedinačnim propisima uređuje privatnost u obrazovnom, zdravstvenom, radnom i drugim okruženjima. GDPR je jedan propis koji se na istovetan način primenjuje u svim sektorima u kojima se obrađuju podaci o ličnosti.

Kao pravni akt koji se neposredno primenjuje na terioriji EU, GDPR uspostavlja osnovna pravila i principe s kojima je neophodno uskladiti svako poslovanje koje dolazi u dodir sa podacima o ličnosti. Pojedine države članice EU su ovlašćene da svojim nacionalnim propisima urede pojedina pitanja i posebne oblike obrade.

ŠEST OSNOVNIH PRINCIPA, opisanih u članu 5 Uredbe, u znatnoj meri predstavljaju poznata i logična načela zaštite podataka o ličnosti, od kojih su mnoga su već ugrađena u nacionalna prava koja poznaju ovu vrstu propisa. Suštinsku novinu predstavlja njihova nesporna primena na digitalno okruženje, kao i težina odgovornosti organizacija koje prikupljaju i obrađuju podatke na internetu. Zahtevi kojima internet kompanije moraju da se prilagode, najavljuju temeljnu reformu onlajn poslovanja.

1. PODACI O LIČNOSTI SE PRIKUPLJAJU ZAKONITO, PRAVIČNO I NA TRANSPARENTAN NAČIN

Državne ustanove, privatne kompanije i građanske organizacije moraju poštovati zakon kad uzimaju podatke građana, pa se **zakonitost** odnosi na sva propisana ograničenja i uslove prilikom obrade podataka. Građani nisu dužni da poznaju svaki od tih uslova, ni složene zakonske procedure. To je obaveza onih na koje se zakon odnosi, koji obrađuju naše podatke. Međutim, uvek je dobro da znamo svoja prava, kako bismo umeli da razlikujemo pravičan odnos prema sebi. Naše je pravo, između ostalog, da znamo šta da očekujemo od usluge koju nam nude državne ili privatne organizacije i kakav je uticaj takve usluge na našu privatnost, što znači da su one dužne da se pridržavaju načela **transparentnosti.**

ZAKONITA OBRADA podataka podrazumeva da su nam podaci uzeti ili na osnovu našeg pristanka, po sili zakona ili u skladu sa nekim drugim, valjanim pravnim osnovom. Za upis u školu, prijem kod lekara, otvaranje računa u banci ili kod internet provajdera, obavezno je utvrđivanje identiteta, zbog čega pristanak nije prepušten našem izboru. Možemo birati banku u kojoj ćemo otvoriti račun, ali svaka ima obavezu da nas identifikuje, što znači da će nam uzeti lične podatke. Uobičajeno, propisi o zaštiti podataka o ličnosti ostavljaju prostor i za izuzetke – kada nije bilo ni pristanka korisnika ni zakonske obaveze provajdera, ali je u nekoj konkretnoj situaciji obrada podataka o ličnosti neophodna kako bi se zaštitio neki vitalni interes pojedinca ili zajednice. Takav izuzetak se strogo procenjuje i ne može služiti kao rupa u zakonu za zloupotrebe.

Kada nam neko uzme podatke o ličnosti, ili uz naš pristanak ili po sili zakona, a krši bilo koje druge obaveze iz propisa o zaštiti podataka o ličnosti, takva obrada podataka o ličnosti nije zakonita.

Što se budemo bolje upoznavali sa pravima koja imamo kao ličnosti, jasnija će nam biti i **pravičnost** u poslovanju organizacija koje obrađuju naše podatke. Znaćemo da su organizacije dužne da nas tačno i potpuno informišu, da ne iskorišćavaju naše tehničko ili pravno neznanje, ili nizak nivo digitalne pismenosti, da nas ne stavljaju u neravnopravan položaj, niti da nas ucenom ili obmanom navode na pristanak.

PRAVO NA IZBOR I PRISTANAK znači da nam onaj ko želi da pristupi našim podacima, nedvosmisleno pruži mogućnost izbora. Pošto nas je obavestio da prikuplja podatke i kako ih koristi, dužan je da nam za to zatraži pristanak. Ranije je pristanak bilo moguće obezbediti tako što nam servis ponudi već čekiranu opciju, ili tako što je opcija "ne slažem se" prikazana u manje vidljivoj formi, pa čak i bez ikakvog posebnog upita, već samo na osnovu činjenice da smo ostali na sajtu ili preuzeli aplikaciju. Sada je validan pristanak samo onaj koji se daje izričitom izjavom volje, koji se može evidentirati i pružiti na uvid, pod uslovom da se daje na osnovu konkretnog obaveštenja o tome šta je to na šta mi u stvari pristajemo. Ovaj zahtev znači i da se korišćenje usluge ne može uslovljavati pristankom na obradu podataka o ličnosti koji nisu neophodni za konkretnu uslugu. Pravo na izbor podrazumeva i pravo da se kasnije predomislimo i odustanemo od usluge, pri čemu će povlačenje pristanka morati da bude jednostavno kao i davanje. Kada poželimo da obrišemo nalog na nekoj onlajn platformi, nećemo morati da prekopavamo opcije, popunjavamo dugačke formulare i slično.

Dva istraživača sa Univerziteta Berkli i Tehničkog univerziteta u Drezdenu su testirali alternativne forme obrazaca za pristanak na obradu podataka na uzorku od oko 80.000 korisnika interneta. Oni kojima je prikazana poruka da je njihov pristanak neophodan zajedno sa potvrdnim izborom "slažem se", u 26% više slučajeva su prihvatali uslove korišćenja u poređenju sa ispitanicima kojima su na fer način ponuđene opcije "da" i "ne".[3] Dizajn koji nas navodi da dajemo pristanak umesto da nudi stvarni izbor, što je do sada bilo gotovo pravilo, neće biti moguć po GDPR-u.

Čak i kada kompanija u međuvremenu razvije novu aplikaciju, ili novu uslugu u okviru postojeće aplikacije, ili novu primenu podataka vezanih za naš korisnički profil - dužna je da nam traži novi pristanak. Ako se na Tviteru, na primer, pojavi usluga pretrage lokalnih restorana ili telefoniranja, ugrađena u osnovnu platformu, stari dogovor koji važi za korišćenje platforme neće obuhvatati druge servise.

Načelo po kom kompanije ne mogu da vežu svoje različite usluge u jedan paket za koji traže jedan pristanak ("sve ili ništa"), svečano je probilo led primene Opšte uredbe kada je, minut posle ponoći 25. maja 2018. austrijski pravnik i aktivista podneo tužbu protiv Gugla, Fejsbuka i povezanih kompanija pred sudovima četiri evropske države. Sudsko tumačenje u ovom slučaju, umnogome će odrediti pravac razvoja najvećih globalnih onlajn servisa.

