

UDK: 342.7

Izvorni znanstveni članak

Izv. prof. dr. sc. Marija Boban,
Pravni fakultet Sveučilišta u Splitu¹
Ivana Cinotti Mujan, mag. forenzike²

INFORMACIJSKA SIGURNOST I ZAŠTITA PRAVA NA PRIVATNOST KAO TEMELJNO LJUDSKO PRAVO

Sažetak:

U današnjem digitalnom i dominantnom informacijsko-komunikacijskom dobu uz Internet koji omogućava prijenos informacija na globalnoj razini, informacijska sigurnost ima neizmjerno važnu ulogu. Osobni podaci pojedinaca obrađuju se svakodnevno u tijelima javne vlasti, organizacijama i ostalim pravnim osobama te se mogu zloupotrijebiti. Koristeći tehnološke naprave za komunikaciju i pristup internetu, svaki korisnik ostavlja virtualne tragove koji se mogu nezakonito obrađivati i preko kojih se korisnika može jednoznačno identificirati te kršiti njegovo pravo na privatnost kao i zakone koji štite osobne podatke i uvjetuju mjere informacijske sigurnosti. Društvene mreže su jedni od najvećih prijenosnika informacija današnjice. Prikupljajući osobne podatke korisnika i prateći njihove aktivnosti mogu profilirati korisnike te vršiti ciljano oglašavanje ili prosljeđivati njihove osobne podatke trećim stranama bez dopuštenja, dok pojedinci mogu sami ugroziti svoju sigurnost i privatnost zbog nedovoljne osviještenosti ili nemara. Autorice u ovom radu, uz prikaz trenutnih prijetnji informacijskoj sigurnosti i prava na privatnost, stavljaju naglasak na prikaz razine osviještenosti građana vezanih uz informacijsku sigurnost i prava na privatnost, kao i prikaz dosadašnjih kršenja tih prava i zlouporabe osobnih podataka s naglaskom na metode zaštite podataka u virtualnom okruženju.

Ključne riječi: društvene mreže, informacijska sigurnost, osobni podaci, privatnost, tehnologija, virtualni svijet, zaštita

¹ Izv. prof. dr. sc. Marija Boban, Predstojnica za ekonomske-financijske i informacijske znanosti i statistiku Pravnog fakulteta Sveučilišta u Splitu

² Ivana Cinotti Mujan, mag. forenzike, diplomirala na Sveučilišnom odjelu za forenične znanosti Sveučilišta u Splitu 2018. godine pod mentorstvom izv. prof. dr. sc. Marije Boban i obranila rad na temu "Informacijska sigurnost i zaštita prava na privatnost kao temeljno ljudsko pravo" temeljem kojeg je izrađen ovaj znanstveni rad u koautorstvu s mentoricom.

Uvod

Paralelnim razvojem tehnologije i sve većoj dostupnosti interneta kao jednog od najvećih prijenosnika informacija današnjice, koračamo vremenom u kojem biti „na mreži“ postaje čovjekova svakodnevnic. Uz korištenje uređaja poput mobitela, tableta ili računala dobivaju se nove mogućnosti za pojedinca i za društvo te one značajno utječu na ljudske živote. Prema podacima iz 2018.g., 4.1 milijarde ljudi je spojeno na internet.³ a taj broj ubrzano raste iz dana u dan. Korištenjem interneta svaki pojedinac ostavlja virtualne tragove kao što su IP adresa, informacije o pretraživaču s kojeg se pristupa na internet i operacijskom sustavu koji se koristi, povijest pretraživanja, točno vrijeme pristupa određenoj web stranici, povijest preuzimanja sadržaja s interneta itd. Takvi podaci se mogu spremati u pozadini pretraživača, web stranica koje se posjećuju, ali i telekomunikacijski operateri pohranjuju i koriste određene podatke kako bi mogli pružiti uslugu krajnjim korisnicima. Od samog rođenja svakog pojedinca osobni podaci o njemu su kreirani (npr. rodni list) i nalaze se u određenom informacijskom sustavu.⁴ Za veliki broj ljudskih interakcija s javnim ustanovama, kompanijama i drugim pravnim osobama potrebno je dati na uvid osobne podatke (osobna iskaznica, putovnica, indeks, zdravstvena kartica, bankovna kartica i dr.), a sve je veći trend njihovog objavljivanja od strane samih korisnika putem društvenih mreža. Osobni podaci mogu biti: ime i prezime, adresa stanovanja, radno mjesto, OIB, medicinski karton, fotografije djece, podaci s kreditne kartice, bankovni računi i transakcije, kupovne navike, političke preferencije, hobiji, rute kretanja, ali i mnoge druge. Informacijski sustavi s takvim podacima mogu biti meta hakera ili se mogu zloupotrijebiti i „iznutra“, preko zaposlenika kojima su takve informacije dostupne. Nadalje, prilikom ispunjavanja raznih anketa, testova, pristupnica itd. također je moguće ostavljanje osobnih podataka koji se potom mogu iskoristiti za svrhe za koje nisu bile predviđene, čak i ako samo prikupljanje nije obavljeno putem mreže.

Osobni podaci su postali interesantni mnogim pravnim i fizičkim osobama koji njihovom obradom mogu doći do određenih koristi, ali jednako tako mogu ugroziti prava i privatnost nezakonitim postupanjem s prikupljenim podacima. Zbog neznanja ili nemara, kao žrtve računalnog kriminaliteta ili drugih oblika kršenja zakona, pojedinac može postati „meta“ onih koji koriste takve podatke na nezakonit način, obrađujući ih u svoju korist, najčešće onu financijsku. Mediji već odavno nisu samo papirnato izdanje novina, televizija

³ Preuzeto sa Internet World Stats (2018). URL: <https://www.internetworldstats.com/stats.htm> [02.03.2021.].

⁴ Vidi šire u Čizmić, J.; Boban, M., Zlatović, D., Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Split: Sveučilište u Splitu Pravni fakultet, 2016.

ili radio, uz jedan pametni telefon, računalo, tablet ili laptop kreiranje sadržaja se omogućuje i pojedincu. Društvene mreže postaju prostor gdje korisnici objavljuju svoje osobne podatke. Te informacije se dijele s bližnjima, poznanicima, ali i potpunim strancima, ne razmišljajući o mogućim posljedicama. S porastom broja korisnika društvenih mreža, taj novi društveni fenomen dijeljenja informacija postaje sve popularniji, a usporedno s tim postaje sve veća prijetnja za zaštitu osobnih podataka od zlouporabe. Krađe identiteta, računalne prijevare, zlostavljanja putem interneta (engl. cyberbullying) samo su neke od mogućih prijetnji kojima se korisnici društvenih mreža izlažu.⁵ Navedeni slučajevi pokazuju različite perspektive prijetnji, ali je svima zajedničko to da koriste i obrađuju osobne podatke o pojedincima bez privole tih pojedinca i vrše zlouporabu samih podataka. Kako bi se umanjila mogućnost zlouporabe a povećala transparentnost samih procesa obrade podataka, pokazalo se potrebno postaviti određena pitanja svima koji dolaze u doticaj s osobnim podacima: Što se u pozadini dešava s podacima koji se nalaze na određenom informacijskom sustavu? Postoji li privola za obradu tih osobnih podataka u svrhu za koju su obrađivani? Što se dešava s osobnim podacima u javnim ustanovama, bankama i ostalim pravnim osobama koje u sklopu obavljanja svojih dužnosti rade s osobnim podacima? Gdje se ti podaci skladište i koliko dugo? Tko im sve ima pristup? Tko ih sve koristi i za koje svrhe? Ako se ti podaci obrišu od strane korisnika, da li oni i dalje ostaju u sustavu? Stoga, autorice u ovom radu analiziraju područje aktualne problematike vezane uz pravo na privatnost pojedinca u vremenu kada vlada virtualna borba za što većim brojem informacija samih pojedinaca. Pravo na privatnost određuje i pravno i etično onu granicu ispod koje nije dozvoljeno ići prilikom prikupljanja tuđih osobnih podataka. Kako zakoni nekad znaju kasniti s realnim potrebama društva, u tom „ratu za informacijama“ je vladao kaos u kojem određena zlodjela nisu bila pravno prepoznata kao takva, a i kad bi se prepoznala, kazne nisu uvijek bile razmjerne nastaloj šteti. Nužno je to pravo zaštititi jer se njegovim kršenjem zadire u čovjekova ljudska prava koja su temelj demokratskog društva kakvo njeguje i Republika Hrvatska, punopravna članica Europske Unije. Kako se problematika informacijske sigurnosti i zaštite prava na privatnost može gledati iz više aspekata, kroz ovaj rad će se biti naglasak na pojedincu kao krajnjem konzumentu virtualnih sadržaja i kreatoru istih. Kao i pravna zaštita koja bi trebala pratiti takve društvene fenomene, pružati pravni okvir koji diktira dopuštene i nedopuštene radnje, a u slučaju kršenja zakona i adekvatnu kaznu.

⁵ O razvoju tehnologija, rizicima te modelima zaštite osobnih podataka vidi više u Boban, M., *Cyber security foundations for compliance within gdpr for business information systems*, Economic and Social Development: Book of Proceedings, Development and Entrepreneurship Agency (VADEA), Varaždin, 2018. str. 541-553

2. INFORMACIJSKA SIGURNOST I SIGURNOSNE PRIJETNJE U DANAŠNJEM MODERNOM DIGITALNOM VREMENU

Današnjica je nezamisliva bez uočavanja vrijednosti same informacije. Čuli smo mnogo puta izjavu „prava informacija u pravo vrijeme na pravom mjestu“ koja dočarava važnost same informacije, a zadire u sve životne sfere, poslovne i privatne, na svim društvenim razinama. Promatrajući je kroz prizmu društvenih pojava, imati važnu informaciju u pravo vrijeme i na pravom mjestu može doprinijeti raznim oblicima privatnog i poslovnog boljitka, kao npr. političkoj pobjedi na izborima, većoj zaradi te uštedi resursa na poslu, novim znanstvenim otkrićima, tehnološkom napretku, spašavanju ljudskih života, pobjedi u ratu i sl. Kada bi se informacija našla na „krivom mjestu“ ili „u krivim rukama“ značilo bi mogućnost štetnih posljedica. Informacija kao temelj znanja je od pamtivijeka bila važan faktor u oblikovanju svijeta i čovječanstva. Bez informacija nema napretka i o njoj ovisi neizmjereno mnogo društvenih, ali i prirodnih procesa te ima vrlo važan utjecaj na svijet koji nas okružuje. Dok se na biološkoj razini informacije prenose preko gena, na društvenoj razini su se informacije prvo prenosile usmenim putem, urezivale su se u drvo ili klesale u kamen, tek kasnije su se zapisivale na papir. Važne zapise su kraljevi držali pod budnim okom stražara jer bi njihov gubitak mogao biti poguban. Znanstvenici su nekad u prošlosti čuvali zapise o svojim izumima vrlo dobro skrivenima, neki su ih zapisivali u šiframa koje su samo oni razumjeli kako bi čak u slučaju krađe ili neovlaštenog pristupa bili sigurni da se neće moći razumjeti. Dok su neki pak birali da nikome ne kažu o izumu niti da ostave ikakav zapis o tome kako ne bi došlo do zlouporabe. Kasnije kroz povijest su se informacije čuvala i prenosila na magnetskim trakama (VHS, kazete), gramofonskim pločama, analognim fotografijama itd. Svima im je zajednička nepraktičnost za obradu samih podataka. Danas, u doba digitalnog društva, novi sadržaji se pretežno kreiraju u digitalnom obliku. Uz prepoznavanje vrijednosti informacija, ulaže se značajan trud za njihovom zaštitom čime počinje nova era informacijske sigurnosti. Posjedovanje ili neposjedovanje određene informacije ima svoju cijenu, stoga ne čudi da se špijunima nude ogromni iznosi novca kako bi otkrili strogo čuvane tajne, pokušava se na ilegalne načine doći do informacija putem raznih vrsta prijevара, hakiranja, neovlaštenim pristupom i sl., dok se s druge strane se ulaže mnogo novaca u podizanje i održavanje potrebitih razina sigurnosti samog informacijskog sustava. U vrijeme kad određene informacije mogu dovesti do velike financijske dobiti, ne čudi potreba da se do željenih informacija dođe na legalne, ali i na ilegalne načine. Čak i bez vanjske prijetnje, čovjek može zbog neznanja ili nemara sam sebi biti najveći neprijatelj. Korištenjem društvenih mreža određeni osobni podaci se objavljuju na svakodnevnoj

razini, a time čovjekovo pravo na privatnost biva ugroženo, kao što dolazi i do kršenja zakona koji štite osobne podatke. Za razumijevanje teme i same problematike potrebno je krenuti od osnova i definicija temeljnih pojmova koji se prožimaju kroz čitav rad kao što su „podatak“, „informacija“, „osobni podatak“, „tajni podatak“, „obrada osobnih podataka“ te „informacijska sigurnost“.⁶

2.1. Podatak i informacija

Postoje mnoge definicije samog pojma podatka, ovisno iz područja promatranja značenja riječi i njenom primjenom u raznim znanstvenim područjima, kao i upotrebu u svakodnevnom životu. Prema Oxfordovom rječniku riječ „data“, koja na engleskom jeziku označava „podatak“, je latinska riječ nastala u 17. stoljeću kao filozofski termin, a pridodaje joj se značenje činjenice koje se skupljaju za daljnje referiranje i analizu.⁷ Ašenbrener Katić (2011) prema Kiš (2002) navodi da je podatak „*bilo koji predmet mišljenja koji može prenijeti informaciju; formalizirani znakovni prikaz činjenica, pojmova i naredaba pogođan za priopćavanje, interpretiranje te analognu i digitalnu obradu.*“⁸

Bez podatka informacija ne bi postojala. Stoga je bitno razumijevanje tog pojma, kao i njegova uloga u odnosu prema informaciji. Prema navedenom, podatak sam po sebi nema značenje, ali je nužan i neizostavan element u formiranju informacije. Riječ „informacija“ (engl. information) je nastala iz latinskog jezika od glagola „informare“ što znači informirati. Pridodaje mu se smisao formiranja uma te učenje prema Oxfordovom rječniku.⁹ Pavlić (2011: 22) u svom radu navodi da je „*informacija protumačeni podatak. Za promatrača koji ne može iz podatka izvući informaciju i koji to nikada neće moći, podatak je tek mrlja tinte na papiru, odnosno informacija je izgubljena. Za odluku da li je neki skup znakova podatak informacija ili tek mrlja na papiru presudna je percepcija promatrača.*“¹⁰ Stahl (2006) prema radu Wiener (1954) navodi da su „*informacije naziv za sadržaj kojeg izmjenjujemo s vanjskim svijetom zbog*

⁶ Tako i šire Boban, M., Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu, Zbornik radova Pravnog fakulteta u Splitu, 49 (2012), 3; str. 575-598

⁷ Prema Oxford Dictionaries (2018). URL: <https://en.oxforddictionaries.com/definition/data> [12.02.2021].

