UVOD U DIGITALNA PRAVA

SHARE FONDACIJA

DECEMBAR, 2021.

SADRŽAJ:

UVOD

Ljudska prava jednako važe na internetu, kao i u fizičkom prostoru.

Digitalne tehnologije otvorile su mnoge nove i zanimljive načine za izražavanje ideja, razmenu informacija, udruživanje, proteste i druge aktivnosti slobodnih građana, koje se nalaze pod univerzalnom zaštitom kao temeljna prava svih ljudi, bez obzira na poreklo, status i druge međusobne razlike.

Istovremeno, digitalizacija svakodnevnih poslova i komunikacije omogućila je i razvoj sredstava za zloupotrebe i kršenje prava. Svesno ili iz neznanja, vođeni komercijalnim interesima ili namerom da uspostave kontrolu, različiti akteri – države, korporacije, političke i druge organizacije – često su na internetu vinovnici cenzure, narušavanja privatnosti građana i diskriminacije po različitim osnovama.

Mada većina ljudi prisutnih na internetu zna kako da koristi pametne uređaje, preuzima i objavljuje sadržaje na onlajn platformama, nije uvek do kraja jasno šta od tih aktivnosti spada u domen zaštite, niti u kojim slučajevima se može govoriti o kršenju prava. Da li su lajk na Tviteru, šerovanje na Fejsbuku ili metapodaci o pretrazi na Guglu – lični podaci? Kada ograničavanje pristupa nekom sajtu prerasta u cenzuru? Koja su temeljna ljudska prava ugrožena prilikom masovne obrade biometrijskih podataka u pametnim sistemima? Može li biti diskriminacije u procesu automatizovanog algoritamskog odlučivanja?

Da bi građani i građanske organizacije mogli da odgovore na ova i mnoga druga pitanja koja nas tek čekaju sa širom primenom još složenijih tehnologija, potrebna su im znanja o digitalnim pravima – ljudskim pravima u digitalnom okruženju. U ovom priručniku predstavljeni su neki od osnovnih pojmova iz ove oblasti, ilustrovani praktičnim primerima iz regiona Zapadnog Balkana.

ZAŠTITA PODATAKA O LIČNOSTI

Pojam zaštite podataka proizilazi iz osnovnog ljudskog prava - prava na privatnost. Pravo na privatan život podrazumeva kontrolu nad informacijama o nama samima, odnosno kontrolu nad time da li će i ko znati kuda se krećemo, šta kupujemo, gde živimo, s kim se dopisujemo. Privatnost je od nesumnjive važnosti za autonoman život svake individue, a s pojavom interneta njena ugroženost postaje očiglednija.

ZAŠTITA PODATAKA O LIČNOSTI U DIGITALNOM PROSTORU

S razvojem tehnologije došlo je do većeg protoka i umožavanja podataka, a najveći deo ovih podataka su podaci o ličnosti, odnosno informacije koje se odnose na konkretnu osobu koju je moguće identifikovati. Zaštita podataka se upravo tiče regulacije procesuiranja podataka (tj. njihovog prikupljanja, korišćenja i skladištenja) u službi zaštite privatnosti pojedinaca u digitalnom prostoru. Danas se podacima o ličnosti pristupa kao vrednom resursu na osnovu koga kompanije ostvaruju profite, a države vrše kontrolu nad građanima. Samim tim očuvanje privatnosti u digitalnom dobu nailazi na dodatne izazove. Ukoliko podaci nisu adekvatno zaštićeni, odnosno, ako dođe do njihovog curenja ili zloupotrebe, naša privatnost je ugrožena.