TRANSPARENTNOST znači da onaj ko želi da koristi naše podatke, mora jasno da nas obavesti o svojoj nameri pre nego što zatraži dozvolu za pristup našim podacima, mora nam objasniti za šta su mu potrebni naši podaci, kao i koliko dugo namerava da ih čuva. Takvo obaveštenje treba da bude lako dostupno, čitljivo, razumljivo, neuslovljeno i blagovremeno dopunjeno svakom kasnijom promenom u poslovanju koja se tiče obrade podataka o ličnosti. Stari običaji odlaze u istoriju: sićušna slova, obaveštenja sakrivena u predugačkim "pravilima korišćenja", na jeziku koji teško razumeju čak i pravnici, dostupna tek pošto je prikupljanje podataka već počelo... Drugim rečima, onaj ko želi da pristupi našim podacima dužan je da nam pruži sažetu i konkretnu informaciju o tome ko prikuplja koje podatke, koliko dugo ih čuva i koja su naša prava u slučaju da želimo da pregledamo svoje prikupljene podatke, da ih obrišemo, i slično. Za usluge koje su namenjene deci i mladima, ovakva obaveštenja moraju biti prilagođena uzrastu korisnika.

03 „No one reads terms of service, studies confirm", The Guardian, bit.ly/2mhOJxw

PREUZMITE ILUSTROVANI VODIČ O BEZBEDNOSTI NA INTERNETU ZA DECU:
resursi.sharefoundation.info/sr/publikacije/

Upućeni kažu da politike privatnosti za korisnike igrice Tetris imaju 407.000 reči; poređenja radi, cela Tolkinova trilogija "Gospodar prstenova" ima 450.000 reči. Procenjuje se da bi za čitanje svih digitalnih ugovora koje prosečan građanin sklapa kada pristane na razne onlajn usluge, bilo neophodno oko 250 sati godišnje. Profesori sa Jork univerziteta u Torontu i Univerziteta u Konektikatu su na uzorku od 543 studenta pokazali da se iza opcije "prihvatam uslove korišćenja" krije najveća laž na internetu. U njihovom istraživanju je, zarad korišćenja izmišljene društvene mreže, 98% ispitanika pristalo da podeli svoje podatke sa Agencijom za nacionalnu bezbednost (NSA), poslodavcima, pa čak i da preda svoje prvorođeno dete.[4]

S druge strane, različite inicijative i građanske organizacije širom sveta razvijaju alate za proveru ovih digitalnih ugovora. Tako projekat "Uslovi korišćenja: Nepročitano" ocenjuje uslove korišćenja onlajn servisa prema njihovom uticaju na privatnost i druga prava potrošača, što znatno olakšava korisnicima da donesu odluku da li će pristati na uslove neke usluge ili ne.[5]

GDPR sada propisuje da ovi uslovi budu sažeti, jasni i razumljivi prosečnim građanima.

PRAVO NA PRISTUP, odnosno uvid, jeste jedan od gradivnih zahteva Opšte uredbe: kad ostvarimo pravo na pristup, primenjuju se i druga prava. Prvi test dobre informisanosti o obradi ličnih podataka biće obaveštenje o posebnoj službi ili ovlašćenoj osobi u okviru organizacije, kojoj se možemo obratiti da bismo ostvarili svoje pravo na uvid.

Pristup ličnim podacima podrazumeva da nas organizacija informiše koje podatke o nama je prikupila, bez obzira da li smo te podatke sami dali ili su prikupljeni iz drugih izvora, da li se naši podaci obrađuju u okviru automatizovanih procesa, kao i da nas obavesti o pravima koje zadržavamo nad svojim podacima – brisanje, ispravka, prigovor i drugo.

Rok za odgovor na zahtev za pristup ličnim podacima ograničen je na mesec dana, uz neke dozvoljene izuzetke. Po pravilu, pristup se ostvaruje besplatno ili uz nadoknadu samo tehničkih troškova.

04 Obar, Jonathan A. i Oeldorf-Hirsch, Anne, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (2016). Istraživanje dostupno na engleskom jeziku: https://ssrn.com/abstract=2757465
05 "Terms of Service; Didn't Read" tosdr.org

SCENA

Dobili ste posao u poznatoj firmi. Po sili zakona, poslodavac je u obavezi da utvrdi vaš identitet i da vam uzme sve one podatke koji su mu potrebni za isplatu plata, poreza i doprinosa. Osim zakona, firma ima i svoje interne propise o privatnosti i podacima o ličnosti gde se, između ostalog, nalazi informacija da poslodavac zadržava pravo na uvid u poruke koju zaposleni šalju i primaju sa poslovnog mejla. Međutim, od kolega saznajete da će vam poslodavac tražiti i uvid u zdravstveno stanje, jer ,,voli da brine o svojim radnicima''.

2. PODACI O LIČNOSTI SE PRIKUPLJAJU ZA KONKRETNE, JASNE I ZAKONITE SVRHE I NE MOGU SE DALJE OBRAĐIVATI NA NAČIN KOJI NIJE USKLAĐEN SA PRIMARNOM SVRHOM

Ovi zahtevi zajedno čine **princip ograničenja svrhe**, što znači da se podaci prikupljeni za jedno, ne mogu koristiti za nešto drugo. Ako nam aplikacija traži pravo ime, fotografiiju i pristup geolokaciji na smartfonu za profil na nekoj društvenoj mreži, te podatke ne može da koristi za druge svrhe. S novom regulativom, kompanije će morati bolje da promisle svoje poslovne modele i ponudu za svoje korisnike. Ako nameravaju da preprodaju naše podatke, o tome će prethodno morati da nas jasno obaveste i da zatraže naš pristanak.

Do sada je kao svrha prikupljanja i obrade podataka moglo da prođe uopšteno obećanje ''unapređenja korisničkog iskustva'' ili nejasno objašnjenje da se podaci traže ''za potrebe marketinga''. Provajderi usluga će sada morati da jasno i nedvosmisleno navedu konkretne namene prikupljenih podataka, ali i da vode računa da su te namene u skladu sa drugim zakonima, uključujući i propise o zabrani diskriminacije, na primer. Takođe, ograničenost svrhe obuhvata i usklađenost dalje, odnosno ponovne upotrebe podataka – to znači da čak i kada smo dali pristanak na dalju upotrebu podataka, izvan primarne svrhe usluge koju koristimo, ta ponovna upotreba ne može drastično da odstupa od svrhe na koju smo pristali. Usklađena ponovna upotreba podataka o našem zdravstvenom stanju, na primer, mogla bi da bude statistička ili obrada za naučne i nastavne svrhe, ali nikako preprodaja reklamnim agencijama.

SCENA

Fejsbuk vas je obavestio da je, zbog primene GDPR, promenio svoje politike privatnosti i ponudio vam novi ,,dogovor'' u zamenu za vaše podatke. Kao i do sada, platforma skuplja podatke o vama, vašem onlajn ponašanju i interesovanjima, koje preprodaje drugim kompanijama za ciljano oglašavanje. To je njihov poslovni model na koji vi pristajete, informisani i svesni da uslugu korišćenja Fejsbuka plaćate svojim podacima o ličnosti. Da li vaš pristanak na razmenu sa Fejsbukom važi samo za korišćenje osnovne platforme ili za sve aplikacije i usluge koje se nude na mreži?

3. PRIKUPLJAJU SE SAMO DOVOLJNI, ODGOVARAJUĆI I PODACI KOJI SU NEOPHODNI

Ove zahteve zovemo i princip svedenosti ili minimizacije, a on podrazumeva da se ne gomilaju podaci o ličnosti preko granice koja je neophodna za uslugu koju koristimo i mimo uslova na koje smo na početku pristali. Ukratko, vrsta i količina podataka koje se traže treba da odgovaraju usluzi: ako je za korišćenje neke aplikacije za obradu fotografija dovoljno da joj omogućimo pristup kameri na svom telefonu, aplikacija ne može da nam traži dozvolu za praćenje komunikacija ili podatke o onlajn kupovinama. Za kropovanje fotografija nije potrebna infomacija o našim kupovnim navikama.