⁸ Ašenbrener Katić (2013). *Predstavljanje znanja: pregled područja*. Kvalifikacijski rad. Rijeka: Sveučilište u Rijeci. URL: http://www.inf.uniri.hr/files/datoteke/majam/asenbrener_katic_martina_kvalifikacijski_rad.pdf [20. 01.2021].

⁹ Oxford Dictionaries (2018). URL: <https://en.oxforddictionaries.com/definition/information> [21.01.2021].

¹⁰ Pavlić, M. (2011). *Informacijski sustavi*. Zagreb: Školska knjiga, str. 22.

*prilagodbe na taj svijet i iskazivanja te prilagodbe.*¹¹ Prema Luić (2009: 36) informacija je „resurs za rukovođenje, poput kapitala i rada te predstavlja jednu od najznačajnijih upotreba informacijske tehnologije kao konkurentskog oružja. Kao resurs ima specifična obilježja jer za razliku od materije i energije ne troši se korištenjem niti smanjuje raspodjelom.”¹²

Woodward (2013) prema Floridi (2013) navodi Opću definiciju informacije (engl. General Definition of Information – GDI), u obliku podatka kojem je pridodano značenje, gdje je σ instanca informacije, shvaćena kao semantičkim sadržajem, ako i samo ako vrijede sva tri zadana uvjeta¹³:

- Uvjet 1: Ako se σ sastoji od jednog ili više podataka
- Uvjet 2: Ako su podaci u σ dobro oblikovani
- Uvjet 3: Ako su dobro oblikovani podaci u σ smisleni

Prema čemu se može zaključiti da informaciju ne mogu prenijeti podaci koji nisu dobro oblikovani ili smisleni. Unatoč tome što podatak sam po sebi nema značenje, stavljajući ga u odgovarajući kontekst dobiva se informacija. Npr. skup znakova „25“ je podatak jer se ne zna na što se točno odnosi. Stavljajući ga u kontekst npr. „Imam 25 godina“ dobiva se informacija. U slučaju da osoba ne razumije jezik kojim je izrečena ili napisana informacija, za tu osobu ne dolazi do procesa informiranja već je ta osoba percipirala podatke koji za nju nemaju nikakvo značenje. Za informaciju se može pretpostaviti da je istinita, ali ona to ne mora uvijek biti, stoga je važno definirati dezinformaciju kao i misinformaciju. Prema Hrvatskom jezičnom portalu dezinformacija predstavlja „lažno, netočno prikazivanje činjenica, netočnu vijest, zlonamjerno naveden podatak, objava u medijima („širenje dezinformacija“).”¹⁴ To su lažne informacije namijenjene zavaravanju, osobito propaganda koje je vladine organizacije izdaju suparničkoj vlasti ili medijima. Dok je misinformacija „lažna ili netočna informacija“ prema Oxfordovom rječniku.¹⁵ Granicu između dezinformacije i misinformacije je teško strogo odrediti. Danas nije strano nailaženje na lažne vijesti koje mogu biti slučajno ili namjerno plasirane u medije što je posebno vidljivo u političkoj sferi, kao što je prisutno u svim sferama od društvenog

¹¹ Stahl, B. (2006). On the Difference or Equality of Information, Misinformation, and Disinformation: A Critical Research Perspective. *Informing Science Journal*, vol. 9, str. 84-85. URL: <https://core.ac.uk/download/pdf/10007.pdf> [26.02.2021].

¹² Luić, Lj. (2009). *Informacijski sustavi: Poslovni, logistički i zdravstveni informacijski sustavi*. Karlovac: Veleučilište u Karlovcu, str. 36.

¹³ Woodward, A. (2016) *Liotard and the Inhuman Condition: Reflections on Nihilism, Information and Art*. Edinburgh: Edinburgh University Press, poglavlje 1.

¹⁴ Hrvatski Jezični Portal. URL: <http://hjp.znanje.hr/> [26.02.2021].

¹⁵ Oxford Dictionaries (2018). URL: <https://en.oxforddictionaries.com/definition/misinformation> [26.02.2021].

interesa, ali i na razini pojedinca koji može slučajno ili namjerno širiti neistine ili iskrivljene dijelove istine o sebi i drugima.

2.2. Osobni podatak i tajni podatak

Za razliku od prethodne definicije pojma podatka gdje bi on bio neshvatljiv i neupotrebljiv bez konteksta, osobni podatak ima specifičnije značenje. To je informacija pomoću koje se može jednoznačno identificirati osobu kojoj takav osobni podatak pripada. U čl. 4. st. 1. Opće uredbe o zaštiti podataka EU 2016/679 (dalje **GDPR**) osobni se podaci definiraju kao „svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca”.¹⁶ Dok je prema članku 2. Zakona o tajnosti podataka (2007) podatak „dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika.”¹⁷ Zlouporebe osobnih podataka dovode do kršenja svih onih zakona koji ih štite, kao što je i kršenje prava svakog čovjeka na privatnost.

¹⁶ Iz gore navedene definicije osobnog podatka razvidno je da se osobnim podacima smatraju svi podaci iz kojih se s priličnom vjerojatnošću može iščitati identitet osobe o čijim se podacima radi. Čak i ako vi osobno ne možete iz tih podataka identificirati određenu osobu, podaci se smatraju osobnima ako bi netko drugi mogao. Na primjer, vi iz nečije slike možda niste u stanju odrediti ime i prezime osobe, ali netko drugi, recimo njihov susjed, itekako jest. Kad god sumnjate u kategorizaciju podataka, ispitajte se na taj način. GDPR iz postojećih zakona preuzima koncept osjetljivih podataka, tj. „posebnih kategorija osobnih podataka“. Na te se podatke primjenjuju strože odredbe kojima se dodatno ograničava njihovo prikupljanje, obrada i pohrana. Posebnim kategorijama podataka pripadaju: raso ili etničko porijeklo, politička, vjerska i filozofska uvjerenja, članstvo u sindikatu, genetski i biometrijski podaci, podaci o zdravlju, spolnom životu i seksualnoj orijentaciji. Usporedi Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) 2016/679, Službeni list Europske unije, L 119, 4 svibnja 2016., dostupno na <https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=HR>

¹⁷ Zakon o tajnosti podataka. Narodne novine, br. 79/07, NN 79/07, 86/12

Ako se riječi podatak pridoda riječ „tajna“ koja prema Hrvatskom jezičnom portalu označava „*ono što se nikomu ne smije reći, ono što mora ostati skriveno, ono što se taji, skriva, što se ne priča, ne objavljuje*“¹⁸ dobije se pojam „tajni podatak“. On je definiran u Zakonu o zaštiti tajnosti podataka (1996) kao „*podatak koji je zakonom, drugim propisom, općim aktom ili drugim aktom nadležnog tijela donesenim na temelju zakona, određen tajnim*.“¹⁹ Npr. otkrivanje tajni osobnog života osobe do kojih se došlo obavljanjem zanimanja kao što su socijalni radnici, odvjetnici, zdravstveni radnici i drugi službenici značilo bi otkrivanje profesionalne tajne.

2.3. Obrada osobnih podataka i informacijska sigurnost

Informacije ne bi bile ni približno iskoristive u današnje doba da ih se ne obrađuje. Uz pomoć računala i mogućnosti skladištenja podataka njihovo obrađivanje je potrebno za funkcioniranje društva kakvog danas poznajemo. Prema rezultatima obrade se donose određeni zaključci i osmišljavaju daljnja djelovanja što ih čini nužnima za većinu poslovnih procesa. GDPR definira obradu osobnih podataka kao „*svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje*“²⁰ Prema Pavlić (2011:31) „*funkcija obrade podataka se ostvaruje programima za automatizaciju procesa sustava (ili ljudskim radom) i to tako da se uzimaju podaci iz baze podataka i njihovi podaci iz sustava te se generiraju podaci za bazi i sam sustav*.“²¹ Ipak, u današnjem vremenu je mnogo veći naglasak na automatizaciji procesa sustava obrade, čijim se uvođenjem minimizira ljudski rad uz pomoć računala, računalnih programa i ostalih tehnoloških naprava. Takva obrada pridonosi povećanoj učinkovitosti poslovnih procesa, što u konačnici može rezultirati benefitima poput uštede resursa te rasta prihoda. No, jedan od najvećih pokretača obrade takvih podataka je ipak financijska korist. Digitaliziranjem brojnih informacija se stvorilo okruženje koje omogućuje da se iz tog „mora informacija“ uz pomoć pametnih algoritma-

¹⁸ Hrvatski Jezični Portal. URL: <http://hjp.znanje.hr/> [29.03.2018].

¹⁹ Zakon o zaštiti tajnosti podataka. Narodne novine, br. 108/1996. (stavljen van snage)

²⁰ GDPR, čl. 4. st. 2.

²¹ Pavlić, M. (2011). *Informacijski sustavi*. Zagreb: Školska knjiga, str. 31.

ma dođe do vrijednih saznanja. Stoga ne čudi potreba raznih firmi, korporacija, udruga i sl. za prikupljanjem i obradom osobnih podataka jer tako mogu doći do samog pojedinca čije se životne navike mogu promatrati i na njih se može pokušati utjecati. Vrlo je bitno naglasiti važnost transparentnosti same obrade jer se ipak radi o podacima koji su pravno zaštićeni. Potrebno je utvrditi: način prikupljanja podataka, postojanje privole za obrađivanjem podataka, vremenski rok čuvanja podataka, službene osobe koje imaju pristup tim podacima itd.

S obzirom na važnost i vrijednost koje informacije mogu imati, bitno je definirati sami pojam informacijske sigurnosti. Člankom 2. Zakona o informacijskoj sigurnosti (2007) definiran je pojam informacijske sigurnosti kao „*stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.*“²² Vrijednost informacije ovisi o promatraču. Za osobu kojoj ta informacija nije u interesu, ona za nju može biti bezvrijedna, bez obzira na to što milijunima drugih ljudi može biti od životne važnosti. Ipak, sve vrijedne i povjerljive informacije je potrebno čuvati i zaštititi određenim sigurnosnim mjerama ovisno o razini tajnosti i trenutnim potrebama kako ne bi došlo do njihove zlouporabe. Stoga je informacijska sigurnost ključ današnjeg informacijskog društva koji se temelji na razmjeni brojnih informacija i stvaranju novih znanja.

2.4. Sigurnost informacijskog sustava i izvori ugrožavanja

Kao što je sam informacijski sustav složen pojam koji se može rastaviti za više zasebnih elemenata od kojih je svaki po svojoj svrsi i sastavu drugačiji od ostalih, također se i prilikom realizacije sigurnosti IS-a treba voditi računa o svakom zasebnom elementu kako bi u cjelini bio što zaštićeniji od napada. Zavod za sigurnost informacijskih sustava definira sigurnost IS kao „*područje IS u okviru kojega se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranoga podatka koji se u informacijskome sustavu obrađuje, pohranjuje ili prenosi. Sigurnost informacijskoga sustava obuhvaća i zaštitu njegove cjelovitosti i raspoloživosti u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskoga sustava.*“²³ Sigurnost informacijskog sustava bi trebala započinjati od samog planiranja. Poželjno je u samom početku misliti na sigurnost i voditi se njome kao smjernicom za di-

²² Zakon o informacijskoj sigurnosti. Narodne novine, br. 79/07. Članak 2.

²³ Zavod za sigurnosti informacijskih sustava (s.a.) URL: <https://www.zsis.hr/default.aspx?id=345> [26.2.2021]

zajnjiranje što sigurnijeg sustava (engl. Security by design) jer je kompliciranije već izgrađeni sustav bitno mijenjati, nego ga odmah izraditi prema adekvatnim sigurnosnim potrebama.

Prema Šimunović (2010: 32) predmet provođenja zaštite i sigurnosti mogu biti²⁴:

- raznovrsni kadrovi
- raznovrsni informatički sadržaji
- raznovrsni objekti, informatička oprema i pomoćna postrojenja
- raznovrsni hardversko-sofverski i mrežni postupci (npr. planirane mjere zaštite i sigurnosti)
- raznovrsne evidencije, tipa: ovlaštenih osoba i informatiziranih korisničkih mjesta
- raznovrsne aplikacije za korištenja povjerljivih (i sl.) podataka IS-a
- raznovrsne evidencije neovlaštenih osoba i terminala

Prema radu Dragičević (1999: 57) napadi se mogu podijeliti i prema samoj volji napadača na *namjerne i slučajne*.²⁵ Kod namjernih, napadač svojom voljom i uz potpunu svjesnost čini štetu sustavu svojim činjenjem ili nečinjenjem tj. svojom pasivnošću u vidu neobavljanja svojih dužnosti. Dok kod slučajnih, nema svjesnosti o mogućim posljedicama radnje koja je izazvala štetu. Svakako da najveću opasnost ipak uvijek ljudski faktor, posebno onaj s atributom namjernosti.

Prema radu Kacian i Filipović (2017: 9) Razlozi napada se mogu podijeliti na²⁶:

- Istraživanje i procjena (engl. Surveying and Assessing)
- Iskorištavanje i prodor (engl. Exploiting and Penetration)
- Povećanje privilegija (engl. Escalation of Privileges)
- Održavanje pristupa (engl. Maintaining Access)

Ciljevi samih napada mogu se uvelike razlikovati ovisno o tome što se s njima želi postići. Neki od njih se izvode kako bi se drugoj strani napravila šteta koja bi bila odmah jasna i vidljiva, dok drugi napadi mogu biti pritajeni kako bi se dugoročnije bilo u doticaju sa sustavom bez da se otkrije da je sustav napadnut. U velikom broju slučajeva sami cilj napada je dolaženje do određenih informacija koje su od određenog interesa. Informacije od kojih bi treće strane mogle biti od materijalne koristi su posebno osjetljive (sustavi banaka, sustavi

²⁴ Šimunović, V. (2010). Uvod u informacijske sustave. Zagreb: Učiteljski fakultet Sveučilišta u Zagrebu, vol. 2. str. 32.

²⁵ Dragičević, D. (1999). Zaštita informacijskih sustava od kompjutorskog kriminaliteta. Disertacija. Zagreb: Sveučilište u Zagrebu, str. 57.