PRIMERI POVREDA

- Na društvenim mrežama počeo je da kruži fajl sa ličnim podacima preko 5 miliona građana jedne države. Procesom nadzora utvrđeno je da je fajl sa podacima prvobitno bio javno dostupan na sajtu državne agencije sa kog je preuziman, a ta agencija se branila tvrdnjom da je do toga došlo putem neovlašćenog pristupa njihovom serveru.
- Podaci poput imena, brojeva telefona i lokacija preko pola milijarde naloga sa jedne društvene mreže procureli su na hakerski forum. Međutim, saznalo se da ovo curenje nije bilo stvar greške, već su ovi podaci namerno izvučeni uz pomoć posebnog softvera, što je bilo omogućeno zbog sistemskog propusta društvene mreže.
- Do jedne međunarodne organizacije za ljudska prava došli su spiskovi sa preko 50,000 mobilnih telefona za koje se sumnja da su bili određeni kao mete potencijalne špijunaže, odnosno softvera koji kompromituje telefon, izvlači iz njega sve podatke i aktivira mikrofon za snimanje razgovora.
- Desetine hiljada muškaraca iz regiona je na aplikaciji Telegram razmenjivalo intimne sadržaje, odnosno slike, video zapise i fotografije žena, među kojima je bilo i maloletnih lica. Sadržaje su članovi grupa ili lično dobili u prošlosti od svojih partnerki ili su ih jednostavno "skidali" sa društvenih mreža i slali u grupe, neretko uz otkrivanje ličnih podataka osobe čiji sadržaj dele.

- Mediji u jednoj državi su objavili detalje velike baze koja sadrži lične podatke više od 910,000 glasača. Lista je uključivala i novinare, aktiviste i druge dobro poznate osobe. Navodno, ovi podaci su dati jednoj političkoj partiji kako bi ih koristila tokom izborne kampanje.

POSLEDICE PO POJEDINCA I DRUŠTVO

Bavljenje zaštitom podataka je od suštinske važnosti kako bi se povrede poput curenja podataka, nezakonitog nadzora komunikacija ili nedozvoljene obrade podataka, sprečile ili barem adekvatno sankcionisale. Ukoliko bi situacije kao što su krađe brojeva bankovnih kartica, ili nadzor naših razgovora na društvenim mrežama, bile neregulisane, jasno je da bismo živeli u svetu gde bi vladao strah i u kom bismo svi bili manje slobodni. Dodatno, oni najmarginalizovaniji među nama bi bili dodatno ugroženi, npr. ako bi kompanije imale pravo da neometano obrađuju senzitivne podatke poput rase ili roda, ti podaci bi mogli biti iskorišćeni u diskriminatorne svrhe.

MEHANIZMI ZAŠTITE

- Pravo na informisanost - kompanije i organizacije su u obavezi da objasne koje podatke obrađuju, odnosno mi imamo pravo da znamo koji podaci o nama se prikupljaju i kako se koriste.
- Pravo na uvid - organizacije su u obavezi da izdaju kopiju podataka koje imaju o nama.
- Pravo na ispravku i dopunu - imamo pravo da ispravimo netačne podatke ili dopunimo nepotpune.
- Pravo na brisanje tj. pravo na zaborav - ovo pravo je ostvarivo u različitim slučajevima poput nezakonite obrade podataka ili kada svrhe za njihovu obradu više nema.
- Ukoliko kompanija ili organizacija želi da obrađuje podatke koji nisu neophodni za pružanje određene usluge ili to nije propisano zakonom, mora za to dobiti naš pristanak za obradu, a taj pristanak uvek možemo povući.

Na ovom linku možete pristupiti našem kratkom videu o zaštiti podataka.

DIGITALNA BEZBEDNOST

Bezbednosti možemo pristupiti kao izrazito bitnom aspektu u životu pojedinaca, budući da predstavlja vid otpora prema nekom događaju ili ponašanju drugih koje može biti ugrožavajuće. Odnosno, ona predstavlja izvesnu zaštitu prema stvarima koje nam mogu naškoditi. Pored toga što se o njoj može govoriti u individualnom kontekstu, na primer da li pripadnici neke seksualne manjine mogu slobodno prošetati ulicom bez straha od fizičkog nasilja, o bezbednosti može biti reči i na nivoima neke organizacije ili države.