Podsetimo se primera iz oflajn sveta u Srbiji: prilikom ulaska u pojedine državne institucije ili poslovne zgrade, na portirnicama je zadržavanje ličnih karata građana redovna praksa. Portir će neretko i bespotrebno prepisati brojne podatke građana, nakon što im je utvrdio identitet. Slične situacije sa prekomernom obradom i prikupljanjem podataka dešavaju se i prilikom reklamacija robe, kada se građanima traži matični broj ili drugi podaci o ličnosti koji nisu potrebni za ostvarivanje prava. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti godinama upozorava da je takva praksa nezakonita, ali se od nje nažalost ne odustaje.

SCENA

Skinuli ste aplikaciju Pokemon Go i krenuli u poteru. Prilikom instalacije, obavešteni ste da aplikacija prikuplja vaše geoprostorne podatke: gde ste bili, koliko dugo ste se zadržali na jednom mestu i kojom brzinom ste se kretali. Takođe, obavešteni ste i da se ti podaci ustupaju ili preprodaju drugim kompanijama za targetirano oglašavanje, detaljno mapiranje fizičkog prostora i slično. Dali ste svoj pristanak i završili instalaciju. Međutim, pokazalo se da aplikacija ima pristup i vašem Gmail nalogu, sadržaju mejlova i poruka.

4. PRIKUPLJENI PODACI O LIČNOSTI SU TAČNI I AŽURNI

Mada se očekuje da su organizacije prirodno motivisane da redovno ažuriraju podatke o svojim korisnicima, kako bi mogle efikasno da isporuče i naplate uslugu, ne utiče kvalitet podataka uvek na njihovo poslovanje. Često, pogrešni podaci mogu izložiti riziku korisnika, a ne kompaniju. Sem toga, zastareli podaci o tome gde smo ranije stanovali, na primer, ili kakav nam je pre pet godina bio porodični ili finansijski status, čine grupu podataka o našoj prošlosti za koju je organizaciji potreban poseban osnov za obradu, izvan usluga koje nam pruža. Ovaj princip bi mogao biti značajan za rad državne uprave u zemljama u razvoju, gde digitalizacija javnih usluga nije sprovedena do kraja. Tačnost i ažurnost podataka o ličnosti građana, naime, jasna je obaveza onih koji prikupljaju i obrađuju podatke.

Princip tačnosti obuhvata jedno novo pravo, formulisano tokom ekspanzije digitalne sfere. To je pravo na brisanje i zaborav, odnosno pravo na brisanje podataka o ličnosti, kao i brisanje svih veza (linkova) koje vode ka našim podacima. Sprovođenje ovog principa posebno će uticati na svakodnevni život i poslovanje na internetu. Stalno treba imati na umu da podaci o ličnosti na internetu nisu samo ime i prezime, ili slike sa letovanja koje delimo na instagramu, već i svaki lajk na fejsu ili kolačići koje naš kompjuter ili telefon razmenjuju sa sajtovima, kao i razni drugi elektronski zapisi koji svedoče o našem onlajn životu. U slučaju kada prestanemo da koristimo neku uslugu ili smo promenili kompaniju koja tu uslugu pruža, povukli smo pristanak na pristup našim podacima

ili pristup našim podacima više nije neophodan, imamo pravo da tražimo brisanje svojih podataka, kao i veza koje su u međuvremenu uspostavljene. Ovaj segment "zaborava" u nekim situacijama može biti teško ostvariv u potpunosti, s obzirom na prirodu interneta, nekontrolisano umnožavanje sadržaja i deljenje linkova, ali se od organizacija očekuje da u tom pravcu preduzmu razumne korake u okviru svojih mogućnosti.

Za razliku od drugih, ostvarivanje prava na zaborav se odmerava u svakom pojedinačnom slučaju, budući da se može naći u direktnoj suprotnosti sa slobodom izražavanja i pravom na pristup informacijama od javnog značaja.

"Pravo na zaborav" ugrađeno je u pravni okvir EU presudom Suda pravde EU u slučaju "Google Spain" iz 2014. godine. Državljanin Španije Mario Kosteha Gonzales je od kompanije Gugl tražio da se iz rezultata pretrage uklone informacije o njegovim dugovima koje su bile objavljene na sajtu lokalnih novina davnih 90-ih godina. Iako je dugove davno vratio, kada se guglalo njegovo ime ponovo je u rezultatima izlazio isti članak iz lokalnih novina, koji više nije bio relevantan. Sud je presudio u Gonzalesovu korist, čime je praktično uspostavljeno pravo građana EU da od servisa za pretraživanje (Gugl, Jahu, Bing, itd) traže da se iz rezultata pretrage traže brišu veze ka podacima koji su "neadekvatni, nerelevantni ili prekomerni u odnosu na svrhu obrade".

5. U OBLIKU KOJI OMOGUĆAVA IDENTIFIKACIJU LIČNOSTI NA KOJU SE ODNOSE, PODACI SE ČUVAJU ONOLIKO DUGO KOLIKO JE NEOPHODNO ZA SVRHU ZA KOJU SE OBRAĐUJU

Ovo je **princip ograničenog čuvanja** i znači da se lični podaci građana brišu ili anonimizuju kada ispune svoju namenu. Zadržavanje podataka mora biti zakonito i opravdano svrhom obrade, a organizacije koje ih čuvaju ne smeju čekati da se mi setimo da proverimo da li su nas izbrisale iz svojih arhiva, pod izgovorom da će nas zauvek smatrati svojim klijentima, već to moraju učiniti automatski. Ako smo svoje podatke dali za jednokratnu uslugu, naši podaci ne mogu da se čuvaju i nakon što je transakcija završena.

Ova obaveza je usko povezana sa principima svedenosti i tačnosti i, mada može delovati manje važno, očekuje se da ozbiljno protrese ekonomiju podataka na internetu. U digitalnom okruženju, naši uređaji spontano generišu podatke čim se povežu na internet, a tržišna vrednost tih podataka neretko se meri dužinom njihove obrade - zarad profilisanja, ukrštanja sa drugim, novim setovima podataka, preprodaje i ciljanog oglašavanja. Poštovanje ovog principa ne znači da će ekonomija podataka postati nelegalna; prosto, znači da će organizacije od početka morati da budu jasne po pitanju šta žele da rade s našim podacima i koliko dugo.

SCENA

Koristili ste usluge turističkog onlajn agenta koji je, u skladu sa ugovorom, u jednom trenutku imao pristup podacima o vašoj fizičkoj adresi, broju telefona i mejlu, ali bez dozvole za duže zadržavanje podataka. Sudeći po reklamama i pozivima koje vam upućuje svake sezone, agent nije poštovao obavezu ograničenog čuvanja. Uskoro saznajete da je u agenciji došlo do bezbednosnog incidenta, kada su kompromitovani svi podaci njihovih stari i novih korisnika, uključujući i vaše.