²⁶ Kacian, D; Filipović, M. (2017) Sigurnost informacijskih sustava. Zagreb: Visoka škola za sigurnost, str. 9.

za novčane transakcije itd.). Kako bi se približili što većem broju potencijalnih žrtava, popularno je izrađivanje malicioznog softvera uz razne tipove prijevара kako bi se na dosjetljive načine pokušalo doći do željenih podataka ili uzrokovanje štete u vidu onemogućavanja uobičajenog rada sustava.

3. UTJECAJ POJEDINCA NA VLASTITU INFORMACIJSKU SIGURNOST

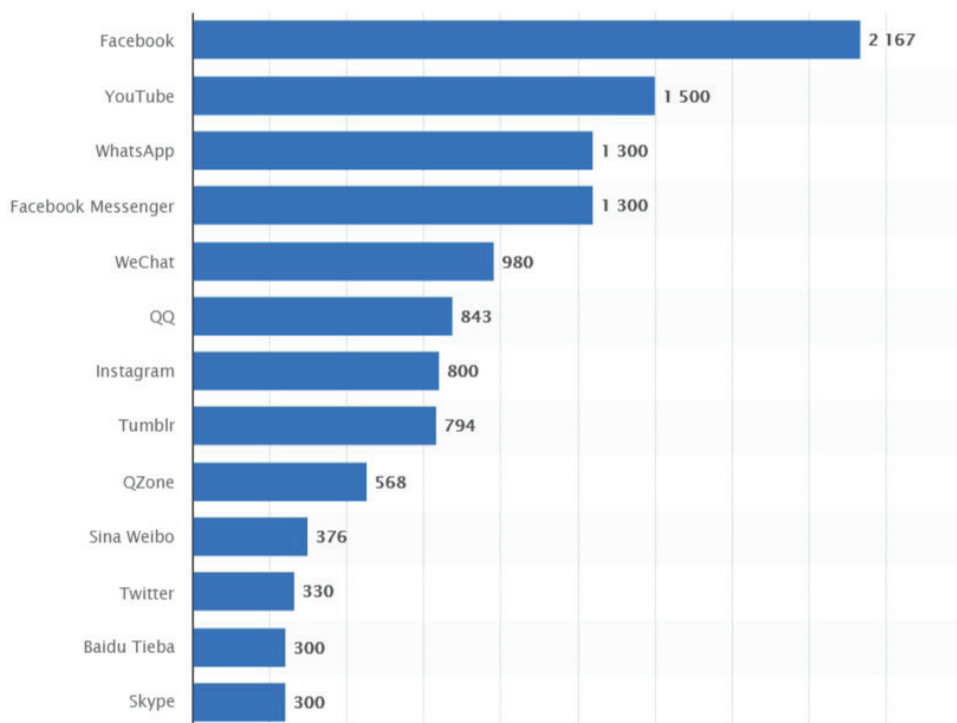
Kada se priča o prijetnjama na internetu, pojedinci mogu čak i u današnjim vremenima zamisliti asocijalnog hakera s kapuljačom u koji u mračnoj prostoriji ispred računala dolazi ilegalnim načinima do tuđih podataka a pritom i do osobne koristi. Pritom se zaboravlja da korisnici sami i to potpuno svojevoljno otkrivaju svoje osobne podatke na svakodnevnoj razini, a svaki pojedinac koji nema dovoljno znanja o mogućim sigurnosnim prijetnjama kao i o pravu na privatnost može sam sebi postati najveći neprijatelj.

3.1. Društvene mreže

Televizija, radio i papirnato izdanje novina i dalje su važni izvori vijesti, ali njihov utjecaj se s porastom broja korisnika interneta smanjio. Ne čudi da su svi ozbiljni mediji odlučili biti „u koraku s vremenom“ te imaju svoje web stranice gdje također objavljuju sadržaje kako bi bili u doticaju sa što većim brojem ljudi te tako imati što veći utjecaj u društvu. Paralelno s porastom broja korisnika laptopa, tableta ali ponajviše mobilnih telefona, društvene mreže postale su bitan dio ljudske svakodnevnice. One omogućuju pojedincu da čita objavljene sadržaje drugih, ali i da sam postane kreator novih sadržaja u bilo kojem trenutku koje mogu imati veliki odjek u javnosti. Razlika između društvene mreže i izvora vijesti ovisi o načinu korištenja samih društvenih mreža, ali njihova područja se u velikom dijelu preklapaju. Uz kameru te mogućnost spajanja na internet, svaki pametni telefon je u mogućnosti objaviti određenu vijest i/ili mišljenje. U svakodnevnom govoru se može čuti „ako nije na Facebook-u kao da ne postoji“, dajući do znanja koliko je u današnjici bitna prisutnost na društvenim mrežama što ima svoje pozitivne i negativne strane. Zbog sličnih fenomena na društvenim mrežama se često može čuti riječ „oversharing“ tj. dijeljenje tolike količine informacija koja se smatra prekoračenjem društveno prihvaćene mjere, ali je podložno subjektivnoj procjeni same mjere. Facebook, Instagram, Twitter, Snapchat samo su neke od društvenih mreža koje se danas

koriste. No, nisu svi korisnici upoznati sa svim mogućnostima društvenih mreža a neke od njih su tu da bi zaštitili njihovu privatnost.

Osim objave vijesti, mobiteli su postali glavni uređaji za međusobnu komunikaciju. Mnoge društvene mreže imaju integriranu mogućnost slanja poruka među svojim korisnicima, kao što to imaju najveće društvene mreže, ali postoje i zasebni servisi za komunikaciju kao što su WhatsApp, Viber, Telegram, WeChat, QQ itd. Prema The Statistics Portal u siječnju 2018. godine ovo su bile najpopularnije društvene mreže i aplikacije za komunikaciju (aplikacije za brzo slanje poruka te poziva/videopoziva) prema broju aktivnih korisnika izraženima u milijunima:



Grafikon 1: Grafički prikaz najpopularnijih društvenih mreža i aplikacija za komunikaciju

Izvor: statista.com (2018), URL: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> [13.02.2021]

Premda društvene mreže imaju mnogo pozitivnih strana, također mogu predstavljati opasnost. Prema Ivanković, Schatten i Bača (2010) opasnosti društvenih mreža koje navodi Joan Goodchild su²⁷:

²⁷

Bača, M; Ivanković, M; Schatten, M. (2010). *Privatnost na Facebook-u i drugim socijalnim mrežama*. URL: <http://bib.irb.hr/datoteka/493687.CZBtemplate.pdf> [11.02.2021].

- Podaci korisnika se dijele trećim stranama
- Postavke privatnosti se mogu vratiti na početne nakon svakog redizajna sustava
- Oglasi mogu sadržavati zlonamjeran softver
- „prijatelji“ mogu jedni druge učiniti ranjivima
- Spameri mogu kreirati lažne profile

Virtualni profili govore korisnicima onoliko koliko im sami dopuste te oni mogu nekad biti sami kreatori sadržaja koji ugrožavaju njihovu sigurnost i privatnost. Npr. objavljivanjem sadržaja (fotografije, videa i ostalih osobnih podataka) djece za koju ne postoji dozvola roditelja (skrbnika) ili objavljivanje sadržaja pomoću kojih se da naslutiti imovinsko stanje (fotografije interijera mjesta stanovanja, marka auta, odjeće i obuće itd.) mogu postati interesantni lopovima kao i objavljivanja fotografija s putovanja može biti dodatan poziv da je stan ili kuća ‘bez nadzora’.

Zbog navedenih razloga bi svakako trebalo više obratiti pozornost na sigurnosne aspekte društvenih mreža, kako bi privatnost samih korisnika bila što očuvanja, a osobni podaci u što manjoj mjeri podložni prijetnjama.

3.2. Pojedinaac na mreži

Kao nastavak na poglavlje o društvenim mrežama potrebno je uvidjeti i problematiku pojedinca na mreži općenito. Ovisno o razini znanja o mogućim prijetnjama, pojedinac može sebe zaštititi od mogućih ugroza, ali može također svoje podatke dovesti u opasnost. Osim društvenih mreža na kojima se objavljuju razni detalji života, fotografije, video sadržaji, trenutne lokacije, interesi itd. što može predstaviti sigurnosni problem, njihovi privatni podaci prestaju biti privatni već se javno otkrivaju i bivaju skladišteni određeno vrijeme na raznim serverima bez znanja samog korisnika što se s njegovim podacima u pozadini događa. No, postoje mnogi drugi načini ugrožavanja, dobrim dijelom zbog nedovoljnog opreza te nedovoljnog znanja samog o načinima na kojima je potrebno zaštititi svoje podatke.

Prema istraživanju Hrvatske Udruge Banaka (2017) o utvrđivanju stupnja osjećaja ugroženosti i razinu osviještenosti o sigurnosnoj zaštiti prilikom korištenja interneta na 1000 ispitanika, zabrinjavajućim se pokazalo što 56% ispitanika smatra da nisu ugroženi na internetu, dok njih 40% uopće ne razmišlja o tome. Nemaju naviku mijenjanja lozinki, 59% ih mijenja jednom godišnje ili rjeđe. Na otvorene mreže se 37% ispitanika se spaja u svakoj prilici. O autentičnosti i pouzdanosti stranice uopće ne razmišlja 34% ispitanika. Pozitivno je

da 93% ignorira ili briše nepoznate poruke ili e-mailove s nepoznatim „linkovima“.²⁸

Spajanjem na otvorenu nepoznatu mrežu korisnici ne mogu znati prati li netko njihove radnje i spremaju li se njihovi podaci u pozadini, a posebno je ugrožavajuće ako pritom koriste aplikacije za mobilno bankarstvo ili obavljaju kupovinu upisujući podatke sa svojih bankovnih kartica. Nepažnja prilikom spremanja lozinki ili dijeljenja lozinki svojih računa s drugima dovodi osobne podatke u opasnost. Posjećivanje stranica koje nemaju certifikate sigurnosti (SSL/TLS) mogu dovesti do zaraze računala s virusima te onemogućiti rad računala te kompromitirati podatke na njemu. Također nije preporučljivo da se na takvim stranicama obavljaju novčane transakcije.

3.3. Djeca na mreži

Najranjiviju skupinu čine djeca. „*Dijete je osoba koja nije navršila 18 godina života.*“ (KZ gl. 8. čl. 87. st. 7.)²⁹ Također, prema Konvenciji o pravima djeteta iz 1989. god. (čl. 1.) „*dijete označava svaku osobu mlađu od 18 godina, osim ako se zakonom koji se primjenjuje na dijete granica punoljetnosti ne odredi ranije.*“³⁰ Ona danas imaju pristup modernoj tehnologiji, pametnim telefonima, tabletima, računalima i igraćim konzolama, preko njih mogu obavljati školske zadaće, igrati se, konzumirati multimedijalni sadržaj, komunicirati s obitelji, svojim vršnjacima ali i potpunim strancima te mogu biti izloženi raznovrsnim neprimjerenim sadržajima ali, nažalost, mogu biti i žrtve kaznenih djela.

Istraživanje „*Pristup i korištenje, rizik i mogućnosti interneta za djecu u Italiji*“ pokazuje da 84% djece u dobi od 9 do 17 godina koristi pametne telefone za pristup internetu bar jednom dnevno. Postotak djece koji je pri tome doživio neku vrstu neugode (uzrujanosti, uplašenosti, uznemirenosti) je 13%. Samo 10% djece je promijenilo svoje postavke privatnosti nakon neugodnog iskustva, svako treće dijete je reagiralo zatvarajući aplikaciju („prozor“) ili je problem ignoriralo dok svako četvrto dijete nije nikome ispričalo za taj događaj. (Mascheroni i Olafsson, 2017)³¹ Istraživanje „*Rizici i sigurnost na inter-*

²⁸ Hrvatska udruga banaka (2017). *U Europskom mjesecu kibernetičke sigurnosti istraživanje HUB-a pokazuje: Hrvati ležerno koriste Internet, no većina je oprezna.* URL: <http://hub.hr/hr/u-europskom-mjesecu-kiberneti%C4%8Dke-sigurnosti-istra%C5%BEivanje-hub-pokazuje-hrvati-le%C5%BEerno-koriste> [06.02.2021].

²⁹ *Kazneni zakon.* Narodne novine, br. 125/11.

³⁰ UNICEF (s.a) *Konvencija o pravima djeteta (1989)* URL: https://www.unicef.hr/wp-content/uploads/2017/05/Konvencija_20o_20pravima_20djeteta_full.pdf [25.02.2021].

³¹ Mascheroni, G; Olafsson, K. (2017) *Access and use, risks and opportunities of the internet for Italian children. Preliminary findings.* URL: <http://www.lse.ac.uk/media->

netu: perspektiva djece Europe“ gdje su ispitanici djeca od 9-16 godina u 25 država pokazuje da je zlouporabu osobnih podataka doživjelo 9% djece od 11 do 16 godina u obliku zlouporabe lozinke (7%), njihovih privatnih podataka (4%) ili novčane prevare (1%). (Livingstone et al., 2012)³²

Što više djece koristi Internet i što duže borave na njemu to je veća šansa da će biti u doticaju s mogućim prijetnjama. Djeca nemaju dovoljno saznanja o svim mogućim opasnostima na koje mogu naići boraveći „na mreži“ niti ih mogu razumjeti kao odrasli, zbog toga je njihova zaštita posebno bitna kao i podizanje svijesti društva za tu najranjiviju skupinu.

4. NOVI IZAZOVI INFORMACIJSKE SIGURNOSTI I PRIVATNOSTI

Već su se mogle uvidjeti pogodnosti tehnološkog napretka te informacijske revolucije. Povezivanjem više računala (uređaja) u isti sustav, dobije se mogućnost da svi istovremeno sudjeluju u izmjeni informacija. Postoji mnogo razolikih sustava, manjih i većih, otvorenih i zatvorenih, lokalnih i globalnih koji razmjenjuju informacije i prema njima djeluju. Što bi se desilo kada bi većina uređaja, usluge i procesa koje svakodnevno obavljamo bila umrežena tako da međusobno dijele informacije? Uz pomoć pametnih algoritama i novih tehnologija, mogućnosti su raznolike i gotovo beskonačne kao npr. indikator slobodnog parkirnog mjesta ili prometnih gužvi, obavijesti takvog tipa bi se mogle servirati na mobilnim uređajima koji bi preko servisa navigacije (GPS-a) mogli pravovremeno obavijestiti korisnike o smjeru kretanja. Mogućnosti su beskonačne a omogućavale bi uštedu vremena uz smanjenje troškova kada bi se do većine potrebitih informacija moglo doći putem računala ili pametnog telefona umjesto čekanja u redu na šalterima banaka, zdravstvenih ustanova itd. Već se radi na projektima povezivanja velikih sustava na državnoj razini, kao npr. približavanje javnih usluga putem servisa e-Građani ili e-Zdravstvo. Ta dva velika sustava mogu biti podsustavi još većeg sustava tzv. „Pametnog okruženja“ koji bi omogućio izmjenu informacija među takvim manjim i većim sustavima te bi mogao promijeniti svakodnevnicu kakva se danas poznaje.

and-communications/assets/documents/research/eu-kids-online/reports/Executive-summary-Italy.pdf [20.02.2021].