BEZBEDNOST U DIGITALNOM PROSTORU

Sajber napadi i sajber kriminal postaju sve prisutniji, sa izgledom da će njihov broj i sofisticiranost samo rasti u budućnosti. Ovo iziskuje bavljenje bezbednošću u digitalnom kontekstu, odnosno konstantno je potrebno raditi na izgradnji rezilijentnosti informacionih sistema i otporu prema potencijalnim napadima i šteti. Mnoge osnovne aktivnosti država i kompanija su se prelile u sajber prostor. Ukoliko uvidimo da su čitavi sektori poput transporta, energije, zdravlja itd. zavisni od digitalnih tehnologija, jasno je da ih to na jedan način čini fragilnijim - odnosno čitavo društvo i ekonomija su izloženi napadima koji sada mogu biti i digitalne prirode. I pojedinci mogu biti meta sajber napada, npr. ukoliko nam je onemogućen pristup nalozima na različitim platformama, to može biti znak da nam je ugrožena privatnost i pristup ličnim podacima, odnosno da je neko došao u posed naših lozinki. Internet nas kao pojedince takođe može dodatno izložiti potencijalnom uznemiravanju ili uhođenju, koje može da se odvija putem lažnih ili anonimnih profila.

PRIMERI POVREDA

- Nekoliko sati nakon objavljivanja o plagiranoj doktorskoj disertaciji funkcionera jedne države, vebsajt koji je to objavio je hakovan. Napadi na sajt su se nastavili tokom sledeće nedelje, a administratori sajta su rekli da već godinama trpe napade zbog svojih politički nepodobnih sadržaja.
- Jedna opština je izdala saopštenje da je njihova arhiva bila napadnuta virusom koji zaključava dokumente, odnosno onemogućava pristup njima. Virus je naveden kao razlog zašto građanima nisu mogli da izdaju nikakve dokumente, a problem je rešen u roku od nekoliko dana, međutim, nije jasno da li je baza tih podataka ukradena u međuvremenu.
- Vebsajt izborne komisije jedne države je bio meta hakerskog napada tri sata, dan nakon što su se održali izbori. Napad nije izazvao veću sistemsku štetu, ali je odložio objavu izbornih rezultata.
- Nekoliko hiljada inficiranih računara je napalo servere na kojima su se nalazili portali koji su objavili vest o privilegijama ćerke guvernerke Narodne banke jedne države. Stranice na kojima je vest bila objavljena pokazivale su 404 Not Found grešku, koja ukazuje da traženi sadržaj ne postoji na datoj adresi.

- Anonimna osoba je registrovala profil na jednoj društvenoj mreži pod imenom i prezimenom jednog profesora koji je poznat i cenjen u svojoj zajednici. Potom, putem ovog profila tražene su finansijske donacije. Nakon što je profesor ukazao da mu je neko ukrao identitet na ovoj društvenoj mreži, dati profil je suspendovan.
- Gradonačelnik jednog grada nije danima mogao da pristupi svom profilu na jednoj društvenoj mreži, te je obavestio korisničku podršku o mogućem hakerskom napadu.
- Prevaranti su koristili ime i sliku direktora jedne velike banke kako bi promovisali usluge vezane za kriptovalute, pripisujući mu rečenice koje nikad nije izgovorio.

POSLEDICE PO POJEDINCA I DRUŠTVO

Ukoliko se ne radi na pojačanju digitalne bezbednosti, kako na individualnom, tako i na organizacionom nivou, efekti malicioznih napada mogu izazivati sve veću štetu po pojedince i čitava društva. Kako se mnogi procesi koji se odvijaju u sajberprostoru tiču velikog broja ljudi, posledice od napada na njih su potencijalno dalekosežnije. S umnožavanjem sajber napada dolazi se i do njihove veće sofisticiranosti, te je nužno konstantno raditi na digitalnoj bezbednosti. Iako sajber napadima možemo biti ugroženi svi, kada govorimo o sajber, tj. digitalnoj bezbednosti, isto kao i kada je reč o bezbednosti u fizičkom prostoru, neki pripadnici društva su ugroženiji od drugih. Pripadnici posebnih kategorija - npr. novinari koji barataju osetljivim informacijama, predstavljaju čestu metu sajber napada. Napadima na njih i uklanjanjem sadržaja ili krađom različitih podataka, hakeri ne utiču samo na predstavnike ove grupe, već na čitavo društvo za čiju informisanost oni rade.