Prenosivost i razmenjivost znači da imamo pravo na preuzimanje, odnosno prenos svojih podataka iz jednog u drugi sistem bez dodatnih komplikacija, jer su podaci prikupljeni i obrađeni u standardnim, mašinski čitljivim formatima. Na taj način je potrošačima omogućeno da promene organizaciju koja im pruža uslugu, recimo, praćenja fitnes aktivnosti, zdravstvenog stanja ili čuvanja fotografija, bez gubitka na kvalitetu usluge ili ulaganja dodatnog vremena. Ovo je takođe nov princip zaštite podataka o ličnosti koji će važiti samo u digitalnom okruženju, očigledno neprimenjiv na podatke prikupljene ručno (papirna dokumentacija i slično). Značajno ograničenje ovom principu čine i podaci koji se obrađuju po zakonskoj obavezi, bez pristanka, ili na način koji iz sigurnosnih razloga nije u standardnoj formi. Podaci izvedeni iz osnovnih podataka koje smo dali, takođe su izuzeti iz ovog principa. Stoga se očekuje da će prenosivost i razmenjivost podataka uticati pre svega na zaštitu potrošača u sferi onlajn trgovine i usluga.

Uzor ovom zahtevu je promena telefonske mreže u fizičkom okruženju: recimo, odlučili ste da promenite kompaniju, jer druga ima niže cene ili bolju pokrivenost. Imate mogućnost da broj telefona koji vam je dodeljen u prvoj kompaniji, ponesete sa sobom, uključujući i pozivni kod.

Međutim, na polju onlajn usluga princip prenosivosti tek će se razvijati do pune primene. Tviter, recimo, već godinama omogućava korisnicima da preuzmu celokupnu arhivu svojih objava, klasifikovanu po mesecima i godinama. Tviteraši mogu među sobom da razmenjuju liste blokiranih naloga. Po pravilu, međutim, velike kompanije omogućavaju prenos sadržaja samo unutar porodice aplikacija koje su u njihovom vlasništvu. Takođe, ni svi formati u širokoj upotrebi ne odgovaraju strogoj definiciji "mašinski čitljivog formata", kao što je PDF koji bitno ograničava automatsku obradu podataka iz sadržaja. Lako i jednostavno preuzimanje podataka koji su vezani za lični nalog na društvenim mrežama, podrazumeva i posebne alate.

Decentralizacija usluga na internetu mogla bi dovesti do razvoja niza platformi sličnih već postojećim: ako bi se pojavila alternativa Fejsbuku za koju bismo se opredelili zato što, za razliku od globalnog giganta, ne prodaje podatke svojih korisnika, trebalo bi da možemo da prebacimo i svoju celokupnu arhivu na drugu mrežu.

6. OBRADA PODATAKA O LIČNOSTI SE OBAVLJA U BEZBEDNIM TEHNIČKIM I ORGANIZACIONIM USLOVIMA KOJI OMOGUĆAVAJU ČUVANJE INTEGRITETA I POVERLJIVOSTI PODATAKA

BEZBEDNOST znači da je onaj ko obrađuje i čuva naše lične podatke, dužan da preduzme sve razumne mere kako bi sprečio njihovo gubljenje, oštećenje ili neovlašćen pristup i zloupotrebu. Bez obzira da li smo mi svesni svih postojećih rizika, da li poznajemo tehnologiju zaštite i da li našim podacima uopšte preti neka realna opasnost, svako ko rukuje podacima o ličnosti ima obavezu da im garantuje bezbednost. Ovo je stari princip zaštite, ali je u novoj regulativi pojačan strožim obavezama i proširenjem odgovornosti. Internet je prerastao u džinovsku fabriku podataka, gde u prikupljanju i obradi za samo jednu jednostavnu uslugu mogu učestvovati brojne organizacije. Bezbednost naših podataka više nije obaveza samo one kompanije kojoj smo dali izričit pristanak, već i svih njenih podizvođača koji će rukovati našim podacima.

- **Podrazumevana privatnost** znači da je zaštita podataka o ličnosti kao standardna vrednost ugrađena ne samo u uslugu koju koristimo, već i u tehničko i organizaciono okruženje u kom se ta usluga obavlja. Decenijama je razvoj digitalnih tehnologija bio vođen komercijalnim načelima jeftine proizvodnje i brze distribucije, dok su se rizici po privatnost tretirali kao propusti koji se krpe u hodu. Sada se od proizvođača i provajdera, ne samo na internetu, zahteva da sistem zaštite podataka o ličnosti ne bude stvar

naknadnog izbora korisnika, te da ne zavisi od njihove svesti o rizicima ili tehničkih znanja. Privatnost mora biti unapred obezbeđena, a korisnicima se kasnije prepušta odluka da samostalno snize stepen svoje bezbednosti.

U tehničkom slengu, ova obaveza se opisuje još i kao privatnost/zaštita podataka "po dizajnu i difoltu".

PRIVATNOST PO DIZAJNU se odnosi na rešenja koja se koriste prilikom obrade podataka. Najčešće je to pseudonimizacija, postupak u kom se podaci o ličnosti konkretne osobe automatski zamenjuju pseudonimima, veštačkim identifikatorima, da bi ih u svakom trenutku bilo moguće vratiti u autentičan oblik. Veza između pravog podatka i pseudonima koji ga menja, čuva se zasebno. Na ovaj način se bitno smanjuje rizik prilikom obrade podataka, bilo da je reč o organizaciji setova podataka, skladištenju, transferu, ili sličnom.

Pseudonimizacija se može izvesti pukim maskiranjem podatka ili njegovom enkripcijom. Na primer, kada objavljuju svoje presude, sudovi u Srbiji maskiraju imena osoba u sporu - zamenjuju ih slovima "aa, bb, vv" i tako dalje, azbučnim redom. Podaci u bankarskim transakcijama se enkriptuju – može ih čitati samo onaj ko ima jedinstveni ključ za dekripciju.

Anonimizacija znači potpuno brisanje podataka o ličnosti, bez mogućnosti povratka pravih informacija. Koristi se kada je prestala obrada podataka o ličnosti, ali se nastavlja sa obradom izvedenih podataka za koju je identitet ljudi nevažan, kao što su statističke svrhe.

PODATAK O LIČNOSTI	PSEUDONIMIZACIJA (MASKIRANJE)	ANONIMIZACIJA
Petar Petrović	šlb 123	xxx xxx
Milan Petrović	šbb 123	xxx xxx
Milan Đorđević	šbb 456	xxx xxx
Petar Đorđević	šlb 456	xxx xxx

U primeru pseudonimizacije maskiranjem, svaki unos "Petar" ima vrednost "šlb" a svaki Milan "šbb"; svaki "Petrović" je "123" dok unos "Đorđević" zamenjuje vrednost "456". S druge strane, anonimizovani podaci su zauvek nečitljivi, a iz njih se može videti samo da je lista imala četiri stavke sa po dva unosa.

PODRAZUMEVANA PRIVATNOST ("po difoltu") znači da načela zaštite podataka o ličnosti čine polaznu osnovu u radu sa korisnicima: na primer, vidljiva i jasna informacija o prikupljanju podataka, obradi i čuvanju, čini sastavni deo izrade vebsajta, u koji je ugrađeno pitanje o pristanku; korisnici su obavešteni o svojim pravima i načinima kako da ih ostvare; obrada podataka je organizovana tako da je identifikacija korisnika svedena na minimum u različitim fazama obrade, itd.