³² Livingstone et al. (2012). Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. *LSE Research Online*, URL: <http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf> [20.02.2021].

4.1. E-Građani

Kako bi se građanima olakšao pristup i komunikacija s javnom upravom, kao i minimizacija procesa te povećana transparentnost unutar same javne uprave, napravljen je sustav e-Građani. Koristeći web stranicu Središnjeg državnog portala www.gov.hr, građani mogu pristupiti javnim uslugama Republike Hrvatske u elektroničkom obliku (matične knjige, provjeriti izabranog liječnika, OIB, ocjene djeteta itd.)³³

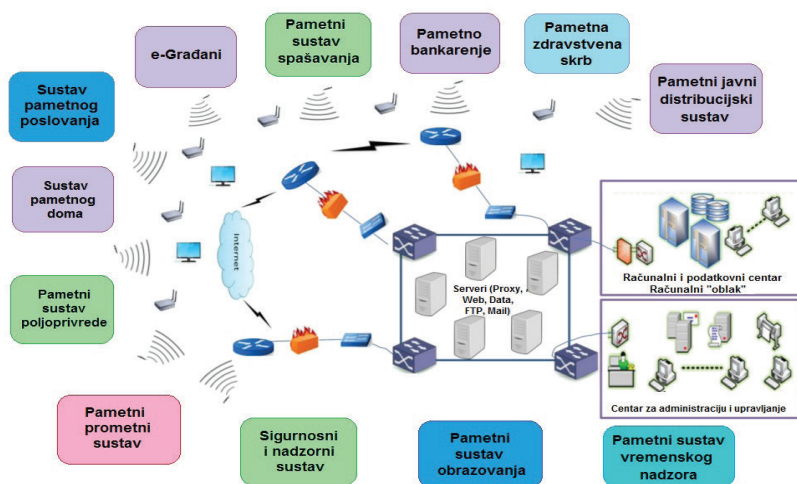
S obzirom na široki raspon usluga koje obuhvaćaju privatne informacije građana, postavlja se pitanje sigurnosti takvog sustava. Sama autentifikacija na sustav je strogo definirana sigurnosnim razinama te provjerenim vjerodajnicama koje su uključene u Nacionalni identifikacijski i autentifikacijski sustav (NIAS) ali jednom hakirani profil određenog građana ili hakiranje cijelog sustava omogućuje da se uvelike naruši privatnost svih građana čiji se privatni podaci tamo nalaze. Ne treba niti zanemariti mogući problem zaposlenika koji rade na samom sustavu zbog njima dostupnim povjerljivim informacijama.

4.2. Internet stvari

Internet stvari (engl. Internet of Things – IoT) „*globalna arhitektura informiranja u nastajanju koja olakšava razmjenu roba i usluga u globalnim mrežama opskrbnog lanca* koja ima utjecaj na sigurnost i privatnost uključenih sudionika“ (Weber, 2010: 23)³⁴ Napretkom tehnologije i sve većom međusobnom povezanosti uređaja na mreži omogućavaju širok spektar novih mogućnosti. Pametni sustavi pomoću naprednih algoritama mogu olakšati čovjekovu svakodnevicu. IoT može raditi na principu ‘oslušivanja’ svih uređaja u njegovom sustavu u realnom vremenu, omogućavajući opskrblijanje sustava traženim informacija i djelovanje prema njima u bilo kojem trenutku. Posljedično dovodi do minimiziranja procesa, smanjenja troškova, pregleda stanja sustava u realnom vremenu, povećanom prilagodljivosti trenutnim potrebama, efikasnijeg i transparen tnijeg sustava na razini samog korisnika, ali i na razini pružatelja usluga. Primjeri primjene modela takvog sustava su: „Pametni parking (engl. Smart Parking)“, „Pametni otpad (Smart Waste)“, Pametni sustav poljoprivrede itd.

³³ Središnji državni portal (s.a) URL: <https://uprava.gov.hr/vijesti/postanite-e-gradjanin/459> [27.07.2020].

³⁴ Weber, R. (2010). Internet of Things – New security and privacy challenges. *Elsevier*. str. 23. URL: <https://pdfs.semanticscholar.org/9d65/08a44e957d837490d69936db5a211432a411.pdf> [29.07.2018].



Slika 1. Primjer „Pametnog okruženja“ utemeljenog na arhitekturi IoT

Izvor: Adaptacija prema Rabara, S; Vimal, J; Bai, D. (2015) Internet of Things (IoT) based Smart Environment integrating various Business Applications.

International Journal of Computer Applications, Vol. 128 (8). str. 33. URL: <https://pdfs.semanticscholar.org/9c90/6adc35824d5d36029b31cb5bf3fb08eacbba.pdf> [19.02.2021.]

Kod „Pametnih okruženja“ je naglašeno pitanje privatnosti jer neovlaštenim pristupom profilu korisnika ili cijelom sustavu se može doći do osobnih podataka korisnika, kao i do informacijama o njihovim životnim navikama. Kada bi došlo do toga, korisnikove navike bi se mogle pratiti bez da on u to ima uopće uvida što je izravno kršenje prava na privatnost.

4.3. Profiliranje

Prema Oxfordovom rječniku profiliranje (engl. profiling) je „*praćenje i analiza osobnih psiholoških i bihevioralnih obilježja kako bi se procijenile ili predvidjele njihove sposobnosti u određenoj sferi ili pomogle u prepoznavanju kategorija ljudi.*“³⁵ Prema Gutwirth i Hildebrandt (2009: 1) „*profiliranje se može odnositi na pojedinu osobu, grupu ili grupe ljudi, ali i životinja, objekata i odnosa među njima.*“³⁶ Svaki pojedinac je tijekom života na neki način bio

³⁵ Oxford Dictionaries (2018). URL: <https://en.oxforddictionaries.com/definition/profiling> [12.01.2021.].

³⁶ Gutwirth, S; Hildebrandt, M. (2009). *Profiling the European Citizen*. URL: https://www.researchgate.net/publication/265271420_Profiling_the_European_Citizen [03.02.2021.].

profiliran. Neki od primjera profiliranja s kojima se ljudi mogu susresti su npr. testiranje za odabir željene srednje škole, fakulteta ili zanimanja, prilikom ispunjanja anketa (telefonskih, na papiru ili preko interneta) o mišljenjima i navikama. No, za takve vrste profiliranja se uglavnom svjesno daje privola. Također se profiliranje može vršiti i bez znanja pojedinca, npr. policija u sklopu obavljanja svojih dužnosti vrši kriminalističko profiliranje. Profiliranje kao pojam postoji u mnogim znanstvenim sferama. Poznaje se kriminalističko profiliranje, geografsko profiliranje, psihološko profiliranje, marketinško profiliranje i dr. No, u ovom radu će biti govora samo o onim razlozima i metodama profiliranja koje nedopušteno krše ljudsko pravo na privatnost.

4.3.1. *Profiliranje u službi ciljanog oglašavanja proizvoda i usluga*

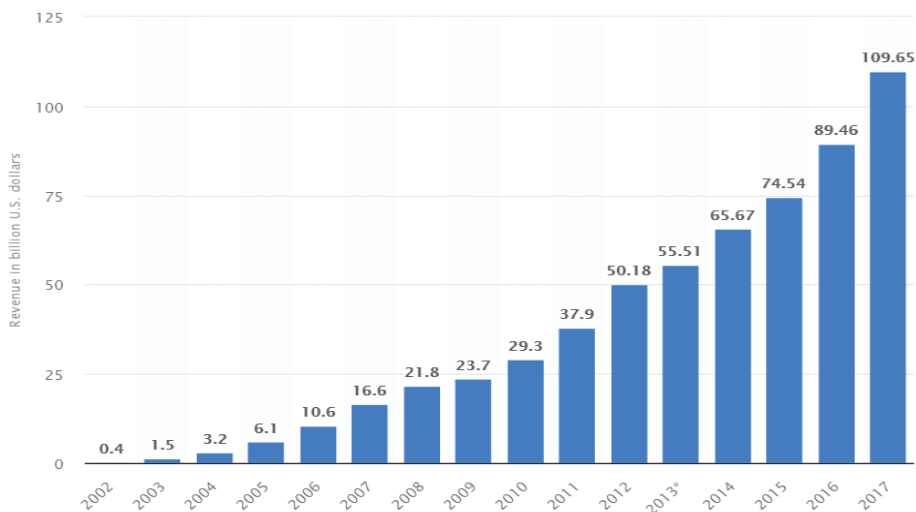
Uz ogromne količine podataka koje se u svakom trenutku prikupljaju i izmjenjuju putem interneta, pokazalo se poželjnim pratiti određene karakteristike ili obrasce ponašanja te iz njih donositi zaključke uz mogućnost predviđanja budućih obrazaca ponašanja. Svaki pojedinac na mreži ostavlja mnoštvo digitalnih tragova koji otkrivaju njegove životne navike. Neki od tragova mogu biti posjećivane web stranice, „lajkane“ fotke i članci na internetu, trenutna lokacija, saznanja o njihovim hobbijima i interesima, saznanja o osobama s kojima se druže, gdje žive, gdje studiraju i rade, koja mjesta posjećuju i mnogi drugi, što ih čini metama za ciljano oglašavanje. Ono je danas sveprisutno i gotovo da nema čovjeka spojenog na internet koji se s takvim oblikom oglašavanja nije već susreo, ponekad i bez da je dao privolu tzv. dopuštenje da se prati njegovo ponašanje na mreži i koristi u takve svrhe. Sloot i Borgesius (2012) prema Radnoj skupini članka 29. (2010) o ciljanom oglašavanju za EU direktivu, navode da „*takvo oglašavanje podrazumijeva praćenje ponašanja korisnika na internetu kako bi se izgradili profili korisnika kojima bi se ciljano prikazivale reklame.*“³⁷ Kao rezultat se onima koji „lajkaju“ npr. stranice i sadržaje o video igrama, mogu se pojaviti reklame s video igrama koje su pretraživali, kao što se mogu predložiti slične igre koje bi tog pojedinca mogle zanimati ili ići korak dalje i predviđati ostale moguće potrebe te reklamirati i opremu za igranje video igara. Najbitniji motiv za to je mogući profit, a videoigre i oprema za igranje čine vrlo veliko i raznoliko tržište u svijetu, samo u 2015. godini njihova tržišna vrijednost je bila 91 milijardu dolara s tendencijom rasta.³⁸ Isto se može primijeniti i na bilo koju drugu skupinu ljudi kao što su ljubitelji nogometa ili

³⁷ Sloot, B; Borgesius, F. (2012) *Google and Personal Data Protection*. URL: https://www.ivir.nl/publicaties/download/Google_Data_Protection_2012.pdf [03.02.2021.].

³⁸ Campbell, C. (2015) *Worldwide video games market will grow 9.4 percent this year, says report*. URL: <https://www.polygon.com/2015/4/22/8471789/worldwide-video-games-market-value-2015> [03.02.2021.].

neko drugog sporta, ljubitelji hrane i restorana, ljubitelji životinja i kućnih ljubimaca itd. primjera je beskonačno mnogo, a nekad je dovoljna samo jedna posjeta određenoj stranici da reklame povezane uz nju „prate“ tog korisnika određeno vrijeme na internetu.

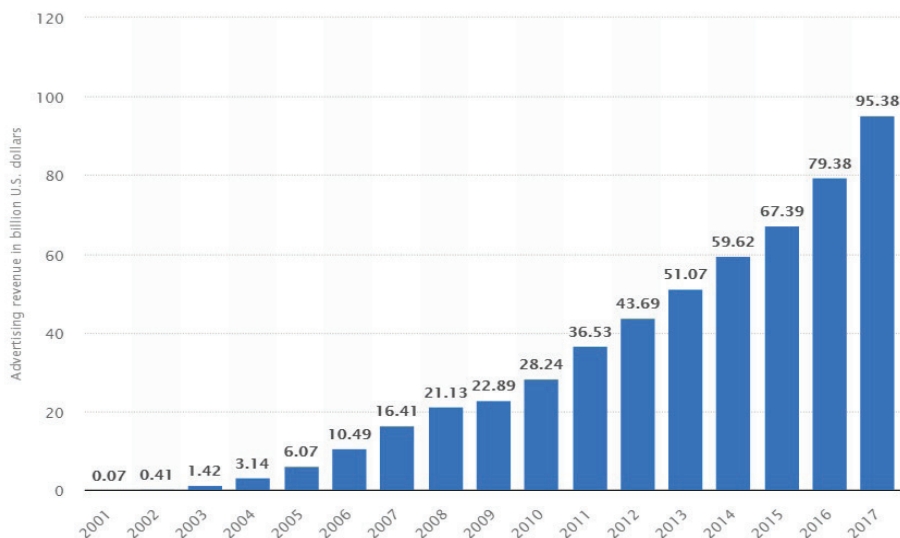
Google kao svjetski internet div svojim korisnicima nudi mnoštvo besplatnih usluga kao što je pretraživanje preko jedne od najrazvijenijih svjetskih tražilica - Google Search, svoj web preglednik Google Chrome, preko kojeg posjećuju web stranice koje ih zanimaju, e-mail server Gmail na kojem se primaju privatni i poslovni mail-ovi kao što su rezervacije letova, hotela, potvrde o kupovini artikala i usluga putem interneta, izvješća tekućih i žiro računa itd. Nadalje, nudi virtualni prostor za spremanje podataka Google Drive, mogućnost automatskog spremanja fotografija i slika korisnici imaju na mobilnim i drugim uređajima i to bez ograničenja kapaciteta preko servisa Google Photos. Što znači da se sve fotografije i slike na tim uređajima, ako ih se tako podesi, automatski kopiraju i šalju na Google servere gdje se čuvaju „vječno“. Popularna je i platforma za gledanje video sadržaja Youtube gdje svatko može kreirati svoj profil i pregledavati među milijardama ponuđenih videa raznih sadržaja prema vlastitim interesima. Uz sveprisutnost i dostupnost svojih besplatnih usluga, Google i dalje bilježi konstantan rast prihoda. Na grafikonu 2. prikazan je raspon prihoda od 2002. do 2017. godine izražen u milijardama dolara:



Grafikon 2: Prihod kompanije Google od 2002. do 2017.