MEHANIZMI ZAŠTITE

- Da bi se zaštitili od malvera, vrste softvera koja može da ukrade ili zaključa podatke, pored instaliranja softvera za njegovo prepoznavanje ključno je i neotvaranje mejlova sa sumnjivih adresa, neinstaliranje neproverenih programa i neposećivanje nepouzdanih sajtova.
- Za svaki nalog je potrebno imati različitu lozinku, a ona treba da bude dugačka i da se sastoji od različitih karaktera i simbola.

- Dvostepena autentifikacija za naloge predstavlja dvostruku potvrdu identiteta, te je dodatna prepreka za hakere.
- Potrebno je koristiti pouzdane aplikacije i redovno ih apdejtovati.

Na ovom linku možete pristupiti našem kratkom videu o digitalnoj bezbednosti.

Za više alata koji mogu ojačati digitalnu bezbednost možete posetiti ovaj sajt.

SLOBODA IZRAŽAVANJA

Sloboda izražavanja podrazumeva slobodu da se iznose različita mišljenja i ideje bez straha i smetnji, ali uključuje i slobodan pristup informacijama bez mešanja države ili drugih entiteta. Međutim, ovo pravo se ne treba shvatiti kao apsolutno, budući da nosi sa sobom i dužnosti i odgovornosti, te je podložno restrikcijama poput zabrane govora mržnje.

SLOBODA IZRAŽAVANJA U DIGITALNOM PROSTORU

S pojavom interneta komunikacija između ljudi je uvećana, pogotovo uzevši u obzir da možemo komunicirati s više ljudi istovremeno, a da oni mogu biti i na različitim kontinentima. Dodatno, internet nam omogućava izvesnu anonimizaciju, mogu se praviti profili koji ne odaju naš identitet, te mnogi komuniciraju mnogo slobodnije u sajberprostoru, smatrajući da posledice ponašanja na internetu ne moraju biti iste kao u fizičkom svetu. Cenzura putem filtriranja i blokiranja sadržaja kojoj pribegavaju razne države i korporacije takođe predstavlja ozbiljan problem, budući da nam onemogućava slobodan pristup informacijama, što isto spada pod slobodu izražavanja. S druge strane, sadržaj može biti uređivan ne samo kroz cenzuru, već i njegovo plasiranje, odnosno algoritmi mogu odlučivati koja vrsta sadržaja će biti vidljiva kom korisniku. Kako se novi načini komunikacije stvaraju, a broj načina njihove restrikcije takođe uvećava, zaštita slobode izražavanja u digitalnom kontekstu može biti posebno izazovna.

PRIMERI POVREDA

- Novinarka jednog medija je uhapšena u sopstvenom domu povodom teksta u kom je pisala o lošim uslovima rada i manjku zaštitne opreme za medicinske radnike tokom COVID-19 pandemije. Zadržana je u pritvoru 48 sati, a bolnica je objavila da novinarka širi lažne informacije i uzrujava javnost.
- Administratori jedne fejsbuk grupe, u kojoj je postavljena slika stada ovaca sa nazivom "Odbornici opštine", kažnjeni su novčanom kaznom nakon što je sud odredio da je ovaj post uvredljiv i ponižavajuć.
- Narodni poslanik jedne države je seksističkim i vulgarnim porukama na Tviteru vređao određene političarke, pozivao na silovanje jedne funkcionerke i pretio streljanjem svojim političkim oponentima.
- Nakon što je jedna aktivistkinja za ljudska prava stala u zaštitu osobe koja je bila izložena šovinističkim napadima, i sama je postala žrtva pretnji i napada preko društvenih mreža. Usled osećaja ugroženosti, ona je podnela više krivičnih prijava, međutim, reakcija nadležnih je izostala, a pretnje su nastavljene.
- Jedna društvena mreža je objavila da je izbrisala na hiljade lažnih, takozvanih "bot" naloga koji su služili da promovišu vladajuće partije u nekoliko država.