PREUZMITE NAŠ VODIČ O OSNOVAMA DIGITALNE BEZBEDNOSTI:

resursi.sharefoundation.info/sr/publikacije

7. PRAVO NA PRIGOVOR AUTOMATIZOVANIM ODLUKAMA

Šest osnovnih principa zaštite ličnih podataka formulisanih u Opštoj uredbi, dopunjeno je principom odgovornosti gde se razrađuju obaveze organizacija koje prikupljaju i obrađuju podatke građana.

Za građane, naročito u digitalnom okruženju, posebno je značajno što nova regulativa prepoznaje odgovornost organizacija i u situacijama kada ličnim podacima "rukuju" mašine. Zato ovo mesto ustupamo pravu na prigovor automatizovanim odlukama koje nam omogućava da zadržimo kontrolu nad svojim podacima i u slučaju kada u njihovoj obradi učestvuju samo mašine i softveri. Imamo pravo da zatražimo preispitivanje odluke koja se tiče nas, a koja je u celini ili delimično doneta na osnovu automatske obrade naših podataka.

Ovo pravo je važna inovacija u zaštiti podataka o ličnosti, a odnosi se na digitalno okruženje u kom se mnoge operacije izvode automatski, po unapred zadatim parametrima. Kada se na stotine parčića informacija koje svakodnevno "proizvodimo" na Mreži, samim tim što smo se ulogovali na fejs, pogledali neki video ili lajkovali nečiju sliku, pomnoži sa milijardama korisnika koji to isto rade – rezultat je nepregledna gomila podataka koju je samo mašina u stanju da sortira. Međutim, automatski prikupljeni i obrađeni podaci koji se tiču neke konkretne osobe, njenih navika, sklonosti i ponašanja na internetu ("profilisanje"), i dalje su podaci o ličnosti, ponekad čak i posebno osetljivi podaci koji uživaju dodatnu zaštitu. Savremena ekonomija podataka i profit mnogih globalnih internet kompanija, upravo su zasnovani na mogućnostima da se unovče automatski obrađeni podaci. Prava koja se tradicionalno vezuju za podatke o ličnosti sada moraju biti na snazi i kada je reč o automatizovanoj obradi – informisani pristanak, uvid, izmena ili brisanje, kao i svi temeljni principi na kojima počiva sama Uredba.

SCENE IZ BUDUĆNOSTI

Došli ste u banku da podignete kredit, predali dokumentaciju i čekate odgovor. Uskoro vam stiže obaveštenje da vaš zahtev nije prihvaćen. Kao obrazloženje, banka navodi da je analizom vaših podataka sa društvenih mreža utvrđeno da "niste pogodni" za odobrenje kredita, jer se vaše aktivnosti previše odnose na kockanje i klađenje. Ili, zamislite da vam je odjednom poskupela rata za životno osiguranje jer je osiguravajuća kuća, analizom podataka na osnovu fotografija i objava na društvenim mrežama, procenila da se nezdravo hranite i neumereno konzumirate alkohol.

ZAŠTITA PODATAKA O LIČNOSTI U SRBIJI

ZAŠTITA PODATAKA O LIČNOSTI U SRBIJI

Važeći zakon koji u Srbiji reguliše ovu oblast donet je pre deset godina. Pored svih primedbi na razne propuste, nelogičnosti ili nejasnu terminologiju, o čemu se može diskutovati, jedno je sasvim izvesno: taj zakon je vreme naprosto pregazilo.

Pokušaji da se donese novi zakon, koji bi bio u skladu sa evropskom Opštom uredbom o zaštiti podataka, traju već godinama bez pouzdane prognoze kada bi se to konačno moglo desiti. Poslednje u nizu obećanja predviđa 2018. kao krajnji rok za novi propis. Zakonodavac u različitim administracijama kroz koje se ovaj proces rasteže, ne obaveštava javnost s kakvim je preprekama suočen i zbog čega nije u mogućnosti da posao privede kraju.

U međuvremenu, podaci o ličnosti građana Srbije su izloženi brojnim rizicima, dok povrede prava često prolaze nekažnjeno. S druge strane, jedna od življih privrednih grana u zemlji, IT industrija koja je pretežno okrenuta evropskom tržištu, samostalno se prilagođava strogim normama koje GDPR uvodi u digitalno poslovanje.

Postojeći zakon prepoznaje neka od opštih načela zaštite podataka o ličnosti, kao što su zabrana obrade bez pristanka ili zakonskog osnova, ograničenost svrhe, te neke elemente minimizacije i slično, ali potpuno previđa neke od ključnih segmenata zaštite podataka o ličnosti u savremenom tehnološkom okruženju, kao što su video-nadzor ili biometrija. Usled manjkavog pravnog okvira, praktično sprovođenje zakonitosti obrade i obezbeđivanje efektivne zaštite podataka o ličnosti, i u javnom i u privatnom sektoru, suočeno je sa raznim problemima i paradoksima. Gotovo je suvišno govoriti koliko se svet promenio od kada je zakon napisan i u kojoj meri su, kao posledica korišćenja informaciono-komunikacionih tehnologija i razvoja ekonomije podataka, pitanja zaštite podataka o ličnosti postala kompleksnija, što domaći pravni okvir uopšte ne prepoznaje.

POŠALJI PISMO FEJSBUKU:

Domaći zakon određuje da se pristanak može dati samo u pisanoj formi ili elektronski uz kvalifikovani elektronski potpis, čime je čitavo poslovanje na internetu, zasnovano na obradi podataka, ostavljeno u sivoj zoni. Naime, po važećem zakonu u Srbiji, servisi kao što su Fejsbuk ili Gugl bi zapravo trebalo da vam traže da im pošaljete "preporučeno i svojeručno potpisano pismo", kako bi pristanak bio validan.

Kao država koja je već uveliko u procesu prilagođavanja domaćih propisa evropskom zakonodavnom okviru, Srbija je neminovno upućena na GDPR. Konačno, u globalnim razmerama, evropska Uredba zasad predstavlja najviši standard zaštite prava građana. Stoga je razumno očekivati da će se domaći propisi u oblasti zaštite podataka o ličnosti kretati u tom pravcu, pa makar i sporo.