Izvor: The Statistics Portal. URL: <https://www.statista.com/statistics/266206/googles-annual-global-revenue/> [05.02.2021.]

Za usporedbu, grafikon 3. prikazuje zaradu od oglašavanja od 2001. do 2017. godine izraženu u milijardama dolara:



Grafikon 3: Prikaz prihoda od oglašavanja kompanije Google.

Izvor: The Statistics Portal URL: <https://www.statista.com/statistics/266249/advertising-revenue-of-google/> [05.05.2018]

Iz priloženog je vidljivo da Google većinu svojih prihoda ostvaruje preko reklamiranja.

Google se godinama fokusirao na manje oglase pored rezultata pretraživanja koji su bili povezani sa samim pretraživanjima korisnika. U to vrijeme je kompanija DoubleClick bila lider u bihevioralnom oglašavanju preko 15 godina te je Google dao 2007. godine 3.1 milijardu dolara za vlasništvo nad tom kompanijom i krenuo još ozbiljnije u to tržište. Sloot i Borgesius (2012).³⁹

Prilikom posjeta na određenoj web stranici, može iskočiti obavijest o prihvaćanju „kolačića“ (engl. cookies) kako bi se omogućilo najugodnije iskustvo surfanja na određenoj stranici. Kolačić je „jednostavna tekstualna datoteka koju na vaše računalo ili mobilni uređaj pohranjuje poslužitelj internetske stranice. Taj poslužitelj onda može pokupiti ili čitati sadržaj vašeg kolačića. Kolačićima upravlja vaš internetski preglednik.“ (Europska Komisija, 2018)⁴⁰ Da nema kolačića, web stranice ne mogle prilikom svakog posjeta korisnika znati

³⁹ Sloot, B; Borgesius, F. (2012) Google and Personal Data Protection. URL: https://www.ivir.nl/publicaties/download/Google_Data_Protection_2012.pdf [03.04.2018].

⁴⁰ Europska komisija (s.a.) Kolačići i privatnost. URL: <http://www.europarl.europa.eu/portal/hr/cookie-policy> [06.04.2018]

da li se radi o novom korisniku ili ne te bi određene postavke trebalo ponovno namještati. Čak i da se ne napusti sama web stranica, bez kolačića se teže pamte radnje korisnika, što otežava korištenje same stranice

Primjer jednog Doubleclick-ovog kolačića (Geary, 2012)⁴¹:

time: 06/Aug/2008 12:01:32

ad_placement_id: 105

ad_id: 1003

userid: 000000000000000001

client_ip: 123.45.67.89

referral_url: "http://youtube.com/categories"

„Time“ označava vrijeme i datum pogledane reklame.

„Ad placement id“ označava jednoznačni identifikacijski broj lokacije na kojem je reklama postavljenja

„Ad id“ označava jednoznačni identifikacijski broj reklame

„Client ip“ označava IP adresu korisnika koji je pristupio reklamama preko koje se može saznati lokaciju korisnika

„Referral url“ označava stranicu na kojoj je reklama pogledana

Facebook kao društvena mreža s najvećim brojem korisnika koji premašuje 2 milijarde, također nudi mogućnost oglašavanja, kao i na Instagram-u, društvenoj mreži od 800 milijuna korisnika koja je također u njihovom vlasništvu. Prema tim impresivnim brojkama se može lako zaključiti zbog čega se pružatelji usluga i proizvoda žele reklamirati i putem tih društvenih mreža. Svi njihovi korisnici ostavljaju mnogo digitalnih tragovima tj. vrijedne informacije koje mogu povezati pružatelje usluga i proizvoda s potencijalnim klijentima. Na Facebooku se prilikom registracije upisuju osobni podaci poput imena, prezimena, datuma rođenja i broja mobitela koji su obavezni. A mnogi upisuju i rubrike poput mjesta rođenja, mjesta stanovanja, škole, fakulteta ili trenutnog radnog mjesta, religijske pripadnosti itd. preko kojih se tu osobu može direktno identificirati. Osim toga, prilikom korištenja same stranice korisnici otkrivaju svoje interese, „lajkaju“ stranice tj. mjesta, usluge i proizvode koji ih interesiraju te ih objavljuju na svom profilu koji je dostupan njihovim Facebook „prijateljima“ ali nekad i potpuno javno, svima dostupno, čak i korisnicima koji nemaju otvoren Facebook profil. Objavljuju raznolik i multimedijalan sadržaj kao što su njihova mišljenja, fotografije, videa, trenutne lokacije, događaji i mjesta koje su posjetili, kao i objavljivanje idućih lokacija, događaja i mjesta koja će posjetiti, ali i serije i filmove koje gledaju, glazbu koju slušaju, fotografije

⁴¹ Geary, J. (2012) URL: DoubleClick (Google): What is it and what does it do? URL: <https://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring> [05.02.2021.].

svoje djece, svojih kućnih ljubimaca ili hrane, kao što i daju do znanja s kojim osobama provode svoje vrijeme i dijele sve te aktivnosti itd. Dok s druge strane, sam Facebook profitira zbog posjedovanja ogromne količine informacija o svojim korisnicima jer može na njih primijeniti ciljano oglašavanje.

4.3.2. Drugi razlozi i načini profiliranja te ciljanog oglašavanja

Problematika profiliranja i ciljanog oglašavanja nije vezana samo za društvene mreže i prodaju konkretnih proizvoda ili usluga putem interneta, već može biti povezana i s drugim popularnim kompanijama poput supermarketa, drogerijskih lanaca i ostalih kompanija koje imaju tzv. kartice povjerenja prema kojima dobivaju uvid u potrošačke navike svojih korisnika, kao i lokacije na kojima se najčešće kreću i kupuju. Za primjer, na stranicama dm-Drogeriemarkt prodajnog lanca su navedena načela kompanije: „DM načela kupaca: Koristeći se svim marketinškim instrumentima, želimo se profilirati prema potrošačima kako bismo pridobili stalne kupce koji svjesno dolaze kupovati kod nas i čije potrebe oplemenjujemo vlastitim proizvodima i uslugama.“⁴²

Ne mora se profiliranje i ciljano oglašavanje vršiti samo zbog internet prodaje. Ono je vrlo interesantna i poželjna metoda obrade podatka i u slučaju političkog djelovanja. Digitalni tragovi mogu otkriti političke preferencije, trenutna mišljenja, nedoumice, koji mogu političkim stranama dati smjernice za daljnje djelovanje kako bi dobili prevagu na izborima. Putem društvenih mreža, e-mailova, blogova, foruma itd. mogu se naići na naizgled nevine ankete koje mogu na prvi pogled djelovati čak i zabavnog karaktera, ali u pozadini se takve informacije bez znanja ispitanika mogu slati trećim stranama koje će na račun njih usmjeravati daljnju kampanju i tako biti u prednosti pred konkurencijom.

5. PRAVO NA PRIVATNOST, NOVI IZAZOVI, METODE ZAŠTITE I MOGUĆNOST NAPRETKA U DOMENI PRAVA

5.1. Privatnost i pravo na privatnost

Prema Oxfordovom rječniku riječ privatnost (engl. privacy) je opisana kao „stanje u kojem pojedinac nije promatran ili uznemiren od strane drugih ljudi.“⁴³ Dok je prema Dictionary rječniku „stanje slobodno od neželjenih ili nepotrebnih upada ili poremećaja u privatnom životu; sloboda od oštećujućeg

⁴² DM Hrvatska. URL: https://www.dm.hr/hr_homepage/o_nama/nacela/ [06.02.2021.]

⁴³ Oxford Dictionaries (2018). URL: <https://en.oxforddictionaries.com/definition/privacy> [07.02.2021].

*publiciteta, javnog nadzora, tajnog nadzora ili neovlaštenog otkrivanja osobnih podataka od strane vlade, korporacije ili pojedinca.*⁴⁴ Kako se navodi u **Općoj deklaraciji o ljudskim pravima** članak 12. „Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada.”⁴⁵ Time se naglasila potreba svakog čovjeka da ima svoj osobni prostor koji mora biti pod posebnom zaštitom, pod njim se ne smatra samo prostorna zaštita već i sveobuhvatno nezadiranje u čovjekovu osobnu sferu što se tiče njegove časti i ugleda, obiteljskog života ili komunikacije s drugima.⁴⁶ **Ustav Republike Hrvatske** (Narodne novine br. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/149) sadrži nekoliko članaka vezanih uz privatnost građana. Članak 34. navodi: „Dom je nepovrediv.”⁴⁷ Time se naglašava važnost privatnog prostora svakog pojedinca i jedino ga se može prekršiti uz poseban pisani nalog koji bi omogućio njegov pretres. Također prema članku 35. „svakom se jamči štovanje i pravna zaštita njegova osobnog i obiteljskog života, dostojanstva, ugleda i časti.”⁴⁸ Čime se naglašava važnost očuvanja čovjekovog ugleda, časti i dostojanstva kao njegovo ljudsko pravo. Osim osobnog života i obiteljski život također je jasno naglašen kao zaštićena sfera. Prema članku 36. „Sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva. Samo se zakonom mogu propisati ograničenja nužna za zaštitu sigurnosti države ili provedbu kaznenog postupka.”⁴⁹ Komunikacija također spada u čovjekovu osobnu sferu, stoga je čovjekovo pravo da se ona i pravno zaštiti. Sami Ustav kao temeljni pravni akt Republike Hrvatske definira načelne propise koje je zabranjeno kršiti jer štite temeljne vrijednosti Hrvatske kao i temeljna ljudska prava pojedinca, a ovim člancima je naglašeno pravo svakog čovjeka na privatnost. Svako kršenje takvih sloboda i prava pojedinca postaje protupravna i protuustavna radnja. Članak 37. navodi „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.”⁵⁰ Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi

⁴⁴ Dictionary.com (2018) URL: <https://www.dictionary.com/> [08.02.2021.]

⁴⁵ Odluka o objavi opće deklaracije o ljudskim pravima. Narodne novine, br. 12/2009, dostupna je na https://narodne-novine.nn.hr/clanci/međunarodni/2009_11_12_143.html [08.02.2021.]

⁴⁶ Ibid.

⁴⁷ Ustav Republike Hrvatske. Narodne novine, br. 85/10. Članak 34.

⁴⁸ Ustav Republike Hrvatske. čl. 35.

⁴⁹ Ustav Republike Hrvatske, čl. 36.

⁵⁰ Ustav Republike Hrvatske, čl. 37.

njihovoga prikupljanja. Članak 33. **Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske** (Narodne novine br. 79/06, 105/06) navodi „SOA može prema građanima primjenjivati mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode. VSOA može primjenjivati mjere tajnog prikupljanja podataka kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode samo prema zaposlenicima, odnosno pripadnicima Ministarstva obrane i Oružanih snaga.“⁵¹ Kršenja prava privatnosti su privremeno dopuštena isključivo pod uvjetom da postoji opasnost da određena osoba ili grupa ljudi predstavlja prijetnju zbog mogućih zakona Republike Hrvatske, drugih članica Europske Unije ili ostalih država s kojima je potpisan takav sporazum.

Konvencija za zaštitu ljudskih prava i temeljnih sloboda (1950) navodi u članku 8. st. 1. da „svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja. St. 2. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.“⁵² Čime se ponovo naglašava važnost osobne sfere svakog pojedinca koja uključuje njegov dom, njegovu obitelj, komunikaciju s drugima te privatan život. Osim u slučajevima nacionalne sigurnosti, mogućih kaznenih djela te ostalih situacija u kojima bi djelovanje protiv tih ljudskih prava bilo „za više dobro“ zbog mogućih prijetnji za RH i njene građane.

Prva definicija osobnog podataka dana je u članku 1. **Zakona o zaštiti osobnih podataka** Narodne novine, br. 103/03. (stavljene van snage 2018. – dalje ZOP), donesenog 2003. godine. navodi da je „zaštita osobnih podataka u Republici Hrvatskoj osigurana svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.“ (ZOP, čl. 1.) Članak 6. navodi „osobni podaci mogu se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom i mogu se dalje obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja. Daljnja obrada osobnih podataka u povijesne, statističke ili znanstvene svrhe neće se smatrati nepodudarnom, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere.“ (ZOP, čl. 6.) Zakon je stavljen van snage 2018. početkom primjene EU Opće uredbe o zaštiti podataka 2016/679 25. svibnja 2018. godine.

⁵¹ Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske. Narodne novine, br. 79/2006.

⁵² Konvencija za zaštitu ljudskih prava i temeljnih sloboda. Narodne novine, br. 18/97

Također **Zakon o tajnosti podataka** (Narodne novine br. 79/07, 86/12) definira klasificirane i neklasificirane podatke. Prema članku 2. **Klasificirani podatak** je „onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje“ **Neklasificirani podatak** je „podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.“⁵³ Prema radu Peran, Goreta i Vukošić (2015: 129) tajne se dijele na javne i privatne. „Javne tajne se odnose na podatke koje su prema propisanim uvjetima dužna čuvati državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te fizičke osobe koje ostvare pristup kvalificiranim i nekvalificiranim podacima. U javne tajne ubrajamo državnu tajnu, vojnu tajnu, službenu tajnu te poslovnu tajnu. Privatne tajne obuhvaćaju podatke koje je jedna osoba saznala od druge na temelju bliskog odnosa i osobnog povjerenja (Jovanović (1959), a dijele se na osobne i profesionalne.“⁵⁴

Za ovaj rad i razumijevanje problematike je bitno naglasiti da određeni osobni podatak može također biti kategoriziran kao tajni podatak. Primjerice, doktori prilikom obavljanja svoje dužnosti mogu dobiti uvid u osobni i obiteljski život svojih pacijenata. Znaju pacijentovu povijest bolesti što spada u njegove najintimnije informacije. Liječničku tj. profesionalnu tajnu doktori, kao i ostalo medicinsko osoblje, dužni su strogo čuvati.

Prema **Kaznenom zakonu Republike Hrvatske** (Narodne novine br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19) čl. 146. st. 1. „Tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba, kaznit će se kaznom zatvora do jedne godine.“ Stavak. 2. „Tko protivno uvjetima određenima u zakonu iznosi osobne podatke iz Republike Hrvatske u svrhu daljnje obrade ili ih objavi ili na drugi način učini dostupnim drugome ili tko radnjom iz stavka 1. ovoga članka sebi ili drugome pribavi znatnu imovinsku korist ili prouzroči znatnu štetu, kaznit će se kaznom zatvora do tri godine.“ Stavak 3. „Kaznom iz stavka 2. ovoga članka kaznit će se tko djelo iz stavka 1. ovoga članka počini prema djetetu ili tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život te osobne podatke fizičkih

⁵³ *Zakon o tajnosti podataka*. Narodne novine, br. 79/07. Članak 2.

⁵⁴ Vidi šire u Peran, B; Goreta, M; Vukošić, K. (2015) *Pojam i vrste tajni*. Zbornik radova Veleučilišta u Šibeniku, 3-4/2015, str. 129

osoba o kaznenom ili prekršajnom postupku.“ Stavak 4. „Ako kazneno djelo iz stavka 1. do 3. ovoga članka počinu službena osoba u obavljanju svojih ovlasti, kaznit će se kaznom zatvora od šest mjeseci do pet godina.“⁵⁵ Čime je posebno naglašeno i kroz Kazneni zakon protupravnost nedopuštenog prikupljanja i obrade osobnih podataka kao i ilegalnog iznošenja osobnih podataka izvan granica RH i njihovo obrađivanje.

5.2. Opća uredba o zaštiti osobnih podataka – GDPR

Kako bi se uvelo reda u kaos koji je vladao zbog nedopuštenog prikupljanja osobnih podataka, njihove obrade i nezakonitog korištenja, Europska unija je 27. travnja 2016. godine odobrila uvođenje Opće uredbe za zaštitu osobnih podataka (engl. *General Data Protection Regulation* - GDPR) na razini svih 28 država članica EU, koja je potom stupila na snagu 25. svibnja 2018. godine, nakon dvije godine adaptacijskog perioda. Time se stavila izvan snage Direktiva 95/46/EZ koja je dotad služila za zaštitu pojedinaca vezano uz obradu njihovih osobnih podataka. Za razliku od direktive, koja daje svakoj pojedinačnoj državi članici mogućnost da odluči kako će njene ciljeve ispuniti, uredba je obavezujući pravni akt za sve države članice i primjenjuje se izravno. Sami ciljevi uvođenja Uredbe su zaštita osobnih podataka svih građana EU, jačanje prava pojedinca koji će nakon uvođenja Uredbe imati veću kontrolu i bolje mehanizme zaštite svojih osobnih podataka, usklađivanje zakona za zaštitu osobnih podataka u svim državama članicama te obavezu prilagođavanja Uredbi svim kompanijama i organizacijama koje žele poslovati na njenom području, kao i one koje posluju izvan područja EU, ali za svoje poslovanje koriste osobne podatke građana EU zbog nuđenja roba i usluga unutar Unije ili praćenja njihovog ponašanja unutar EU. Važno je napomenuti da je zaštita osobnih podataka podignuta na razinu temeljnih ljudskih prava. Prema Uredbi „*Zaštita pojedinaca s obzirom na obradu osobnih podataka temeljno je pravo. člankom 8. stavkom 1. Povelje Europske unije o temeljnim pravima („Povelja”) te člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije (UFEU) utvrđuje se da svatko ima pravo na zaštitu svojih osobnih podataka.*“⁵⁶ Dok se pod razlozima Uredbe napominje da „*obrada osobnih podataka bi trebala biti osmišljena da bude u službi čovječanstva. Pravo na zaštitu osobnih podataka nije apsolutno*

⁵⁵ Kazneni zakon, čl. 146. st. 1

⁵⁶ Vidi više u Boban, M., Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world, Proceedings of 16th International Scientific Conference ESD 2016., „The legal challenges of modern world, 1-2 (2016), str. 191-201

pravo; Ono se mora razmatrati u vezi s njegovom funkcijom u društvu te ga treba ujednačiti s drugim temeljnim pravima u skladu s načelom proporcionalnosti.⁵⁷ U Uredbi se također navodi poštivanje privatnog i obiteljskog života, što je temelj za razvitak i zaštitu prava na privatnost uz već napomenutu zaštitu osobnih podataka koje se međusobno nadopunjuju.

Članak 2. stavak 2. „*Uredba se ne odnosi na obradu osobnih podataka: tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije, otijekom djelatnosti koja nije obuhvaćena opsegom prava Unije, koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a, koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti, koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.*“⁵⁸

Uredba također definira važne pojmove koje su u skladu s potrebama današnjice. Tako osobni podatak ne uključuje samo uobičajene informacije poput imena i prezimena, već su pridodani i digitalni identifikatori poput mrežnih identifikatora što je nezaobilazno u današnje digitalno doba. U Uredbi, članak 4. stavak 1. osobni podaci su „*svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi ("ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.*“⁵⁹

Što se samog dizajniranja sustava tiče, Privatnost po dizajnu (engl. *Privacy by design*) je postao standard. Time se naglašava da je potrebno paziti na zaštitu podataka od samog početka planiranja i dizajniranja sustava kako bi on bio što zaštićeniji od zlouporaba još u samom nastanku. Potrebno je unaprijed misliti na sve moguće slabe točke sustava i na vrijeme poduzeti sve potrebite mjere za zaštitu osobnih podataka koje se na njima nalaze. Voditelj obrade u tome ima važnu ulogu te bi trebao imati kompetencije provođenja tehničkih i organizacijskih mjera zaštite kako ne bi došlo do kršenja Uredbe a posljedično i sankcija.

5.2.1. Službenici za zaštitu podataka

Uredba donosi nove definicije i dužnosti. Prema članku 4. st. 7. **voditelj obrade** „*fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje*

⁵⁷ Ibid.

⁵⁸ GDPR., čl. 2. st. 2.

⁵⁹ GDPR, čl. 4. st. 1.

samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predviđeti pravom Unije ili pravom države članice“⁶⁰ Dok članak 4. st. 8. definira **izvršitelja obrade** kao „fizičku ili pravnu osobu, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.“⁶¹ Ako ga je prema Uredbi potrebno imenovati, Službenik za zaštitu podataka ima dužnost da informira i savjetuje voditelja i izvršitelja obrade vezano uz njihove obaveze prema Uredbi. Također treba pratiti izvršavanje tih obaveza i surađivati s nadzornim tijelom.⁶²

5.2.2. Privole

Kod prijašnjih slučajeva pristanaka na obradu podataka, bilo je dosta konfuzno i teško saznati na što se točno pristaje te koje su posljedice samog pristanka. Korisnici bi često dobili nerazumljive i jako duge tekstove u kojima je unatoč velikom broju napisanih riječi bilo gotovo nemoguće razaznati ono najvažnije: koji se sve osobni podaci prikupljaju, koliko dugo će se ti podaci čuvati, tko sve ima uvid u te podatke, hoće li se dijeliti dalje trećim stranama, a to su samo neki od mogućih scenarija kršenja prava na privatnost i zlouporabe osobnih podataka što se iskorištavalo i zloupotrebljavalo zbog zakona koji nisu bili u skladu s tadašnjim potrebama. S Uredbom je stavljen veliki naglasak na privole, uz obavezu da svatko tko obrađuje osobne podatke mora strogo definirati svrhu korištenja podataka, koliko dugo se ti podaci čuvaju i tko je sve zadužen za obradu podataka i to sve predstaviti nedvosmisleno, na što razumljiviji i jednostavniji način, što je velika i pozitivna novost. Članak 4. st. 11. Uredbe definira privole kao „svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose“⁶³ Također se predefinirano označavanje svake zasebne privole se više ne računa kao pristanak, već pojedinci trebaju sami označiti svaku pojedinačnu privolu. Kao još jedna velika novost je mogućnost povlačenja privole svakog pojedinca. Iako u jednom trenutku pristanu na obradu, mora im se omogućiti naknadno

⁶⁰ GDPR, čl. 4. st. 7.

⁶¹ GDPR, čl. 4. st. 8.

⁶² Boban, M., Protection of personal data and public and private sector provisions in the implementation of the general EU directive on personal data (GDPR), 27th International Scientific Conference on Economic and Social Development, Rim, Italija, 2018., str. 161-169

⁶³ GDPR, čl. 4. st. 11.

povlačenje ili odbijanje privole. Privola mora biti dokaziva, a teret dokazivanja je na voditelju obrade. Za djecu ispod 16 godina, privolu daju roditelji, iako se na razini svake članice može odrediti niža dobna granica, ali ne ispod 13 godina. Prema Papić (2018) privola kao pravni temelj za obradu osobnih podataka mora biti⁶⁴:

- jasna i afirmativna radnja ispitanika
- nedvosmislena
- u točno određenu svrhu
- razumljiva
- opoziva
- dokaziva

Stoga, privola je ovim jasnije definirana i teže je manipulirati pisanjem bitnih informacija „sitnim slovima“ prilikom davanja privole ili njihovim potpunim izostavljanjem kao što je to dotad bio slučaj. S obzirom da GDPR određuje smjernice i obaveze za sve koji žele biti dio tržišta Europske Unije, sve velike kompanije u što spadaju i društvene mreže, već su trebale poduzeti određene korake kako od 25. svibnja ne bi odmah došlo do kršenja novih zakona uz moguće stroge kazne za sve prekršitelje.

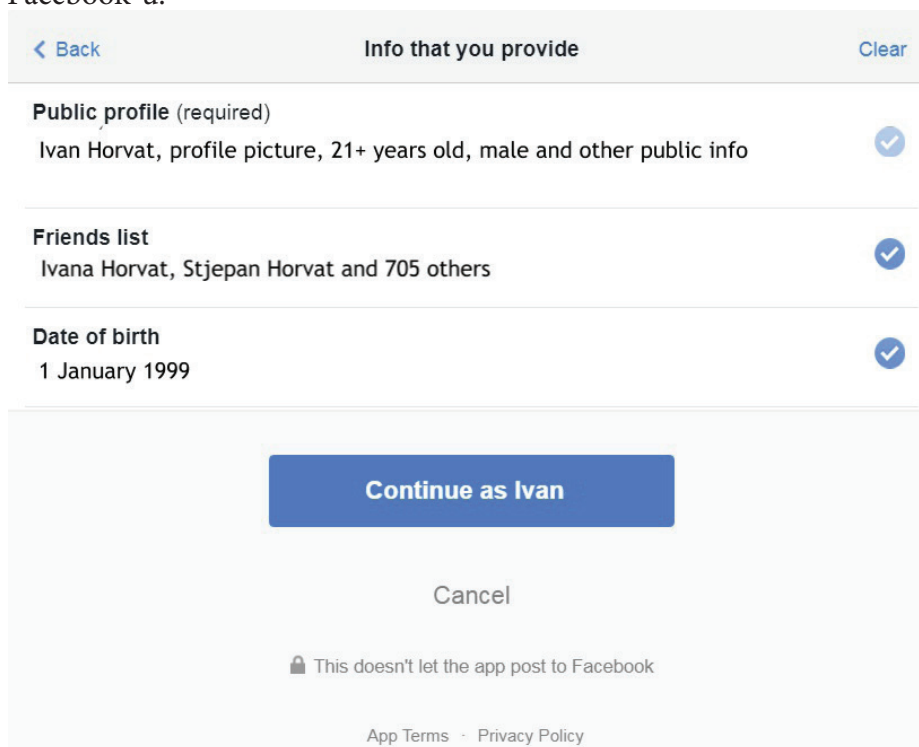
Sam Facebook je već uveo opcije koje su do prije koju godinu bile nezamislive, opcije da korisnici sami odlučuju koje podatke žele dijeliti. Slika 9. prikazuje kako Facebook traži od korisnika uvid u javni profil, popis prijatelja, datum rođenja i email adresu prilikom instaliranja igre Megapolis.



Slika 2. Traženje privola prilikom instaliranja igre Megapolis putem društvene mreže Facebook (Izvor: „screenshot“ - prikaz instalacije igre Megapolis – dostupno na <https://play.google.com/store/apps/details?id=com.socialquantum.acityint&hl=hr&gl=US> [06.02.2021.])

⁶⁴ Papić, P. (2018) Zaštita osobnih podataka – zakonodavni okvir i praksa. URL: http://www.azoo.hr/images/strucni_ispiti_2018/2._3._Petra_Papic_Zastita_osobnih_podataka.pdf [06.02.2021.].

Prije korisnici nisu imali nikakvu mogućnost odlučivanja koji podatak žele podijeliti, a koji ne. Vrijedilo je pravilo „sve ili ništa“. Tko želi igrati igru, morao je ustupiti svoje podatke Facebook-u, a moguće i trećim stranama za ciljano oglašavanje. Tada su korisnici mahom instalirali takve aplikacije ne razmišljajući što se dalje s njihovim podacima dešava. No, uz pomoć zakonskog pritiska na sve koji u sklopu obavljanja svojih dužnosti jesu u doticaju s osobnim podacima, došlo je do promjene. Tako sam Facebook uvodi mogućnost uređivanja privola od strane korisnika, a bez da im se uskrati cjelokupna usluga. Na slici 10. prikazan je popis svih privola za instaliranje igre Megapolis na Facebook-u:



Slika 3. Popis privola korisnika prilikom instaliranja igre Megapolis na Facebook-u
Izvor: „screenshot“ - prikaz instalacije igre Megapolis – dostupno na <https://play.google.com/store/apps/details?id=com.socialquantum.acityint&hl=hr&gl=US>
[06.02.2021.]

Ukoliko korisnik želi, može svaku privolu posebno ukloniti s liste. Popis prijatelja i datum rođenja korisnika nisu obavezni i za njih se mogu izostaviti privole, dok su javni podaci na korisnikovom profilu obavezni ukoliko se želi pristupiti igri.

< Back Info that you provide Reset

Public profile (required)
Ivan Horvat, profile picture, 21+ years old, male and other public info ☒

Friends list
Iva Horvat, Stjepan Horvat and 705 others ☐

Date of birth
1 January 1999 ☐

Slika 4. Uklonjene neobvezne privole za prikupljanje podataka prilikom instaliranja igrice Megapolis na društvenoj mreži Facebook

Izvor: „screenshot“ - prikaz instalacije igre Megapolis – dostupno na <https://play.google.com/store/apps/details?id=com.socialquantum.acityint&hl=hr&gl=US> [06.02.2021.]

Zbog Uredbe su se i velike kompanije morale prilagoditi dajući korisnicima mogućnosti da biraju koje podatke žele podijeliti a koje ne. U ovom slučaju se nije dijelio datum rođenja korisnika i njegov popis prijatelja zbog toga što nisu bili obavezni, čime su neki od neobveznih podataka izostavljeni od dijeljenja s društvenom mrežom Facebook. Takva praksa razrađenijih i jasnijih opcija privola uz više mogućnosti za korisnika se nakon Uredbe sve češće može primjetiti na raznim web stranicama, aplikacijama i servisima.

5.3. Slučajevi kršenja prava na privatnost i zlouporabe osobnih podataka u Europskoj Uniji i svijetu

Najveća novčana kazna od 2,42 milijarde eura je izrečena od strane Europske komisije (EC) gigantu Google-u nakon što je nezakonito davao kao rezultate pretraživanja prednost svojim proizvodima pred proizvodima ostalih kompanija i tako zloupotrijebio svoju dominaciju na tržištu te građanima Unije uskraćivao moguću raznoliku ponudu proizvoda. Čak 90% Google-ove zarade proizlazi od oglašavanja, a putem pretraživača su mogli dobiti dovoljno informacija za ciljano oglašavanje svojih proizvoda i njihovo postavljanje iznad drugih proizvoda. (Europska Komisija, 2017)⁶⁵

⁶⁵ *Europska Komisija* (2017) Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. URL: http://europa.eu/rapid/press-release_IP-17-1784_en.htm [11.02.2021].

U svibnju 2017. Francuska agencija za zaštitu podataka – CNIL (fra. Commission nationale de l'informatique et des libertés) je nakon opsežnog istraživanja koje je uključivalo Belgiju, Njemačku, Nizozemsku i Španjolsku, kaznila Facebook s 150.000 eura zbog grešaka u sprječavanju da korisnički podaci budu dostupni oglašivačima. Kazna bi trebala biti veća s obzirom na tržišnu vrijednost Facebook-a, ali je to bila maksimalna moguća kazna u okviru njihovog tadašnjeg važećeg zakona, uz donošenje vremenskog okvira u kojem Facebook mora prestati pratiti osobe koje nisu njihovi korisnici („non users“) bez njihovog znanja te im je dao zabranu transfera privatnih informacija u Sjedinjene Američke Države. (Kar-Gupta i Rosemain, 2017)⁶⁶

Također u svibnju 2017. Europska komisija (EC) kažnjava Facebook sa 110 milijuna eura novčane kazne zbog obmanjujućih informacija vezanih uz preuzimanje kompanije WhatsApp u 2014. godini. *„Facebook je 2014. obavijestio komisiju da neće biti moguće automatsko spajanje Facebook i WhatsApp profila. No u kolovozu 2016. je došlo do ažuriranja Uvjeta korištenja usluge kao i pravila privatnosti, s mogućnošću njihovog spajanja WhatsApp broja mobitela s Facebook korisničkim profilom i identitetom.“* (Europska Komisija, 2017)⁶⁷

U rujnu 2017. je Španjolska agencija za zaštitu podataka – APED (esp. Agencia Española de Protección de Datos) kaznila Facebook s 1.2 milijuna eura zbog povrede prava privatnosti te korištenja osobnih podataka za ciljano oglašavanje. Agencija je naglasila način na koji Facebook prikuplja podatke o korisnikovim ideologijama, religijskim uvjerenjima i osobnom ukusu te preferencijama bez da je o tome obavijestio korisnike na regularan način, a uz to je također došlo do kršenja zakona jer se ti podaci nisu obrisali nakon što više nisu bili korišteni. Facebook je temeljio svoju obranu na tome da do reklamiranja nije dolazilo zbog navedenog prikupljanja podataka već prema „lajkovima“ korisnika. (Meyer, 2017)⁶⁸

Poseban je slučaj zvan Cambrigde Analytcs koji je pokazao kolika je moć društvenih mreža i medija te koliki mogu biti razmjeri zlouporabe osobnih podataka. Kompanija Cambridge Analytics je osnovana 2013. godine te je bila usmjerena na izbore u Sjedinjenim Američkim Državama. Konzervativac Robert Mercer investira 15 milijuna dolara u kompaniju, koja kasnije sudjeluje

⁶⁶ Gupta-Kar, S; Rosemain, M. (2017) Facebook fined 150,000 euros by French data watchdog. URL: <https://www.reuters.com/article/facebook-france/facebook-fined-150000-euros-by-french-data-watchdog-idUSL2N1I1I00> [11.02.2021]

⁶⁷ Europska Komisija (2017) Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. URL: http://europa.eu/rapid/press-release_IP-17-1369_en.htm [11.02.2021]

⁶⁸ Meyer, D. (2017) Here's Why Facebook Got a \$1.4 Million Privacy Fine in Spain. URL: <https://finance.yahoo.com/news/why-facebook-got-1-4-112358861.html> [12.02.2021].

u predsjedničkoj kampanji trenutnog predsjednika SAD-a Donalda Trumpa. (Rossenberg, Confessore i Cadwalladr, 2018)⁶⁹ Tu kompaniju se optužuje da je od početka 2014. godine nezakonito došla do podataka preko 50 milijuna Facebook korisnika obmanom. Žviždač Christopher Wylie je kao bivši zaposlenik Cambridge Analytics tvrdio da je Facebook znao još od prosinca 2015. da su podaci obrađivani od strane Cambridge Analytics zbog nadolazećih izbora, ali se o tome šutjelo. (Wylie, 2018.)⁷⁰ U svjetskim medijima je ta priča odjeknula i Facebook se našao kao meta optužbi zbog mogućih kršenja ovlasti koje su imali nad osobnim podacima. Mark Zuckerberg tim povodom na svom Facebook profilu objavljuje: „Iako ovo posebno pitanje koje uključuje Cambridge Analytics se ne bi trebalo dogoditi s novim aplikacijama danas, to ne mijenja ono što se dogodilo u prošlosti. Naučit ćemo iz ovog iskustva kako bismo osigurali našu platformu i učinili zajednicu sigurnijom za sve.“⁷¹

U borbi za povjerenje svojih korisnika ali i prilagodbi nadolazećim promjenama u zakonu vezanih uz privatnost korisnika koji stupaju na snagu na razini Europske Unije (Opću uredbu o zaštiti osobnih podataka – GDPR), Facebook uvodi alate koji će korisnicima olakšati informiranje i upravljanje sigurnosnim postavkama svog profila. Uz uvedene „Centra za privatnost“ te 20 000 novih radnih mjesta u domeni sigurnosti i privatnosti do kraja 2018. godine. (Hern, 2018)⁷²

Otkako je 25. svibnja 2018. godine na snagu stupila Opća uredba o zaštiti podataka, odnosno GDPR, u Europskoj uniji, Norveškoj, Islandu i Lihtenštajnu u 2020. godini zabilježeno je preko 160 tisuća slučajeva kršenja ove regulative. Prema najnovijim podacima koje je prikupila i objavila odvjetnička kuća DLA Piper, do sada je, u godinu i pol, na području EU izrečeno kazni u vrijednosti 114 milijuna eura za razne prekršaje vezane uz kršenje GDPR-a. Kad je riječ o podjeli prema zemljama, i broj prijavljenih prekršaja i visine izrečenih kazni značajno variraju. Daleko najviše prekršaja evidentirano je u Nizozemskoj (preko 40.000), Njemačkoj i Ujedinjenom Kraljevstvu, a najviši zbroj novča-

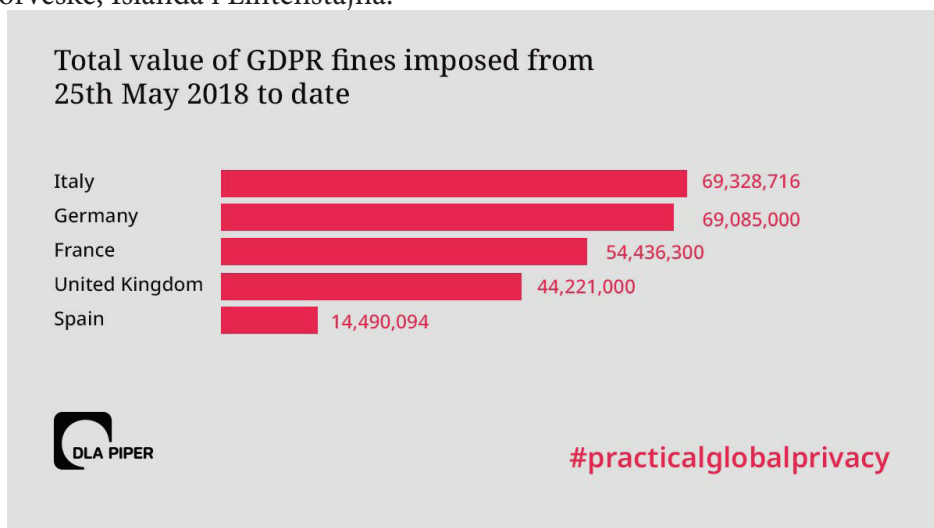
⁶⁹ Rossenberg, M; Confessore, N; Cadwalladr (2018) How Trump Consultants Exploited the Facebook Data of Millions. URL: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [13.02.2021]

⁷⁰ Wylie, C. (2018) Christopher Wylie: Why I broke the Facebook data story – and what should happen now. URL: <https://www.theguardian.com/uk-news/2018/apr/07/christopher-wylie-why-i-broke-the-facebook-data-story-and-what-should-happen-now> [15.02.2021]

⁷¹ Zuckerberg, M. (2018) Facebook.com. URL: <https://www.facebook.com/zuck/posts/10104712037900071> [12.08.2021]

⁷² Hern, A. (2018) Facebook to roll out new tools in response to EU privacy laws. URL: <https://www.theguardian.com/technology/2018/jan/23/facebook-new-privacy-tools-response-to-eu-privacy-laws-sheryl-sandberg> [12.02.2021.]

nih kazni izrečen je u Francuskoj, Njemačkoj i Austriji (51, 24,5 te 18 milijuna eura). Najviša pojedinačna kazna, zbog je je Francuska na vrhu ove liste, jest ona izrečena Googleu u toj zemlji, a iznosila je 50 milijuna eura. Predviđene kazne za kršenje odredbi GDPR-a, bilo nedovoljno dobrom zaštitom podataka, nepravilnim traženjem privola ili curenjem podataka u javnost, mogu iznositi do 10 milijuna eura ili 2% ukupnog godišnjeg prometa kompanije, ovisno o tome koji iznos je veći. Unatoč velikim kaznama prekršaji su sve češći. U razdoblju od svibnja 2018. do veljače 2019. zabilježeno je prosječno 247 prekršaja na dan, a taj je broj u proteklih godinu dana porastao na prosječno 278, što je povećanje od 12,6%.⁷³ Prema najnovijim podacima DLA Piper objavljenim u siječnju 2021. izrečeno je ukupno 272,5 milijuna eura (oko 3332,4 milijuna USD / 245,3 milijuna GBP). Brojka je preuzeta iz najnovijeg godišnjeg zakona o općim propisima o zaštiti podataka (GDPR) odvjetničkog ureda i izvješća o kršenju podataka 27 država članica Europske unije, te Ujedinjenog Kraljevstva, Norveške, Islanda i Lihtenštajna.⁷⁴



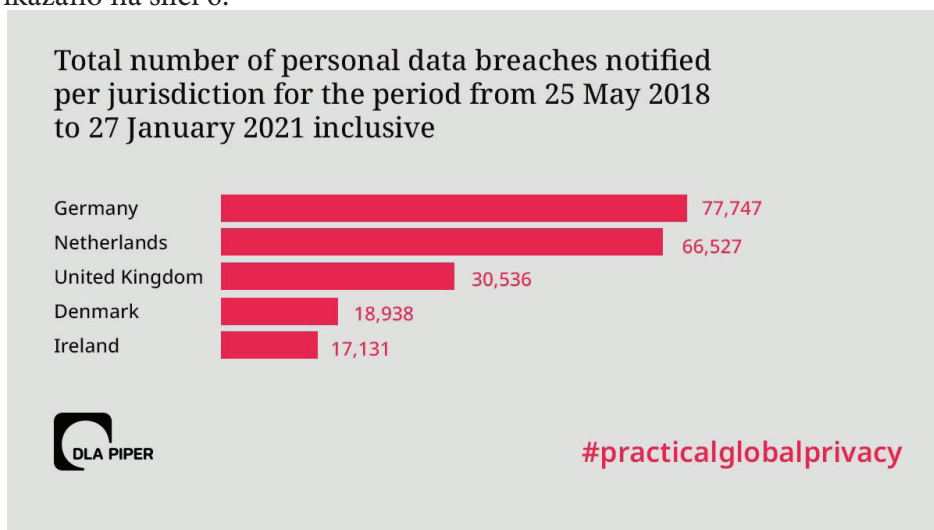
Slika 5. Prikaz ukupnog broja izrečenih kazni za kršenje GDPR-a od početka primjene Uredbe 2018.

Izvor: DLA Piper GDPR fines and data breach survey: January 2021, A report produced by DLA Piper's cybersecurity and data protection team, <https://www.dlapiper.com/en/europe/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/> [12.02.2021].

⁷³

⁷⁴ DLA Piper GDPR fines and data breach survey: January 2021, A report produced by DLA Piper's cybersecurity and data protection team <https://www.dlapiper.com/en/europe/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/> [12.02.2021].

Ukupno je bilo više od 281.000 obavijesti o kršenju podataka od primjene GDPR-a 25. svibnja 2018. s Njemačkom (77.747), Nizozemskom (66.527) i UK-om (30.536) na vrhu tablice broja povreda podataka prijavljenih regulatorima. Francuska i Italija, zemlje s populacijom preko 67 milijuna, odnosno 62 milijuna ljudi, zabilježile su samo 5389 i 3460 obavijesti o kršenju podataka za isto razdoblje koje ilustriraju kulturne razlike u pristupu prijavi kršenja kako je prikazano na slici 6.⁷⁵



Slika 6. Prikaz ukupnog broja izrečenih kazni za kršenje GDPR-a od početka primjene Uredbe 2018.

Izvor: DLA Piper GDPR fines and data breach survey: January 2021, A report produced by DLA Piper's cybersecurity and data protection team, <https://www.dlapiper.com/en/europe/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/> [12.02.2021].

I hrvatska Agencija za zaštitu osobnih podataka je po službenoj dužnosti donosi rješenje i izriče upravne novčane kazne. U priopćenju od 22. veljače 2021. Agencija iznosi kako je doneseno rješenje kojim se zaštitarskom društvu sa sjedištem u Zagrebu (dalje u tekstu: društvo) kao izvršitelju obrade, izriče upravna novčana kazna zbog povrede članka 32. stavka 1. točke b) i d) te stavka 2. i 4. Opće uredbe o zaštiti podataka, točnije zbog nepoduzimanja odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka, što je dovelo do neovlaštene obrade osobnih podataka ispitanika njihovom javnom objavom na društvenim mrežama i u medijima, odnosno do neovlaštenog otkrivanja osobnih podataka ispitanika. Naime, Agenciji za zaštitu osobnih podataka obratio se voditelj obrade, sukladno članku 33. stavku 1. Opće uredbe o zašti-

⁷⁵

Ibidem

ti podataka s prijavom povrede osobnih podataka ispitanika koja je nastala u njihovoj poslovnici, na način da je zaposlenik društva izvršitelja obrade, koje temeljem ugovora obavlja poslove tehničke i fizičke zaštite u poslovnici, snimio mobilnim uređajem snimku videonadzora s nadzornog ekrana te je podijelio s trećom osobom, nakon čega je snimka dospjela na društvene mreže i u medije. Agencija je provela postupak u kojemu je utvrdila da je društvo, zbog nepoduzimanja odgovarajućih tehničkih mjera sigurnosti, omogućilo svojem zaposleniku stvaranje snimke videonadzornog monitora mobilnim uređajem. Tijekom postupka je utvrđeno da izvršitelj obrade nije poduzeo odgovarajuće tehničke mjere sigurnosti, niti prije, a niti nakon incidenta, koje su trebale spriječiti ili svesti rizik iste ili slične povrede na najmanju moguću razinu, zbog čega je Agencija odlučila izreći upravnu novčanu kaznu. Nakon detaljnog razmatranja raspoloživih korektivnih mjera iz članka 58. stavka 2. Opće uredbe o zaštiti podataka te uzimajući u obzir utvrđene okolnosti, kao i da svaka korektivna mjera mora biti učinkovita, proporcionalna i odvraćajuća, Agencija je odlučila izreći upravnu novčanu kaznu. Pri odlučivanju o izricanju upravne novčane kazne, kao i njenom iznosu, Agencija se vodila kriterijima propisanim člankom 83. stavak 2. Opće uredbe o zaštiti podataka. Pritom je utvrđeno da izvršitelj obrade krši obveze o provedbi odgovarajućih tehničkih mjera sigurnosti obrade osobnih podataka više od dvije i pol godine te ono traje i dalje, jer nakon spornog incidenta izvršitelj obrade nije predvidio niti implementirao odgovarajuće tehničke mjere zaštite. Također, obrađivani su osobni podaci jednog ispitanika na način da je snimka dospjela na društvene mreže i u medije te je posljedično ispitanik bio izložen uvredama, podsmjehu i izrugivanju u javnosti, što je moglo prouzročiti određenu nematerijalnu štetu, odnosno utjecati na njegov duševni integritet. Društvo nije poduzelo nikakve radnje kako bi se sporna snimka uklonila s društvenih mreža, odnosno iz medija te je ista ostala javno dostupna. Agencija je kao otegotnu okolnost uzela i činjenicu da izvršitelj obrade nije ispunio svoju zakonsku obvezu obavješćavanja voditelja obrade o predmetnom incidentu kako ga obvezuje članak 33. stavak 2. Opće uredbe, već je očitovanje o istom dostavio voditelju obrade na njihovo traženje nakon zaprimljenog prigovora ispitanika. Također, kao otegotna okolnost je uzeta i činjenica da je osnovna djelatnost društva pružanje fizičke i tehničke zaštite, koje uključuje primjenu i uporabu videonadzora te je društvo jedno od vodećih u Republici Hrvatskoj u navedenoj djelatnosti. Stoga bi društvo kao takvo, trebalo biti relevantni subjekt u davanju mišljenja, smjernica, savjeta i predlagati rješenja voditeljima obrade o uporabi videonadzornog sustava te istovremeno davati primjer svojim radom i pridavati veću pažnju tome od drugih.⁷⁶

⁷⁶ Tekst službenog priopćenja preuzet je sa internetskih stranica Agencije za zaštitu osobnih podataka Republike Hrvatske, dostupno na <https://azop.hr/izdana-nova-upravna-novcana-kazna/> [22.02.2021].

6. METODE ZAŠTITE INFORMACIJSKE SIGURNOSTI I PRAVA NA PRIVATNOST

Kako bi se moglo predviđati, prepoznavati i reagirati na nepravilnosti, kršenja postojećih prava te dopunjavati postojeće i stvarati nove zakone kad trenutni pokažu neadekvatnim za rješavanje svih postojećih situacija, potrebno je djelovati na više razina. Pojedinaac ima pravni okvir koji mu omogućuje da reagira na svako nezakonito kršenje njegovih prava, a također postoje metode za napredak tih prava. Još jedno od prava pojedinca je pravo na pritužbu nadzornom tijelu zbog moguće zlouporabe podataka. Prema čl. 51. st. 1. Uredbe „svaka država članica osigurava da je jedno ili više neovisnih tijela javne vlasti odgovorno za praćenje primjene ove Uredbe kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar Unije (*“nadzorno tijelo”*).“⁷⁷ U Republici Hrvatskoj tu dužnost obavlja Agencija za zaštitu osobnih podataka (u daljnjem tekstu „Agencija“). Agencija je „pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o provedbi Opće uredbe o zaštiti podataka („Narodne novine“, broj 42/18) kojim se osigurava provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. 04. 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka (Opće uredbe o zaštiti podataka)“⁷⁸ Statut joj je odobren 2004. godine otkad kreće s radom. S obzirom na složenost problematike zaštite osobnih podataka, Agencija ima širok spektar zaduženja i nadležnosti. Neke od najbitnijih su nadgledanje i reagiranje u slučaju nepravilnosti i zlouporabe prilikom prikupljanja osobnih podataka te sukladno s procjenom Agencije moguće je predlaganje pokretanja prekršajnog ili kaznenog postupka. Savjetuje napredak u načinu organizacije i tehničkim mjerama zaštite osobnih podataka i nadgleda ga, također uz pozornost na informacijsku sigurnost. (Agencija, s.a.)⁷⁹

S obzirom na Opću uredbu o zaštiti osobnih podataka te općenitoj razini znanja o ovoj problematici, u slučaju ikakve nedoumice preporučuje se poslati upit direktno Agenciji i tako izbjeći moguće probleme koji mogu dovesti do prekršajnih i kaznenih prijava, financijske štete, na kraju krajeva i diskreditiranja te općeg nepovjerenja prema danoj firmi, ustanovi ili nekoj drugoj pravnoj osobi koja kroz svoj posao dolazi u doticaj s osobnim podacima, kao i privatnoj osobi koja zloupotrijebi tuđe osobne podatke. Nakon donošene Europske kon-

⁷⁷ GDPR, čl. 51. st. 1.

⁷⁸ Agencija za zaštitu osobnih podataka (2021.) O AZOP-u, Djelokrug, URL: <https://azop.hr/djelokrug/> [23.02.2021.]

⁷⁹ AZOP, Ibid.

vencije o ljudskim pravima 1950. godine pokazalo se potrebnim osnovati i sud koji bi ta prava štitio. Europski sud za ljudska prava (engl. European Court of Human Rights – ECHR) osnovan je 1959. godine, a djelovao je paralelno s Europskom komisijom za ljudska prava, a nakon njenog gašenja preuzima vodeću funkciju borbi za zaštitu ljudskih prava u Europi. Sjedište mu je u Strasbourgu u Francuskoj. Broj sudaca je trenutno 47 što je jednako broju država članica Vijeća Europe koji se biraju na 9 godina. Sud prima otprilike 50.000 zaprimljenih zahtjeva godišnje. (Europski sud za ljudska prava, s.a.)⁸⁰

Zahtjev će biti dopušten ako su ispunjeni uvjeti

- Iscrpljena sva domaća pravna sredstva
- Rok od šest mjeseci od donošenja konačne odluke domaćeg suda
- Prigovor se temelji na povredi Konvencije
- Pretrpljena značajna šteta počinitelja.⁸¹

Također, i edukacija predstavlja ključni element u zaštiti informacijske sigurnosti i prava na privatnost, Edukacija građana kao cjeloživotni proces, koji nikad ne bi trebao prestati u ovom polju bi trebao biti dostupan svim građanima. Posebna pozornost bi se trebala obratiti na djecu koja pristupaju mreži ali nisu u stanju razumjeti i percipirati sve moguće prijetnje na koje mogu pritom naići. Poželjno je da obitelji, odgajatelji te skrbnici približe djeci načine na koje se trebaju zaštititi na internetu jednako kao što ih uče i o ostalim prijetnjama na koje mogu naići u „stvarnom životu“. Zatim mladi, koji mogu također biti aktivni sudionici društva, kao i politički aktivni zbog čega je bitno i dalje provoditi edukacije kroz odgojno-obrazovni sustav, bilo kao gostujuća predavanja MUP-a, djelatnika Agencije za zaštitu osobnih podataka, fakultetskih profesora iz tog znanstvenog područja i ostalih adekvatnih predavača ili u sklopu programa koji će biti uvršten u osnovne i srednje škole kao obavezan predmet, kao i njihovom kombinacijom. Ne treba zanemariti ni moć medija preko kojih bi se mogle takve informacije učiniti još vidljivima i dostupnima velikom broju građana i bez da napuste svoje domove. Kroz edukacije i program unaprjeđenja školskih kurikuluma povećao bi se utjecaj na mlade da steknu znanja o demokratskom društvu uz sve njegove vrednote kao što su sloboda, tolerancija, nenasilje, uvažavanje različitosti, međusobno razumijevanje i suradnja uz mnoge druge. Poticalo bi ih se da izražavaju svoje stavove, da kritički razmišljaju, da su svjesni svojih ljudskih prava i da znaju što se treba napraviti u slučaju njihovog kršenja.

⁸⁰ Ured zastupnika Republike Hrvatske pred Europskim sudom za ljudska prava (2021.) Europski sud za ljudska prava. URL: <https://uredzastupnika.gov.hr/o-uredu/europski-sud-za-ljudska-prava-186/186> [15.2.2021].

⁸¹ Ibid.

ZAKLJUČAK

Pravo na zaštitu osobnih podataka jedno je od temeljnih prava svakog čovjeka. Svrha informacijske sigurnosti i zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Također, pravo na zaštitu osobnih podataka je pravo zaštite legitimnih interesa građanina (pojedince) koje se odnosi na sprječavanje i sankcioniranje zlouporaba osobnih podataka, a zajamčeno je međunarodnim i nacionalnim propisima. Općom uredbom o zaštiti podataka, koja se izravno primjenjuje u Republici Hrvatskoj i svim državama članicama Europske unije od 25. svibnja 2018. godine, moderniziran je regulatorni okvir kako bi išao u korak s brzim razvojem tehnologije i postao učinkovit u današnje digitalno doba, a ujedno i ojačao povjerenje pojedinaca u elektroničke usluge i jedinstveno digitalno tržište. Zakonom o provedbi Opće uredbe o zaštiti podataka koji je stupio na snagu 25. svibnja 2018. osigurava se provedba Opće uredbe o zaštiti podataka. Donošenje GDPR-a prvenstveno predstavlja ključni pravni okvir kojim je Europska unija odlučila je zaštititi privatnost svojih građana i povećati kontrolu nad obradom osobnih podataka građana uz uvođenje zakonske obveze procjene učinka na zaštitu podataka. Također, ova Uredba dodatno donosi i stroža pravila obrade posebnih kategorija podataka te se samim time uistinu očekuje potreba edukacije i usklađivanja s Uredbom. Kako je i prikazano u radu, prekršiteljima se izriču kazne kojima se regulira provođenje i primjena Uredbe. Propisana je gornja granica sankcija i upravnih novčanih kazni te je prepušteno nacionalnim zakonodavstvima da reguliraju same sankcije. U današnjem digitalnom i dominantnom informacijsko-komunikacijskom dobu uz Internet koji omogućava prijenos informacija na globalnoj razini, upravo informacijska sigurnost ima neizmjerljivo važnu ulogu. Osobni podaci pojedinaca obrađuju se svakodnevno u tijelima javne vlasti, organizacijama i ostalim pravnim osobama te se mogu zloupotrijebiti. Nove informacijsko-komunikacijske tehnologije i pristup internetu, omogućavaju nove rizike i kršenja prava na privatnost te je stoga od ključne važnosti bila upravo provedena reforma pravnog okvira zaštite osobnih podataka koja zakonom uvodi i uvjetuje provođenje mjere informacijske sigurnosti. U radu su istaknute i društvene mreže kao jedan od najvećih prijenosnika informacija današnjice. Prikupljajući osobne podatke korisnika i prateći njihove aktivnosti mogu profilirati korisnike te vršiti ciljano oglašavanje ili prosljeđivati njihove osobne podatke trećim stranama bez dopuštenja, dok pojedinci mogu sami ugroziti svoju sigurnost i privatnost zbog nedovoljne osviještenosti ili nemara. Također, uz aktualni zakonodavni okvir i zaštitu od aktualnih prijetnje infor-

macijskoj sigurnosti i pravu na privatnost važno je naglasiti i potrebu edukacije građana i povećanje razine osviještenosti građana o načinima zaštite osobnih podataka. Upravo edukacija građana uz provođenje aktualnog pravnog okvira zaštite osobnih podataka predstavlja pravi put zaštite privatnosti (prevencije) te samim time smanjenja kršenja prava na privatnost i zlouporabe osobnih podataka s naglaskom na provođenje metoda zaštite informacijske sigurnosti u virtualnom okruženju.

INFORMATION SECURITY AND PROTECTION OF THE RIGHT TO PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

SUMMARY

In today's digital and dominant age of information and communication technologies and the Internet, which enables the transfer of information on a global level, information security plays an extremely important role. Personal data are processed on a daily basis in public authorities, organizations and other legal entities and they can be misused. By using technological devices for communication and Internet access, each user leaves virtual traces that can be illegally processed and through which the user can uniquely identify and violate his right to privacy as well as laws containing personal data and information security measures. Social networks are one of the biggest transmitters of information today. By collecting users' personal information and tracking their activities, they may profile users and target advertising or pass on their personal information to third parties without permission, while individuals may compromise their security and privacy due to lack of awareness or negligence. In this paper, the authors, in addition to presenting threats to information security and the right to privacy, emphasize the display of different awareness of citizens related to information security and privacy rights, as well as previous violations of these rights and misuse of personal data, virtual environment.

Keywords: *social networks, information security, personal data, privacy, technology, virtual world, protection*