- Nekoliko onlajn medija je pokradeno i kopirano tako što su napravljeni sajtovi skoro identičnog domena i dizajna, koji su potom korišćeni da promovišu rad vladajuće partije i zbune redovne čitaoce tih medija.

POSLEDICE PO POJEDINCA I DRUŠTVO

Manjak slobode izražavanja šteti čitavom društvu budući da mu onegomućava pristup raznovrsnim idejama ili informacijama koje mogu biti od javnog značaja, tj. koje mogu dovesti do progresa ili ukazivanja na izvesne društvene probleme. S druge strane, sloboda izražavanja obuhvata i regulaciju potencijalne manipulacije i širenja lažnih informacija. Ograničavanje slobode govora u vidu borbe protiv govora mržnje, pretnji, omalovažavanja itd. je isto ključno jer takav govor može izazvati ili uvećati broj akta nasilja i diskriminacije, narušiti ugled i dostojanstvo ili osećaj slobode i bezbednosti pojedinaca, utišati pripadnike manjinskih grupa, te umanjiti koheziju čitavog društva.

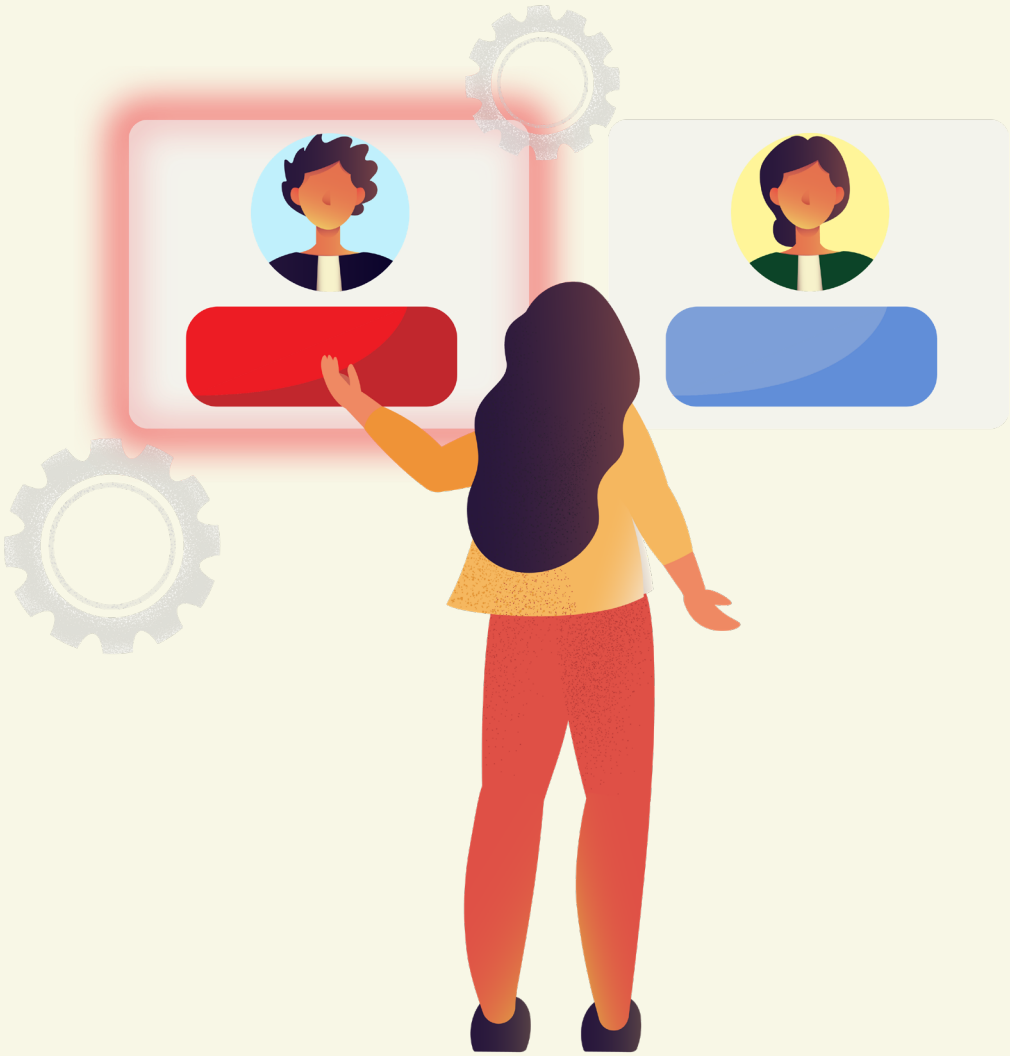
MEHANIZMI ZAŠTITE

- Internet nam omogućava da budemo ne samo korisnici, već i da produkujemo sadržaj, te to treba imati u vidu kada se u našem društvu događaju stvari koje mogu biti cenzurisane (npr. protesti).
- Ukoliko postoje nedostupni sadržaji u državi u kojoj živimo, njima možemo pristupiti kroz npr. Tor pretraživač, koji nam omogućava anonimizaciju i slobodan pristup internetu.
- Ukoliko smatramo da će određene stranice biti nedostupne ili obrisane, možemo ih sačuvati putem alata poput The Wayback Machine. Ovaj alat je omogućila Internet Archive, digitalna biblioteka čiji je cilj univerzalni pristup svom znanju.
- Ukoliko nas neko vređa, preti nam ili ugrožava naša lična prava na drugi način, potrebno je da obavestimo svoje okruženje i da blokiramo i prijavimo društvenoj mreži osobu koja nas ugrožava. Ukoliko se napadi nastave, treba da se obratimo nadležnim organima i insistiramo na pravnoj pomoći i zaštiti.