POSETITE NAŠ SAJT POSVEĆEN ZAŠTITI PODATAKA O LIČNOSTI U JAVNOM SEKTORU U SRBIJI:

mojipodaci.rs

LOŠA ISKUSTVA

CURENJE PODATAKA SKORO SVIH PUNOLETNIH GRAĐANA SRBIJE: SLUČAJ AGENCIJE ZA PRIVATIZACIJU

Krajem 2013. godine, društvenim mrežama je kružio link ka bazi Agencije za privatizaciju "teškoj" 19 gigabajta, koja je sadržala podatke više od pet miliona građana Srbije i oko 4000 finansijskih dokumenata. Konkretni podaci o ličnosti bili su ime, prezime, srednje ime, matični broj i status građana u evidenciji nosilaca prava na besplatne akcije. Dakle, ako ste se 2008. godine prijavili za besplatne akcije, vaši podaci su kompromitovani. Agencija za privatizaciju je u međuvremenu ugašena, a odgovornost za ovaj bezbednosni propust je izostala, jer je slučaj pred nadležnim organima zastareo, uprkos insistiranju i urgencijama Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.[7]

BAZA O POLITIČKIM STAVOVIMA 400.000 GRAĐANA DOSTUPNA NA JAVNOM SERVERU

Tokom kampanje za predsedničke izbore 2017. godine, javnost u Srbiji je posredstvom medija saznala za bazu podataka o ličnosti 400.000 građana, koja se nalazila na javnom serveru, što znači da je mogao da joj pristupi svako ko je znao za njeno postojanje. Baza je sadržala 222 tabele u kojima su se nalazili podaci poput broja telefona, adrese, broja lične karte, već kompromitovanog JMBG-a, ali i naročito osetljive informacije iz domena privatnog života, kao što su političko uverenje, ekonomska situacija, zdravstveno stanje. Postoje indicije da je baza korišćena za ekonomsko i političko profilisanje građana, a samo uspostavljanje ovakve baze predstavlja krivično delo jer za nju ne postoji nikakav pravni osnov. Važno je napomenuti da su ovako strukturirani podaci podobni za brojne zloupotrebe, socijalni inžinjering, finansijske prevare, što sve povlači materijalnu odgovornosti za nastalu štetu. Već i samo objavljivanje ovakvih podataka predstavlja neprimereno zadiranje u privatnost i može biti osnov za naknadu nematerijalne štete.[8]

APLIKACIJA "IZABRANI DOKTOR": ZDRAVSTVENI PODACI GRAĐANA POD RIZIKOM

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je krajem maja 2018. upozorio građane da budu obazrivi prilikom korišćenja aplikacije "Izabrani doktor", koja omogućava zakazivanje lekarskih pregleda.[9] Zbog nejasnoća i ozbiljnih propusta u vezi sa prikupljanjem i obradom podataka o ličnosti građana (ime, adresa, lični broj zdravstvenog osiguranika, IP adresa, domen servera, vrsta uređaja sa koga se pristupa aplikaciji, kontakti, e-mail nalog, SMS poruke, kalendar, lokacija...) Poverenik je kompaniji koja je izradila aplikaciju zabranio dalju obradu podataka. Politika privatnosti, koja je u međuvremenu izbrisana sa aplikacije, omogućavala je čak i direktan marketing i profilisanje građana. Takođe, prva verzija aplikacije je zahtevala samo lični broj osiguranika (LBO) za pristup sistemu zakazivanja lekarskih pregleda, što praktično znači da je svako ko je znao taj broj mogao da pristupa podacima o pregledima građana.

07 "Neovlašćeno objavljeni podaci o ličnosti više od 5 miliona građana Srbije", SHARE Fondacija, decembar 2014. http://www.shareconference.net/sh/defense/neovlasceno-objavljeni-podaci-o-licnosti-vise-od-5-miliona-gradana-srbije

08 "Monitoring predsedničke onlajn kampanje 2017: Politika i lični podaci", SHARE Labs, mart 2017. https://labs.rs/sr/izbori2017/#Politika

09 "Poverenik sugerisao građanima: oprezno sa aplikacijom 'Izabrani doktor'", maj 2018. https://goo.gl/1xVv6p

NOVI SVET DIGITALNE EKONOMI-JE

NOVI SVET DIGITALNE EKONOMIJE

Sajber-svet ne poznaje mnoga ograničenja fizičkog prostora. Na internetu se razdaljine između tačke A i tačke B mere brzinom konekcije i kapacitetom uređaja koji koristimo, a danas su to već neslućene mogućnosti.

Dok se čitav taj buran život na internetu odvija samo na ekranu, imamo utisak da je Mreža nematerijalni univerzum iz neke paralelne dimenzije. Međutim, internet zauzima ogroman deo našeg fizičkog sveta. Serveri, kablovi, ruteri, bazne stanice... i nepregledno more kancelarija i osoblja koji taj sistem opslužuju, kao operatori, provajderi, administratori. O programerima i dizajnerima da i ne govorimo.

Razvoj tehnologije omogućio je rast čitavih ekonomija na proizvodima i uslugama koje postoje samo na internetu. O nekim kompanijama govori se kao o globalnim gigantima, a to su najčešće platforme na kojima korisnici proizvode sadržaj i razmenjuju vrednosti. Bez korisnika, te platforme bi bile prazne.

Kao što je promenilo svetsku ekonomiju, način poslovanja i robu kojom se trguje, novo okruženje menja i naše navike i običaje. Bez uobičajenih ograničenja fizičkog prostora, u sajber sferi i nacionalne granice postaju relativne. Kompanija sa sedištem u Irskoj, osobljem u Indiji i korisnicima širom sveta, postala je nova ekonomska paradigma.

PUT OKO SVETA ZA JEDNU SEKUNDU: PRIČA O INFRASTRUKTURI INTERNETA

Kao i svakog jutra, jedan profesor iz Novog Sada i danas gleda u ekran svog smartfona dok srče svoju prvu kafu. Prvo treba da proveri mejl i mesindžer na fejsu: ispitni je rok i studenti mu opsedaju inbokse pitanjima i izgovorima.

Mada koristi popularan model, njegov telefon ima jedinstveni identifikacioni broj, jedan jedini na svetu, međunarodni identifikator uređaja (International Mobile Equipment Identity, IMEI). Čak i da nema SIM karticu u telefonu, bio bi povezan na mrežu mobilne telefonije i u hitnim slučajevima mogao bi da pozove u pomoć. Profesor, naravno, ima pretplatnički broj (Subscriber Identification Module, SIM) preko kog mu je dodeljen međunarodni pretplatnički identitet (International Mobile Subscriber Identity, IMSI), koji je takođe jedinstven na svetu.

Umesto standardne GSM mreže, profesor koristi LTE mrežu četvrte generacije (4G) koja se, kao i prethodne generacije, oslanja na operatore i njihove bazne stanice, mrežu antena za razmenu signala i paketa informacija. Antene u fizičkom prostoru, preko kojih se povezuje na internet, neprestano prenose signale od uređaja do centrale i nazad, da bi protok bio stabilan. Sastavni deo tih signala je i numerička oznaka tačne fizičke lokacije profesorovog uređaja.

U trenutku kada je profesor kliknuo da otvori inboks na fejsu, paketić informacija o tom kliku krenuo je na svoj daleki put: u paketu se između ostalog nalaze svi brojevi koji identifikuju uređaj, pretplatnika, lokaciju, provajdera i njegovu mrežu. Tu su i podaci o kliku, izraženi u formi čitljivoj mašinama: profesorov jedinstveni nalog na Fejsbuku i njegov upit za otvaranje inboksa.

Paketić je sa telefona skočio do kućnog rutera, a zatim podzemnim kablom do rutera u novosadskoj centrali provajdera. Da stigne od Novog Sada do beogradskog SBB TeleParka, treba mu oko 10 milisekundi. Odatle će se otisnuti u svet, prvo ka Frankfurtu, gde se nalazi najveća svetska "tačka razmene" na internetu (IXP – Internet Exchange Point), sa protokom od oko 2523 gigabita u sekundi.

Najčešće, nevidljivi paket informacija poslat iz Novog Sada ne svraća u neku od brojnih drugih tačaka razmene na tlu kontinen-

talne Evrope, već ide pravo u Dablin u Irskoj. Na britanskim ostrvima će možda biti primoran da skrene s puta, u neki mračni ćošak Mreže, gde se nadzire globalni internet saobraćaj. Pretres ne traje dugo i profesorov paket uskoro kreće optičkim kablom razvučenim po dnu Atlantskog okeana, prevaljujući i do 50 miliona metara u sekundi.

U Novi svet stići će preko jedne od glavnih telekomunikacionih "luka" na istočnoj obali Amerike. Odatle kreće ka Virdžiniji, u "zonu razmene", kroz koju prolazi najveća količina svetskog internet saobraćaja. Do krajnje destinacije, Forest Sitija u Severnoj Karolini, čeka ga poslednja etapa puta od 700 kilometara. Tu je Fejsbuk 2010. izgradio svoj data centar.

Paketić se zapljunuo u neki od nebrojenih servera, javio da profesor iz Novog Sada hoće da vidi šta ima u inboksu i otišao na počinak. Svojim prisustvom pokrenuo je stvaranje novog paketa koji je već krenuo nazad u Novi Sad, da javi profesoru šta mu pišu studenti.

Deset hiljada kilometara prešao je za samo jednu sekundu. [10]

ŠTA JE BILO POSLE: PRIČA O ALGORITMIMA

Na čitavoj trasi puta od nacionalnog provajdera, preko raznih čvorišta i tačaka razmene, do servera kompanije na drugoj strani sveta, paket informacija ostavio je trag za sobom, repliku podataka koji se razmenjuju. To su metapodaci o našoj komunikaciji, koji se u mnogim slučajevima mogu tretirati i kao podaci o ličnosti.

Paketi koje naši uređaji razmenjuju sa serverima kompanija čije usluge koristimo, pored metapodataka, nose i informacija o nama i našem ponašanju. Šta smo lajkovali, kupili, slušali; s kim smo prijatelji i koga smo blokirali; gde živimo, a gde idemo na letovanje. Mnogi od nas su već stvorili višegodišnju arhivu autentičnih podataka o privatnom životu, iz kojih je moguće izvesti relativno pouzdane prozgnoze o našim budućim postupcima ili o situacijama koje bi kod nas mogle izazvati određenu aktivnost.

Obrada podataka o ličnosti na ovakav način se zove profilisanje, a obavljaju ga kompjuterski programi. Profili su na prodaju, najčešće marketinškim agencijama specijalizovanim za "mikrotargeting", individualno ciljanje potencijalnih mušterija, koje je postalo sastavni deo mnogih onlajn usluga. Nekada su se oglasi obraćali čitavim grupama ljudi, razvrstanim po uzrastu ili sličnim opštim karakteristikama, dok su se informacije o ukusima i sklonostima uglavnom prikupljale peške, mukotrpno, bez garancije da anketirani građani govore istinu.

S razvojem internet usluga, obilje autentičnih podataka na raspolaganju je za vrlo precizno ciljanje korisnika. Oglas koji se prikazuje starijoj, fakultetski obrazovanoj korisnici sa periferije Kraljeva, na primer, više ne mora da bude isti kao oglas koju ista kompanija, za isti proizvod, plasira studentu iz Subotice. Industrija je sad u prilici da oblikuje oglašavanje u odnosu na prognozu šta bi kog korisnika moglo da navede na kupovinu. Ta prognoza se izrađuje na osnovu podataka o ličnosti prikupljenih na platformama provajdera internet usluga.

U fokus svetske javnosti mikrotargeting je stigao kada su objavljene sume koje su britanski konzervativci dali za oglašavanje na Fejsbuku tokom poslednjih izbora. Obrnutim inženjeringom, istraživači su došli do zaključka da se stranka potencijalnim glasačima predstavljala u zavisnosti od njihovih prihoda, porekla, pa i osećanja, pri čemu nikome nije prikazivala svoje političko stanovište u celini.

Gotovo sve velike afere sa interneta koje su poslednjih godina potresale svet, imaju jednu zajedničku crtu: zloupotrebu podataka o ličnosti građana. Od problema bezbednog čuvanja prilikom tehničkih napada na bolnice, gde su "zaključavani" pristupi zdravstvenim kartonima pacijenata, preko curenja podataka o kreditnoj sposobnosti polovine američkih stanovnika – sve do profilisanja korisnika Fejsbuka i selekcije vesti kojima će korisnici biti izloženi kako bi se manipulisalo njihovim političkim izborom.

10 Više o uzbudljivom putu internet paketa i podacima o komunikaciji: labs.rs

Poslednji u nizu skandala prinudio je vlasnika najveće društvene mreže da polaže račune članovima američkog Kongresa, a zatim i poslanicima parlamenta EU, zbog neovlašćenog prikupljanja i omogućavanja zloupotrebe podataka o ličnosti preko 85 miliona korisnika Fejsbuka. U centru afere bila je kompanija "Kembridž analitika" koja je došla u posed ogromnih setova podataka, prikupljenih na osnovu psihološkog upitnika koji se delio preko Fejsbuka, kakve često rešavamo na mrežama, a zatim ih nudila na prodaju oglašivačima, političkim partijama i pojedincima, uz obećanje "uticaja na ponašanje publike".

Da je GDPR u to vreme bio na snazi, Fejsbuk bi se u Evropskoj uniji suočio sa kršenjem najmanje tri osnovna principa: transparentnosti, nužne za informisan pristanak, ograničenosti svrhe i bezbednosti obrade podataka. Naročit problem predstavlja profilisanje korisnika, čiji se podaci koriste za manipulaciju njihovog ponašanja.

MOJA PRAVA, PREGLED

MOJA PRAVA, PREGLED

PRAVO NA INFORMISANOST
Right to be informed

1. Kompanije i organizacije su sada u obavezi da, jasnim i razumljivim jezikom, objasne koje podatke o ličnosti obrađuju i kako ih koriste.
2. Ako kompanija ili organizacija gradi vaš profil (npr. na osnovu podataka iz različitih izvora koje su ukrstili), imate pravo da znate šta se nalazi u tom profilu i koje podatke prikuplja iz kog izvora.
3. GDPR postavlja određene standarde, te reguliše da obaveštenja o obradi moraju biti:
   - koncizna, transparentna, razumljiva i lako dostupna;
   - napisana jasnim i jednostavnim jezikom (naročito kada su upućena detetu);
   - data besplatno.

PRAVO PRISTUPA - PRAVO NA UVID
Right of Access

1. Imate pravo na potvrdu o tome da li se obrađuju vaši podaci i, ako da, pravo pristupa tim podacima i dobijanja određenih informacija u vezi sa njihovom obradom (koje se poklapaju u velikoj meri sa informacijama koje rukovalac obavezno mora da obelodani u okviru poštovanja prava na informisanost)
2. Organizacije su u obavezi da, na vaš zahtev, izdaju kopiju podataka. Ovo pravo može biti ograničeno samo ukoliko izdavanje kopije povređuje prava i slobode drugih (npr. poslovnu tajnu ili prava intelektualne svojine).

PRAVO NA ISPRAVKU NETAČNIH PODATAKA I DOPUNU NEPOTPUNIH
Right to Rectification

Svako ima bezuslovno pravo na ispravku netačnih i dopunu nepotpunih podataka. Ako u bilo kom trenutku primetite da neki podatak o vama nije potpun ili tačan, rukovalac podataka je dužan da izvrši

ispravku. Ovo pravo je naročito važno jer kad se podaci o ličnosti građana jednom prikupe često se ne vodi računa o njihovoj ažurnosti, što može predstavljati problem, npr. prilikom razmene podataka između državnih organa.

PRAVO NA BRISANJE - "PRAVO NA ZABORAV"

The Right to Erasure - 'Right to be Forgotten'

1. Ostvarenje ovog prava možete zahtevati ukoliko:
   - podaci više nisu neophodni za svrhe u koje su prikupljeni,
   - povučen je pristanak, koji je bio osnov za obradu,
   - uložen je prigovor na obradu ;
   - podaci su nezakonito obrađeni;
   - brisanje je u skladu sa zakonskom obavezom rukovaoca,
   - podaci su prikupljeni od deteta u vezi s ponudom usluga informacionog društva,
2. Ako je organizacija takođe javno objavila predmetne podatke onda je dužna da, uzimajući u obzir dostupnu tehnologiju i troškove sprovođenja, obavesti ostale organizacije koji ih obrađuju, kako bi bili obrisani svi linkovi do podataka ili kopije.
3. Postoje određeni izuzeci od ovog prava kada postoji prevladujući javni interes te organizacija ne mora da postupi po zahtevu (uključujući slobodu govora, arhiviranje, naučne i statističke svrhe, ostvarivanje ili odbrana od pravnih zahteva)

PRAVO NA OBUSTAVLJANJE OBRADE

Restriction of Processing

1. Situacije u kojima možete da zahtevate ostvarivanje ovog prava su sledeće:
   - osporavate tačnost podataka, u roku koji organizaciji omogućava da proveri tačnost podataka o ličnosti;
   - obrada je nezakonita, a vi se protivite brisanju podataka i umesto toga tražite ograničavanje upotrebe;
   - organizaciji više nisu potrebni podaci, ali jesu vama za ostvarivanja pravnih zahteva;
   - uložilli ste prigovor a još nije potvrđeno da li legitimni razlozi organizacije preovladuju nad vašim pravima.
2. Ako je organizacija prihvatila zahtev i ograničila obradu, tada

se podaci smeju obrađivati (izuzev čuvanja) samo u jasno definisanim situacijama, npr. uz vaš pristanak, za ostvarivanje pravnih zahteva, za zaštitu prava drugog fizičkog ili pravnog lica.

PRAVO NA PRENOSIVOST PODATAKA

Right to Data Portability

1. Ovo je novo pravo predviđeno GDPR-om kako bi se ojačala kontrola nad podacima.
2. Ono je ne neki način proširenje prava pristupa, jer zahteva od organizacija da vam na vaš zahtev obezbede i dostave podatke o ličnosti u strukturiranom, uobičajenom i mašinski čitljivom formatu, a vi imate pravo da ih prenesete drugom licu, bez ometanja.
3. Od organizacije se takođe može zahtevati da prenese podatke direktno drugoj organizaciji, kada je takav postupak tehnički izvodljiv.

PRAVO NA PRIGOVOR

Right to Object

1. Ako je pravni osnov za obradu javni interes ili bilo koji od legitimnih interesa, jasno je da taj pravni osnov nije apsolutan, i da imate pravo da se suprotstavite takvoj obradi.
2. U tom slučaju organizacija mora obustaviti takvu obradu podataka o ličnosti osim ako:
   - može pokazati da postoje legitimni razlozi za obradu koji preovlađuju nad interesima, pravima i slobodama tog lica; ili
   - je obrada neophodna radi odbrane pravnih zahteva.
3. Takođe u slučaju prigovora direktnom marketingu (što uključuje profilisanje) organizacija mora obustaviti obradu u tu svrhu čim primi prigovor.

PRILIKOM DONOŠENJA AUTOMATIZOVANIH ODLUKA, IMATE PRAVO NA OBJAŠNJENJE I LJUDSKU INTERVENCIJU

1. Ako je doneta odluka o vama korišćenjem automatizovanih mehanizama, imate pravo da znate kako je ta odluka doneta (npr. imate pravo na objašnjenje logike iza mehanizma donošenja odluke)
2. Kod automatizovanog donošenja odluka, imate pravo na ljudsku intervenciju, kao i pravo da osporite automatizovanu odluku.

IMATE PRAVO DA KORISTITE USLUGU BEZ DAVANJA DODATNIH PODATAKA

Ako kompanija ili organizacija želi da obrađuje podatke o ličnosti koji nisu neophodni za pružanje određene usluge (npr. aplikacija za transport koja traži pristup vašoj listi kontakata) moraće da dobije vaš izričit pristanak kako bi mogla da obrađuje te podatke (čak iako kompanija smatra da je obrada određenih podataka u njihovom interesu, to ne znači da su ti podaci uvek potrebni). Ako ste već pristali na obradu dodatnih podataka, uvek možete da povučete pristanak.

DA LI KAO POJEDINAC TREBA DA URADIM NEŠTO?

Ne. Na kompanijama i organizacijama je da se pobrinu da su vaši podaci o ličnosti zaštićeni. Ipak, postoje neke odluke koje treba da donesete:

- Za korišćenje novih servisa: ako kompanija traži da joj date podatke, da li se zaista slažete sa tim? (Ako servis obrađuje samo neophodne podatke, obavezan je da vas obavesti ali ne mora da traži poseban pristanak za to. Međutim, moraju da vam traže izričit pristanak kada žele da prikupljaju podatke koji nisu neophodni)
- Za servise koje trenutno koristite: da li vam i dalje odgovara način na koji kompanija/organizacija prikuplja, analizira i deli vaše podatke o ličnosti? Ako se ne slažete, jednostavno možete da kažete "ne".
- Na kraju, ako smatrate da se vaša prava ne poštuju, možete to da prijavite nadležnom organu za zaštitu podataka o ličnosti ili čak da pokrenete sudski postupak protiv kompanije.

ŠTA MOGU DA UČINIM AKO KOMPANIJA KORISTI MOJE PODATKE PROTIVNO MOJOJ VOLJI?

- Može biti korisno da prvo kontaktirate kompaniju. Bez obzira da li to uradite, možete da podnesete žalbu organu nadležnom za zaštitu podataka o ličnosti - čak iako kompanija nema sedište u vašoj zemlji. Ako niste zadovoljni odlukom nadležnom organa, možete pokrenuti sudski postupak protiv kompanije.
- Takođe možete da preskočite žalbu nadležnom organu i idete pravo na sud ukoliko osećate da su vam prava povređena.
- Ako ste zbog povrede prava pretrpeli materijalnu ili nematerijalnu štetu, možete da tražite finansijsku nadoknadu.
- Treće strane, kao što su udruženja za zaštitu potrošača, organizacije za zaštitu digitalnih prava ili druge interesne grupe, takođe mogu pokrenuti sudske procese u ime vas i drugih ljudi.

RESURSI:

Baza znanja - resursi.sharefoundation.info

Istraživačka laboratorija - Labs.rs

Podaci o ličnosti u javnom sektoru - mojipodaci.rs

2018