- Jedan od načina na koji se može reagovati na ućutkivanja jeste dodatno pričanje. Ukoliko smo ućutkivani zbog neke kritike ili neslaganja,

upoznavanje šire javnosti sa datim problemom može nam vratiti osećaj kontrole nad situacijom.

- Ukoliko smo žrtva govora mržnje, odnosno verbalnog napada na osnovu rasne, verske, nacionalne, seksualne, političke, sindikalne i neke druge pripadnosti ili ličnog svojstva, potrebno je da se obratimo nekoj od institucija, poput policije ili Poverenika za zaštitu ravnopravnosti.

Na ovom linku možete pristupiti našem kratkom videu o slobodi izražavanja.



DIGITALNA PRAVA U REGIONU

SHARE fondacija je uspostavila stalni monitoring prava i sloboda građana u digitalnom okruženju i objavljuje redovne godišnje izveštaje svojih nalaza. Ovaj proces monitoringa i dokumentovanja povreda digitalnih prava SHARE je započeo 2014. godine u Srbiji, a 2019. godine se u saradnji sa BIRN-om širi i na region, trenutno sprovodeći se i u Bosni i Hercegovini, Hrvatskoj, Mađarskoj, Rumuniji i Severnoj Makedoniji. Pored toga što nam monitoring povreda prava i sloboda na internetu omogućava da upozorimo i mobilišemo javnost, on nam omogućava i da aktivno učestvujemo u zagovoranju novih i kritičkoj analizi postojećih zakonskih predloga koji se tiču regulacije života pojedinaca, koji se sada odvijaju i u fizičkom i u digitalnom prostoru.

Bazi povreda digitalnih prava u ovih 6 država možete pristupiti na ovom linku.

Na ovom linku možete naći studiju o regulativi iz tri oblasti pokrivene ovim vodičem u šest država regiona: Albanija, Bosna i Hercegovina, Kosovo, Crna Gora, Severna Makedonija i Srbija.

USAID
OD AMERIČKOG NARODA

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND