Privatnost i prostor slobode kroz primjenu GDPR-a na prostoru Republike Hrvatske

Perišić, Matej

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:122:753346

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-16**

Repository / Repozitorij:

University North Digital Repository

Sveučilište Sjever

Završni rad br. 286/PIM/2021

Privatnost i prostor slobode kroz primjenu GDPR-a na prostoru Republike Hrvatske

Matej Perišić, matični broj studenta

0052/2012

rujan 2021. godine

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL Odjel za ekonomiju

STUDIJ preddiplomski stru ni studij Poslovanje i menadžment u medijima

PRISTUPNIK Matej Perišić | MATIČNI BROJ 0052/2012

DATUM 05.09.2021. | KOLEGIJ Poslovna i medijska etika

NASLOV RADA Privatnost i prostor slobode kroz primjenu GDPR-a na prostoru Republike Hrvatske

NASLOV RADA NA ENGL. JEZIKU Privacy and space of freedom through the application of the GDPR in territory of the Republic of Croatia

MENTOR Sead Alić | ZVANJE prof. dr. sc.

ČLANOVI POVJERENSTVA

1. doc.dr.sc. Mirko Smoljić , predsj.
2. doc.dr.sc. Ana Globočnik Žunac, lan
3. prof. dr. Sead Alić , mentor
4. Livija Pavletić , pred., zamj. lan
5.

Zadatak završnog rada

BROJ 286/PIM/2021

OPIS

Definirati pojam privatnosti i valorizirati različite pristupe razumijevanju tog fenomena
Detektirati ključne oblike privatnosti relevantne za društvenu i ekonomsku sferu
Analizirati utjecaj suvremenih tehnika na promjene odnosa prema privatnosti
Posebno analizirati utjecaje suvremenih masmedija i društvenih mreža na fenomen privatnosti
Definirati pozicije AZOP-a u hrvatskom društvu
Predstaviti važnost, obveze i zahtjeve GDPR-a
Komparirati provođenje zaštite i povreda osobnih podataka u Hrvatskoj i u EU
Testirati teze na anketnom istraživanju
U zaključku definirati smjernice razvoja fenomena privatnosti u budućim društvima

ZADATAK URUČEN 13. 9. 2021 | POTPIS MENTORA

SVEUČILIŠTE SJEVER

Sveučilište
Sjever

Odjel za ekonomiju, i menadžment u medijima

Završni rad br. 286/PIM/2021

Privatnost i prostor slobode kroz primjenu GDPR-a na prostoru Republike Hrvatske

Student

Matej Perišić, matični broj
0052/2012

Mentor

Prof. dr. sc. Sead Alić

Koprivnica, lipanj 2021. godine

Predgovor

Na početku ovog završnog rada želio bih zahvaliti svojem mentoru, izv. prof. dr. sc. Seadu Aliću, što je pristao mentorirati me i što mi je pomogao brojnim savjetima i u ovome radu i na kolegijima za vrijeme studija.

Isto bih volio zahvaliti svim profesorima Sveučilišta Sjever s kojima sam uspješno surađivao za cijelo vrijeme trajanja mojeg studiranja i što su me naučili struci, ali i mnogim stvarima iz života.

Za kraj, zahvaljujem svojoj obitelji, rodbini i prijateljima, koji su me podržavali kroz sve ove godine studiranja.

Sažetak

U ovom radu detaljno se analizira pojam privatnosti, stoga će se prvi dio rada odnositi na definicije najznačajnih autora te na njezin procesni model.

U drugom dijelu rada razmatrat će se kako je razvoj tehnologije utjecao na privatnost.

Treći dio rada temelji se na utjecaju medija na privatnost, kakva je njihova veza, koje su medijske odgovornosti i što je pojam invazije na privatnost.

Predzadnji dio rada tiče se zakonske zaštite privatnosti u obliku Opće uredbe o zaštiti osobnih podataka. Obradit će se njezine obveze i zahtjevi, krovna agencija koja djeluje na teritoriju Republike Hrvatske, što u slučaju da dođe do povrede osobnih podataka i koje sankcije slijede prekršitelje te naposlijetku, što ona sama znači za građane Europske unije.

Zadnji dio rada bit će posvećen kvantitativnom istraživanju u obliku ankete.

Ključne riječi: privatnost, etika, pravo, model procesa privatnosti, tehnologija, mediji, medijska odgovornost, invazija na privatnost, GDPR, AZOP, povreda privatnosti, pseudonimizacija

Summary

This paper analyses the notion of privacy in detail, therefore the first part of the paper pertains to its definitions by the most prominent authors, as well as its process model.

The second part of the paper will elaborate on the effect the development of technology has had on privacy.

The third section of this paper concerns the influence of the media on privacy, the relationship between the two, media responsibility and the concept of invasion of privacy.

The penultimate part of the paper deals with the legal protection of privacy in the form of the General Data Protection Regulation. This section will discuss the obligations and the requirements of the Regulation, the umbrella agency operating on the territory of the Republic of Croatia, the consequences of personal data violation as well as the sanctions applicable to violators and, lastly, what the Regulation itself means for the citizens of the European Union.

The last part of the paper will be dedicated to quantitative research in the form of a survey.

Keywords: privacy, ethics, law, privacy process model, technology, media, media responsibility, invasion of privacy, GDPR, AZOP, privacy violation, pseudonymisation

Popis korištenih kratica

AZOP Agencija za zaštitu osobnih podataka
DPO Data Protection Officer (Voditelj obrade podataka)
ENISA European Union Agency for Cybersecurity (Agencija Europske unije za kibersigurnost)
EU Europska unija
EUROJUST European Union Agency for Criminal Justice Cooperation (Agencija Europske unije za suradnju u kaznenom pravosuđu)
EUROPOL European Union Agency for Law Enforcement Cooperation (Agencija Europske unije za suradnju u provođenju zakona)
GDPR General Data Protection Regulation (Opća uredba o zaštiti osobnih podataka)
HVIS Hrvatski vizni informacijski sustav
IT informacijske tehnologije
PPM The Privacy Process Model (Model procesa privatnosti)
RH Republika Hrvatska
SIS II Schengen Information System (Schengenski informacijski sustav)

Sadržaj

1. Uvod

Privatnost je kroz povijest percipirana na različite načine. Jedan autor je kritizirao drugoga, njega je kritizirao netko treći, slažući se s onim prvim i tako su nastale mnogobrojne teorije koje su polako oblikovale ljudska stajališta, ali i zakone koji su pokušali zaštititi pojedinčevu privatnost. Stoga možemo reći kako privatnost čini širok raspon interesa i za etiku i za pravo. Svatko od nas definira privatnost na svoj način, što je u potpunosti u redu, jer prave definicije zapravo nema. Kultura, norme i tradicija oblikovale su privatnost s etičke strane, dok su političke, društvene i gospodarske promjene mijenjale pravna stajališta, odnosno zakone. Tako je pravo u početku prepoznavalo i štitilo samo fizičko miješanje u tuđi život i imovinu, a tek kasnije čovjekova unutarnja stanja i duhovnost. Pravo na slobodu dobilo je u potpunosti nova značenja – čovjek je odlučio njegovati privilegije koje je stekao u društvu i zaista uživati u svome životu. Prvotno fizičko vlasništvo više nije bilo samo fizički opipljivo, tu je sada uključeno i ono nematerijalno, što ima puno dublju vrijednost i značenje.

Dakle, privatnost ima više oblika i može ju se rasporediti na fizičku, društvenu, psihološku i informacijsku. Može se reći da je jedan oblik gradio drugi. Fizička privatnost odnosi se na nas same i na našu imovinu. I mi i naša imovina se nalazimo u nekoj državi, u nekom društvu i sami odlučujemo s kime ćemo se družiti te u kojoj mjeri. Svaki pojedinac zasebno je potpuno drugačiji, stoga sam odlučuje kome će, što će, kako i kada reći. To je oblikovalo psihološku i informacijsku privatnost. Upravo je informacijska privatnost ona koja se najduže razvijala i još uvijek je u nekom stadiju razvitka.

Ovaj rad, osim što detaljno analizira privatnost, teorije o njoj, model procesa kroz koji se oblikuje, analizira i njen razvoj kroz tehnologiju i medije, a naposlijetku dolazi do krovnog zakona koji ju štiti u Europskoj uniji, ali i šire. Važnost tehnologije i njezinog napretka pri definiranju privatnosti skoro je stopostotno ovisna o internetu koji pomaže različitim poslovnim djelatnostima, olakšavajaći i pojednostavljujući različite poslovne procese, digitalizirajući javne zapise, sačinjavajući kategorizirane baze podataka za privatne, ali i državne tvrtke. Takvi podaci nerijetko postaju meta onih koji ih zloupotrebljavaju, stoga je velika potreba da ih zakoni maksimalno zaštite. Etičari zbog toga imaju mnogo posla, pa oblikuju stavove je li nešto vrijedno i moralno saznanja očiju javnosti. Mediji tu igraju veliku ulogu, jer znatiželjnici žele saznati baš sve, ne misleći pri tome kako je to nečiji stvarni život i da ta osoba možda ne želi da drugi o njoj znaju toliko ili uopće išta.

Upravo iz ovih razloga proizlazili su mnogi zakoni, a 25. svibnja 2018. godine na području svih članica Europske unije primjenjuje se Opća uredba o zaštiti osobnih podataka (u daljnjem tekstu: GDPR). Zemlje članice Europske unije (u daljnjem tekstu: EU) morale su prilagoditi

svoje već postojeće zakone ovoj uredbi, stoga je njeno tumačenje još uvijek vrlo kompleksno i stvara mnogo problema i pojedincima i tvrtkama.

2. Privatnost i prostor slobode

Privatnost je temeljno pravo i važna etička norma, bitna za autonomiju i zaštitu ljudskog dostojanstva te služi kao temelj na kojemu počivaju mnoga druga ljudska prava. Privatnost nam omogućuje stvaranje granica i upravljanje prostorom slobode kako bismo se zaštitili od neopravdanog miješanja u naše živote, te nam omogućuje da pravilno definiramo tko smo i kako želimo komunicirati sa svijetom koji nas okružuje. Privatnost nam pomaže uspostaviti granice kako bismo ograničili tko ima pristup našim tijelima, mjestima i stvarima, kao i našoj komunikaciji i našim osobnim podacima.

U ubrzanoj svakodnevnici globalnog sela pravila koja štite privatnost daju nam mogućnost da ostvarimo svoja prava suočeni sa značajnom neravnotežom moći. Zbog toga je privatnost bitan način na koji nastojimo zaštititi sebe i društvo od neopravdane upotrebe moći. Omogućuje nam prostor da budemo sami bez osude, slobodno razmišljanje bez diskriminacije i važan je element koji nam daje kontrolu nad pitanjima: Tko sve zna te što zna o nama?

Dok si postavljamo pitanje zašto je privatnost važna, odgovor pronalazimo u modernom društvu koji razmatranje privatnosti definira raspravom o suvremenim slobodama.

Tehnologija je oduvijek bila isprepletena s pravom na privatnost. Uzimajući za primjer naše sposobnosti zaštite privatnosti, koje su danas veće nego ikad prije, mogućnosti nadzora iste su relativne. Internet, mediji i društvene mreže lako iskrivljavaju percepciju vrijednosti poimanja privatnosti kao etičkog prava svakog pojedinca.

Danas možemo na jednostavan način identificirati pojedince usred masovnih skupova podataka i tijekova informacija, te jednako tako donositi odluke o pojedinim osobama na temelju širokog raspona podataka. Uz svu današnju tehnologiju vrlo lako je moguće otkriti sva mjesta koja smo posjetili, sve kupovne transakcije koje smo proveli, sve razgovore koje smo vodili, što čini filtracijski sustav između tržišta i krajnjeg konzumenta. Ove mogućnosti, koje nam je tehnologija omogućila, mogu dovesti do krajnje negativnih posljedica na pojedince, potrošačke skupine, pa čak i na društvo, jer kritiziraju, isključuju i diskriminiraju te u konačnici narušavanju privatnost i sužavaju prostor slobode. Trenutno najznačajniji izazov privatnosti je taj da se svatko može vrlo lako ugroziti bez da je toga svjestan.[1]

Važnost privatnosti ističe autor Marx u svojih 10 točaka:

[1] https://media.privacyinternational.org/w/7zVySBTDcJUpe3YqoAZK1x, dostupno 15.07.2021.

I. Sposobnost kontrole širenja informacija o sebi povezana je s dostojanstvom svakog pojedinca, samopoštovanjem i osobnošću, a samoprezentacija i naše ponašanje ovise uvelike o takvoj vrsti kontrole.

II. Anonimnost može biti društveno korisna jer potiče iskrenost, poduzimanje rizika, eksperimentiranje i kreativnost kod svakog pojedinca.

III. Povjerljivost poboljšava komunikacijske tokove i od vitalnog je značaja za povjerenje u profesionalce poput liječnika, odvjetnika i sl. te za povjerenje u različita korporativna okruženja.

IV. Privatnost je resurs u međuljudskim odnosima, a dodjeljuje se i razmjenjuje ovisno o napretku odnosa. Intimnost se temelji na dobrovoljnom dijeljenju osobnih podataka s drugima. Pojedinci se bolje osjećaju u svojoj koži kako upoznaju druge ljude te na taj način stječu samopouzdanje.

V. Kontrola informacija je strateški resurs u neosobnim odnosima. Primjer toga su poslovne tajne i autorska prava.

VI. Granice među grupama ljudi kontroliraju tko zna koliko, odnosno tko je unutra ili vani, a djelomično su temeljene na organizacijskim pozicijama koje ograničavaju tko ima čemu pristup čemu te koliko zna o tome.

VII. Privatnost omogućava ostvarenje „američkog sna“ dajući pojedincu svjež početak.

VIII. Poštenje se može zaštititi odbijanjem pristupa davanju informacija koje bi se mogle zlouporabiti.

IX. Privatnost pomaže u osami i miru svakog pojedinca, neophodnih za mentalno zdravlje i kreativnost u dinamičnom društvu.

X. Postoji širi simbol načela koja štite privatnost. Takva načela su najčešće na razini države, koja su narodu potrebna za vlastitu vitalnost i individualnost, a pruža im prava da kontroliraju informacije o sebi.[2]

2.1. Paradigma privatnosti

Privatnost kao pojam veže se uz pojmove privatna sfera i privatni život što u konačnici izražava pravni i etički koncept prema kojem svaka osoba može svoje određene aktivnosti, te uz njih vezane stvari, misli i osjećaje zadržati za sebe, to jest ne dozvoliti da druge osobe,

[2] G. T. Marx: Privacy and Techonology, Telektronikk, br. 1/96, 1996., str. 42

organizacije, društvo ili javnost saznaju. Privatnost kao uobičajan pojam današnjice razvijen je na bazi zapadnog svijeta, koji utječe već određeno vrijeme, dok je u mnogim kuturama taj pojam donedavno bio potpuna nepoznanica. Shvaćanje privatnosti dijeli se u nekoliko koncepata, što čini privatnost kao fizičku vrijednost i informacijsku vrijednost.

Pod značenjem fizičke vrijednosti privatnost podrazumjeva zadržavanje privatnosti tijela, odnosa i stvari od pogleda javnosti. Informacijska privatnost pojedinca svodi se na privatnost podataka vezanu uz zdravstveno stanje, političko opredjeljenje, financijsko stanje, lokalitet na kojem pojedinac obitava te obiteljski status.[3]

Univerzalna definicija privatnosti ne postoji, stoga svaki od mnogobrojnih teoretičara objašnjava istu ovisno iz kojeg ju kuta proučava. Tako neki autori razgraničavaju pojam privatnosti u četiri ili pet grubo podjeljenih kategorija.

2.1.1. Prva kategorija definiranja privatnosti: privatnost kao mjesto

Prva kategorija proizlazi iz feminističke kritike privatnosti, a obuhvaća pojam „mjesta“ pod definiciju privatnosti. Kako se mjesto veže uz dom, a kroz povijest je ženski spol vezan isključivo za domaćinstvo i odgoj djece kod kuće, dok je za muški spol bio rezerviran poslovni i politički svijet, određene feministice kasnije oštro kritiziraju takvo stajalište. No, neke od njih ne vide ništa loše u takvoj kategorizaciji, stoga opravdavaju takvo stajalište argumentom kako je posjedovanje prostornih i materijalnih aspekata vrijednosti privatnosti pozitivno, obzirom da je i ženama i muškarcima podjednako važno i vrijedno imati svoj dom.[4]

2.1.2. Druga kategorija definiranja privatnosti: privatnost kao pravo biti ostavljen na miru

Druga kategorija privatnosti zauzima pravno stajalište te se prvi puta definira kao „pravo biti ostavljen na miru“ autora Warrena i Brandeisa s kraja 19. stoljeća. Izraz je nastao kao potreba za stvaranjem zakona koji bi definirao privatnost i štitio pojedinca, obzirom da su u medijima sve češće počeli izlaziti različiti članci s detaljima iz privatnih života, popularizirao se „žuti tisak“, a

[3] A. D. Moore, Defining Privacy: Journal of Social Philosophy, br. 3/39, 2008., str. 411-412

[4] A. Pavuna: Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova, Doktorska disertacija, Fakultet političkih znanosti, Zagreb, 2019., str. 13

nerijetko su izlazile i fotografije kojima su se dotični pojedinci protivili. Mediji su već tada počeli prelaziti očite granice pristojnosti, a informacije su postale sredstvo trgovine. Na taj način je ljudski rod uvidio što znači duševna bol i koliko je veća od fizičke boli, obzirom da šteti ugledu i časti pojedinca. Autori navode kako svaki trač proporcionalno s njegovim optjecajem rezultira snižavanjem društvenih standarda i morala.[5]

2.1.3. Treća kategorija definiranja privatnosti: privatnost kao ograničen pristup osobi

Upravo treća kategorija privatnosti proizlazi iz druge, definirajući je kao „ograničen pristup osobi". Autorica Gavison objašnjava ovaj izraz osvrćući se na privatnost u tri konteksta. Prvi navodi kako moramo imati neutralan pristup privatnosti kako bismo utvrdili je li ona zapravo narušena. Drugi kontekst navodi kako privatnost mora imati koherentnost kao vrijednost. Treći kontekst kaže da privatnost mora biti koristan koncept u pravnom smislu, tj. koncept koji omogućuje identifikaciju onih prilika koje zahtijevaju pravnu zaštitu. Autorica nadalje navodi da je naš interes za privatnošću povezan s našom zabrinutošću zbog pristupačnosti drugima, tj. u kojoj smo mjeri poznati drugima, koliki i kakav fizički pristup drugi ljudi imaju prema nama i u kojoj smo mjeri predmet pažnje drugih. Ovakav koncept privatnosti predstavlja brigu za ograničenu pristupačnost te omogućuje da identificiramo kada dolazi do njezinog gubitka. U sugestivnom smislu, privatnost je ograničenje pristupa drugima, a kao metodološko polazište autorica navodi kako pojedinac uživa u savršenoj privatnosti kada je u potpunosti nedostupan drugima. Savršena privatnost ima tri komponente: nitko nema nikakve informacije o pojedincu, nitko ne obraća pozornost na pojedinca i nitko nema fizički pristup pojedincu. No, savršena privatnost je u bilo kojem društvu neizvediva te iz toga proizlazi koncept gubitka privatnosti.[6]

2.1.4. Četvrta kategorija definiranja privatnosti: privatnost kao kontrola pristupa

Četvrta kategorija privatnosti je zapravo najviše puta komentirana od strane mnogobrojnih autora, a ona podrazumijeva „kontrolu pristupa". Kontrola pristupa odnosi se na kontrolu nad

[5] L. D. Brandeis, S. D. Warren: The Right to Privacy, Harvard Law Review, br. 5/4, prosinac 1890.

[6] R. Gavison: Privacy and the Limits of Law, The Yale Law Journal, br. 3/89, siječanj 1890., str. 423-429

informacijama o sebi, na kontrolu nad sferom intimnosti, na kontrolu nad pristupom osobi ili kombinaciji istih. Obzirom na golemu različitost među ljudima (jesu li introverti ili ekstroverti, kakve su im navike, stajališta, iz koje kulture potječu i sl.) privatnost je mogućnost svakog pojedinca da sam sebi odredi kome, kako, koliko i kada će prezentirati sebe i dati informacije o sebi drugima. Stoga se čovjek svakodnevno prilagođava okolini i samosvjesno određuje koliko će i tko znati o njemu. Ovakvo stajalište zauzima autor Westin, dok ga s druge strane opovrgava kritičar Parent koji tvrdi kako se čovjek odriče svoje privatnosti kada dijeli informacije o sebi s drugima. On također smatra kako je sve što je objavljeno u javnim zapisima, različitim dokumentima pa i medijima dio javne, a ne privatne sfere, stoga se takve dokumentirane informacije ne smatraju kao ugroza privatnosti. Dakako, i autor Parent je imao kritičare koji su komentirali njegova stajališta, a najoštriji je bio Moore koji zauzima stajalište da osoba izlaskom u javnost odaje o sebi fizičke podatke (spol, dob, izgled i sl.) stoga npr. u svojem domu među obitelji pojedinac dijeli informacije o sebi, a da se pritom ne odriče vlastite privatnosti.[7]

2.1.5 Peta kategorija definiranja privatnosti: privatnost kao višedimenzionalna stanja

Peta kategorija definira privatnost kao „višedimenzionalnu“, a ima četiri stanja – samoću, intimnost, anonimnost te zadršku. Prema Westinu, samoća i intimnost podrazumijevaju slobodu od promatranja drugih, a glavna razlika je u tome je li pojedinac sam ili unutar manje grupe ljudi. Anonimnost pojedincu omogućuje nedostupnost u smislu pažnje, dok zadrška predstavlja slobodu od otkrivanja podataka o sebi drugima.[8]

Privatnost slično objašnjava i autorica Gavison koja tvrdi kako je savršena privatnost definirana kada je pojedinac u potpunosti nedostupan drugima te upozorava na tri stanja nedostupnosti – tajnost, anonimnost i samoću. Tajnost predstavlja nedostupnost u smislu znanja, anonimnost u smislu nedostupnosti pažnje, a samoću u smislu fizičke nedostupnosti.[9] Glavna razlika između tumačenja pojma anonimnosti je u tome da autorica Gavison smatra kako kršenje anonimnosti uključuje na skretanje pozornosti na pojedinca, a postojanje predmetom pozornosti

[7] A. Pavuna: Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova, Doktorska disertacija, Fakultet političkih znanosti, Zagreb, 2019., str. 14-16

[8] L. M. Austin, Re-reading Westin: Theoretical Inquiries in Law, br. 53/20, 2019., str. 56

[9] R. Gavison: Privacy and the Limits of Law, The Yale Law Journal, br. 3/89, siječanj 1890., str. 428-429

uključuje gubitak privatnosti, dok Westin objašnjava pojam anonimnosti kroz Simmelov primjer „fenomena stranca“ koji kaže da, iako stranac nije u pojedinčevom životu, niti će možda ikada biti, on može ponuditi objektivne odgovore na postavljena pitanja pojedinca, bez da nad njim izvršava autoritet ili ga na neki način ograničava.[10]

Autorica Burgoon predlaže četiri međusobno povezane dimenzije privatnosti – fizičku, interakcijsku, psihološku i informacijsku privatnost. Fizička dimenzija omogućuje pojedincu da regulira stupanj nadzora i fizički pristup osobnom prostoru. Interakcijska dimenzija podrazumijeva autonomno uključivanje ili povlačenje iz društvenih susreta. Psihološka dimenzija uključuje sposobnost pojedinca da spriječi uplitanje u svoje spoznaje i osjećaje. Informacijska privatnost omogućuje pojedincu da kontrolira prikupljanje i širenje informacija o sebi.[11]

Svi ovi autori složili su se u jednoj stvari – privatnost je teško, gotovo nemoguće, univerzalno definirati. Ona zauzima veoma važno mjesto u javnosti i o njoj se raspravlja iz različitih kuteva gledišta. O njoj se filozofira, pokušava ju se regulirati zakonima, na nju se gleda kroz psiho-socijalni aspekt, ali i kao na tehnikaliju. Sljedeće poglavlje odnosi se na procesni model privatnosti kojega je donio suvremeni autor Dienlin nakon proučavanje gore navedenih autora i nekih drugih kojih se ovaj rad ne dotiče.

2.2. Model procesa privatnosti – PPM

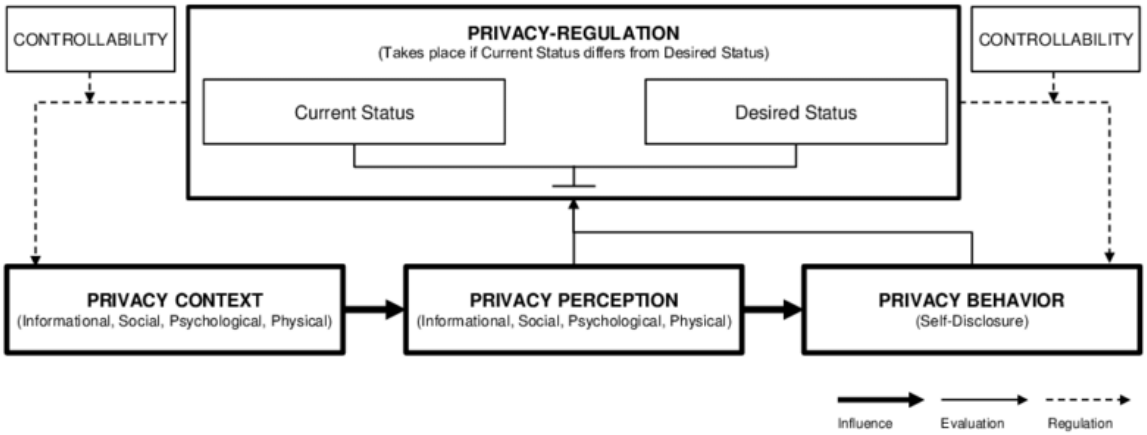
Model procesa privatnosti (u daljnjem tekstu: PPM), ili izvorno *The Privacy Process Model*, autora Tobiasa Dienlina, nastao je temeljem analize postojeće literature o privatnosti. PPM analizira zasebne uvjete, mehanizme i propise o privatnosti.

Kreće se od identifikacije objektivnog konteksta privatnosti. On se dijeli na informacijsku, društvenu, psihološku i fizičku dimenziju. Nakon toga se ispituje subjektivna percepcija privatnosti koja se također dijeli na navedene dimenzije. U konačnici se promatra ponašanje vezano uz privatnost, tj. koliko se ljudi otkrivaju pred drugima. Ukoliko se percepcija privatnosti ili ponašanje privatnosti razlikuje od poželjnog statusa, ljudi će utoliko pokušati promijeniti kontekst privatnosti ili samo ponašanje.

[10] L. M. Austin, Re-reading Westin: Theoretical Inquiries in Law, br. 53/20, 2019., str. 60

[11] J. K. Burgoon, Privacy and Communication: Annals of the International Communication Association, br. 6, siječanj 1982., str. 206-243

Na Slici 1. vizualno je prikazan shematski prikaz PPM-a.



Slika 1. Model procesa privatnosti

Dakle, autor Dienlin osvrće se na definiciju privatnosti autora Westina te sugerira kako je privatnost objektivan uvjet, gdje se pojedinac nalazi u nekom društvu ili je sam. Stupanj privatnosti bi stoga trebao biti objektivno mjerljiv. U takvoj definiciji je sadržan prvi faktor PPM-a koji se naziva „kontekst privatnosti“.

U kontekstu informacijske privatnosti mjeri se količina prikupljanja informacija koja se odvija u danom trenutku. Pitanja koja si možemo postaviti su: „Koristi li se trenutno video nadzor u ovoj situaciji?“ ili „Vodi li netko bilješke o meni?“

Kontekst društvene privatnosti se odnosi na broj prisutnih osoba u prostoriji. Što je manje ljudi prisutno, a koji se međusobno upoznaju, kontekst društvene privatnosti postaje viši.

Kontekst psihološke privatnosti u ovom slučaju je uzeta kao mjera do koje se prisutni pojedinci uključuju u razgovoru, koji može biti intiman, tj. veoma osoban, ali i sasvim trivijalan i usputan. Iz toga zaključujemo da, što je pojedinac otvoreniji i iznosi više intimnih detalja iz svojeg života, to je kontekst psihološke privatnosti viši, odnosno ukoliko je razgovor usputan i priča se o vremenskoj prognozi, utoliko je kontekst psihološke privatnosti niži.

Kontekst fizičke privatnosti tiče se opsega blizine drugih ljudi. Postavljamo si pitanja „Koliko smo bliski s drugim ljudima?“. Sva četiri konteksta su međusobno neovisna te se razlikuju jedni među drugima.

Drugi faktor PPM-a je subjektivna percepcija privatnosti koja se može opisati i ocijeniti na objektivan način. I ovaj faktor ima svoja četiri konteksta, odnosno dimenzije.

Prva dimenzija je informacijska privatnost koju ljudi percipiraju tako da se u javnosti osjećaju anonimno i nezapaženo. No, jesu li oni zaista nezapaženi? Obratimo pozornost na najbanalniji primjer nadzornih kamera koje se nalaze svugdje oko nas - na ulicama, različitim

ustanovama, *shopping* centrima ili hotelima. Narušavaju li one našu privatnost ili nas štite? Ako nas netko snima na javnom mjestu, za takvo što treba biti jasno i krupno izložena obavijest o tome.

Druga dimenzija privatnosti je ona društvena. Njezin primjer se najbolje ogleda na društvenoj mreži *Facebook*, gdje ljudi na svojim vremenskim crtama objavljuju različite stvari iz svojega života, pritom misleći da to vide samo njihovi prijatelji, a njihove objave zapravo vidi puno više ljudi. Iz ovoga proizlazi zaključak da percepcija ljudi o njihovoj društvenoj privatnosti nadilazi stvarni kontekst društvene privatnosti, obzirom da nije moguće pronaći pravu razinu samootkrivanja.

Treća dimenzija psihološke privatnosti također se može kvalitetno sagledati iz kuta društvene mreže *Facebook*. Ljudi se sve više povode jedni drugima te dijele mnogo privatnih podataka na svojim vremenskim crtama. Iz ovoga se može zaključiti kako ljudi precjenjuju količinu i intimnost informacija.

Fizičku dimenziju privatnosti ljudi procjenjuju na različite načine, ovisno o npr. kulturi iz koje dolaze. Tako netko pri razgovoru doživljava fizički kontakt, npr. dodir za ruku u znak podrške, kao normalnu stvar, dok bi se u nekoj drugoj kulturi to moglo shvatiti kao ometanje njihove fizičke privatnosti.

Opet je važno naglasiti kako su sve četiri dimenzije zasebno za sebe gledane, jer se u mnogočemu razlikuju, ali iz njih svakako proizlazi pitanje: „Kako privatnost utječe na ljudsko ponašanje?“, što je ujedno i treći faktor PPM-a.

Što zapravo znači ponašanje u vezi s privatnošću? To je svako ponašanje koje uključuje radnje samootkrivanja. Ako se ljudi nalaze u grupi bliskih ljudi, skloniji su otkrivati više intimnih podataka o sebi. Zaključujemo kako se ljudi najbolje otkrivaju jedni pred drugima kada se nalaze među sebi bliskim osobama, odnosno njihov stupanj percepcije privatnosti je visok.

Za percepciju privatnosti, kao i za ponašanje u vezi s privatnošću, ljudi opažaju trenutni status privatnosti koji uspoređuju sa željenim statusom privatnosti. Ako postoji razlika između trenutnog statusa i željenog statusa, ljudi se automatski uključuju u proces regulacije privatnosti. U procesu regulacije, ljudi ili mijenjaju kontekst privatnosti ili samo ponašanje. Kako bi se mogla provesti regulacija privatnosti, mogućnost kontrole konteksta privatnosti ili ponašanja

privatnosti mora biti zajamčena. Što više ljudi kontrolira svoj kontekst privatnosti i ponašanje u vezi s privatnošću, to se više prilagođavaju situaciji. [12]

Uzmimo za primjer ovu situaciju: čovjek sjeda za stol večerati sa svojom suprugom i sinom. Obzirom da je njegov najstariji sin trenutno odsutan, stolica pored mlađeg sina je prazna. Zbog sinove fizičke odsutnosti, percepcija fizičke privatnosti je povećana. Budući da čovjek trenutno želi dijeliti bliske trenutke sa svojom prisutnom obitelji, njegova željena percepcija fizičke privatnosti je niska. Možda odluči promijeniti kontekst privatnosti – neće sjesti na mjesto za stolom na kojemu inače sjedi, nego će sjesti na mjesto svojeg najstarijeg sina, kako bi se približio mlađem sinu i supruzi. Na taj način regulira privatnost smanjujući kontekst fizičke privatnosti.

U sljedećoj situaciji čovjek i njegova supruga sjede sami za stolom. On želi razgovarati o vrlo napornom danu na poslu i zbog čega se osjeća loše, pa je njegova željena razina za samootkrivanjem visoka. Ipak primjećuje kako on i supruga cijelu večer razgovaraju o trivijalnim stvarima. Stoga, mijenja temu u željenu, pa počinje govoriti o svojim emocijama i danu na poslu. Na taj način je promijenio svoje ponašanje u vezi s privatnošću povećavajući razinu samootkrivanja.[13]

Za zaključiti je kako glavni okvir PPM-a čine dimenzije konteksta privatnosti, elementi percepcije privatnosti i ponašanje u vezi s privatnošću, dok mehanizam regulacije privatnosti i kontrola iste ga u konačnici zaokružuju. Slika 1. jednostavno se tumači na sljedeći način: svaki pojedinac ima vlastitu percepciju privatnosti, jer se nalazi u određenom kontekstu privatnosti. Ljudi otkrivaju onoliko o sebi ovisno o tome koju razinu privatnosti osjećaju, tj. koliko su slobodni otkriti o sebi, a to ovisi o broju osoba s kojima se trenutno nalaze, odnosu u kojemu su s tim ljudima i sl., stoga se taj dio naziva ponašanje u vezi s privatnošću. Naravno, tijekom razgovora pojedinci reguliraju i kontroliraju kontekste privatnosti, stoga su to dinamičke odrednice PPM-a.

[12] S. Garnett, S. Halft, M. Herz, J. M. Mönig: Media and Privacy, Stutz, Passau, 2014., str. 105-122

[13] T. Dienlin: The psychology of privacy: Analyzing processes of media use and interpersonal communication, Doktorski rad, University of Hohenheim, Hohenheim, str. 35-36

3. Privatnost i tehnologija

Tehnološki napredak stvorio je veliku napetost između prava na privatnost i detaljnog prikupljanja podataka, na kojemu se temelji digitalizacija. Umjetna inteligencija omogućila je ne samo prikupljanje, nego i prepoznavanje te grupiranje mase podataka prikupljene jeftinim oblicima pohrane podataka. Nove tehnologije za prikupljanje osobnih informacija nadilaze tradicionalne metode prikupljanja informacija. Moć državnih, ali i privatnih tvrtki, koje manipuliraju prikupljanje podataka i informacija na temelju nepotpunih zakona ili samih okolnosti sve više raste. Prikupljanje informacija odvija se nevidljivo, automatski i na daljinu, a ugrađeno je u rutinske aktivnosti.

Ljudi sve češće zaboravljaju koliko su praćeni te olako shvaćaju podatke koje iznose o sebi na internetu. Stoga, važno je istaknuti tri perspektive prava na privatnost koja bi nas trebala podsjetiti na stvarnu važnost vlastite privatnosti i anonimnosti.

Prva perspektiva privatnosti u digitalnom svijetu predstavlja ideju da samostalno odlučujemo tko, kada i kako može koristiti naše osobne podatke. Primjerice, preuzimajući bilo koju aplikaciju na naš pametni telefon, neposredno nakon instalacije dobivamo obavijest o tome kako aplikacija prikuplja naše osobne podatke te traži od nas pristanak za to. Jako malo ljudi zaista čita uvjete koje nam aplikacija postavlja, stoga većina pristaje na njih, bez obzira kolika je ozbiljnost onoga što u njima piše. Ovaj opći problem, pri čemu poslovni subjekti koriste velike količine privatnih podataka, a da za to nisu dobili stvarnu suglasnost, ukazuje na korištenje naših osobnih podataka u različite svrhe, od kojih su neke vrijedne, dok druge predstavljaju ozbiljnu prijetnju društvu.

Druga perspektiva se osvrće na pravo biti ostavljen na miru. Započnimo od činjenice da su naši pametni telefoni postali toliko „pametni“ da se otključavaju, umjesto četveroznamenkastim pin-om, otiskom našeg prsta ili očitavajući crte našeg lica. Takvi tzv. humanizirani uređaji stvaraju privid toga da je u prostoriji s nama još jedna osoba, da nismo zapravo sami, čime pravo da budemo ostavljeni sami dobiva potpuno novo značenje.

Treća perspektiva prava na privatnost je fenomen poznat pod nazivom „zamka autonomije“. Ovaj fenomen se odnosi na informacije o emocionalnim sklonostima pojedinca, seksualnoj orijentaciji pojedinca, njegovim nesigurnostima, strahovima, tjeskobama i sl. Prikupljanjem takvih podataka, marketinški stručnjaci oblikuju reklame „samo za vas“, a mi istima dopuštamo da odlučuju o tome što ćemo jesti ili gdje ćemo kupovati. Internet osobni asistenti uče o nama, a mi im nesvjesno otkrivamo svoje interese, s kim se družimo ili kako se osjećamo danas, kako bi nam oni zatim poslali poruku, nazvali nas ili nam jednostavno oglasili putem interneta što

možemo naručiti ili rezervirati za sebe. Sve ovo dovodi do nepovjerenja potrošača, jer oni s vremenom postaju svjesni da se njihovim izborima manipulira.[14]

Javno prihvaćena načela određuju što se sve zapravo smije koristiti od osobnih podataka prikupljenima od strane informacijskih tehnologija, a razjašnjavaju vrijednosti i prava koje pojedinci imaju. Za primjer, još 1973. godine donešen je Kodeks pravičnosti informacijskih praksi za američko Ministarstvo zdravstva, obrazovanja i socijalne skrbi, koje se odrazilo na europske standarde zaštite podataka.

Kodeks pravičnosti informacijskih praksi
1. Ne smije postojati tajno prikupljanje podataka.
2. Osoba ima pravo saznanja na podatke iz evidencije i u koje su svrhu korištene.
3. Podaci dobiveni za jednu evidenciju ne smiju se koristiti u drugoj evidenciji za druge svrhe bez pristanka osobe.
4. Osoba ima pravo ispraviti ili izmijeniti podatke o sebi.
5. Bilo koja organizacija koja stvara, održava ili koristi baze o osobnim podacima mora osigurati pouzdanost podataka za njihovu namjeravanu upotrebu te moraju poduzeti mjere opreza kako bi spriječile zlouporabe osobnih podataka.

Tablica 1. Kodeks pravičnosti informacijskih praksi

Tako su dalje nastala ostala načela, poput načela minimiziranja prema kojem se prikupljeni i obrađeni podaci ne smiju čuvati, niti dalje koristiti, osim ako je to bitno iz razloga koji su unaprijed navedeni radi potpore privatnosti podataka[15] ; načela obnove koji kaže da oni koji mijenjaju status quo privatnosti trebaju snositi odgovornost zbog izmjena; načelo sigurnosne mreže ili jednakosti koje kaže kako svatko ima pravo na minimalni prag privatnosti; načelo pravovremenosti koje iziskuje ažurnost podataka, a zastarjele informacije trebaju biti uništene; načelo zajedničkog vlasništva nad transakcijskim podacima koje nalaže objema strankama koje

[14] https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANGe4anGvggpEzq3aCd1eUa_DdFWyPpVkKwGV4vFhe50KEQxgoqnY3JEGnMIQ0khZM0t5O6Yd9P1pLuPoqrQ2VJCel-bFSGX6g_ZI7AT8TgCgAt8Db_A3hNcTSTOWPj8eewpKfy0cDQHnyVroIbFF3ahMvban7-uBja4xvtdGyS0, dostupno 22.07.2021.

[15] https://www.experian.co.uk/business/glossary/data-minimisation/, dostupno 22.07.2021.

kreiraju transakciju pristanak na svaku kasniju uporabu podataka; i načelo odštete za one koji su podložni narušavanju privatnosti, kako bi bili otkriveni i dobili nadoknadu kršenja podataka.[16]

Što se tiče društvenih znanosti, komunikacijske tehnologije uvrštene su u kategoriju ekonomske i formalne racionalnosti. Max Weber zabrinjavao se pretežno oko racionalizacijskih procesa u ekonomiji, vladavini i zakonodavstvu, nikad ne analizirajući ulogu tehnologije kao sredstva izrazite moći u racionalizaciji društva. Unatoč tome što je bio svjestan tehnoloških previranja i transformacijskih moći industrijskih strojeva, tehnologiju je kategorizirao kao namjernu racionalnost u kapitalističkoj ekonomiji. Nakon njega su mnogobrojni autori analizirali tehnološku racionalnost kao društvenu i kulturalnu činjenicu. Kako su tehnološki posredovane prakse međusobno povezane sa društveno-tehnološkim sustavima te kako se one stabiliziraju u datom vremenu, razvile su digitalnu racionalizaciju ekonomije, rastuće medijske i uslužne industrije tzv. „postindustrijskog društva“ te distanciranje socijalnih sustava tzv. „stručnih sustava“ koji su težili postati informacijskim sustavima. Informacijski sustavi društveno se reproduciraju namjernom i nenamjernom cirkulacijom informacija i komunikacije, a gledajući iz šireg kuta, predstavljaju društvenu činjenicu koja može potrajati dulje od svojih članova.[17]

Rastuće neprijateljstvo prema tehnološkim divovima uzrokuje pomak koji se može osjetiti u cijeloj industriji. Fenomen pod nazivom „*techlash*“ je snažna i raširena negativna reakcija na rastuću moć i utjecaj velikih tehnoloških tvrtki, osobito onih sa sjedištem u Silicijskoj dolini. *Techlash* proizlazi i od potrošača koji gube povjerenje u tehnološke divove, ali i od vlada koje zamjeraju sve veću moć koju ove tvrtke posjeduju.[18]

[16] G. T. Marx: Privacy and Techonology, Telektronikk, br. 1, svezak 96, 1996., str. 45-46

[17] Ibid., str. 59

[18] https://www.balticapprenticeships.com/blog/what-is-techlash-and-what-does-it-mean-for-the-digital-industry, dostupno 23.07.2021.

4. Privatnost i mediji

U ovom se radu do sada gledalo i opisivalo privatnost iz različitih uglova, prolazeći kroz povijest i prateći njezin razvoj. Što se društvo više globaliziralo i digitaliziralo, stvorilo se mnoštvo novih pitanja na koja imamo nepotpune ili nejasne odgovore. U prethodnom poglavlju osvrnuo sam se na odraz tehnologije na privatnost. Obzirom da je tehnologija postala na neki način dio nas – kupujemo, učimo, radimo, pratimo novosti, družimo se putem interneta, bilo preko računala, laptopa, tableta ili mobitela – poželjno je obratiti pozornost koliko kome odajemo o sebi i na koji način uopće funkcioniramo u stvarnosti u odnosu na „život na internetu“. Taj problem samootkrivanja imaju gotovo svi, no zamislite još da ste i poznata javna ličnost. Političari, ugledni odvjetnici, filmske zvijezde ili popularni pjevači se svakodnevno susreću s novinarima i fotografima koji prate svaki njihov korak. Koliko je to moralno i etički, je li to stvarno vrijedno novinskog članka i nečije pažnje, osvrnut ću se u ovom dijelu rada.

4.1. Razvoj medija i utjecaj na privatnost

Nekada su ljudi svakodnevno kupovali novine i pratili dnevne vijesti preko radija ili televizora. Danas su novine digitalizirane u internet portale ili različite profile na društvenim mrežama poput *Facebooka* i *Instagrama*, a vijesti gledamo češće preko *YouTubea* nego na televizijskim ekranima. Na internetu možemo pronaći apsolutno svaku kategoriju vijesti koju poželimo: politika, ekonomija i gospodarstvo, poljoprivreda, kriminal, crna kronika, životni stil, umjetnost, kultura itd. Vijesti možemo pratiti onako kako mi to želimo, biramo teme koje nas zanimaju, a izbjegavamo ono što nas ne zanima.

Teme o kojima se u novinama pisalo nekad također se razlikuju od današnjih. Krajem 18. i početkom 19. stoljeća samo su obrazovani čitali novine. Tridesetih godina 19. stoljeća, pojavom masovnog obrazovanja, povećao se i broj novinskih čitatelja. Razvijaju se masmediji u najurbanijim krajevima, što otvara put oglašivačima koji svoju priliku zasigurno nisu propustili, povećavajući potrošnju svojih proizvoda i povećavajući vlastitu zaradu. Novine postaju novi bijeg od stvarnosti, pa se i sadržaj sve više tome prilagođavao. Sada se teme proširuju, a život prosječnog građanina počinje se spominjati u medijima. Takvo senzacionalističko novinarstvo pokazalo se loše po određene pojedince, pa su ljudi obratili pozornost na svoju privatnost kao moralno pravo. „Ta situacija postavila je moralnu dilemu kulturi koja vrednuje i privatnost i slobodu štampe: dok štampa brani narušavanje privatnosti informativnom vrijednošću, njeni kritičari pokušavaju da nametnu odgovornost u javnosti za ono što smatraju neetičkim kršenjem

novinske pristojnosti. U okviru takvog okruženja pravo na privatnost postalo je pravni, ali istovremeno i moralni koncept.“[19]

4.2. Paradoks veze medija i privatnosti

Mediji i privatnost imaju dugu, tešku i paradoksalnu vezu. Dobro novinarstvo otkriva zloupotrebu moći vodećih državnika i vlada, financijske prevare, tajne ugovore i afere za koje ljudi na pozicijama ne žele da javnost sazna. Gledajući s te strane, novinarstvo postoji da bi održalo obećanje demokracije, da se ljudima pruže relevantni i transparentni podaci o tome kako moćne institucije funkcioniraju. Iako novinari često otkrivaju naše tajne, pa se zato smatra da vole kršiti privatnost, oni ipak ovise o njoj. Razlog tomu su izvori informacija koji su povjerljivi. U praktičnom smislu, ovo znači da ne postoji autoritet ili sud koji bi omogućio novinaru da otkrije identitet anonimne osobe. Novinari si zato postavljaju pitanje je li neka tema od javnog interesa i što javnost zanima, a glavna razlika je što javnost treba znati i što javnost želi znati.

Javne osobe i javni prostor primjer su paradoksalnosti medija i privatnosti. Naime, brojni *paparazzi* fotografi uhode slavne osobe, pa su na taj način izgubile pravo na privatnost, obzirom da su postale meta tisuća ili milijuna znatiželjnika diljem svijeta. Javne osobe zbog svoje osobnosti i poslova, koje su istaknuli u javnosti, odnosno, tražili su publicitet za njih te našli put ka popularnosti, su samim time pristali pristali na njegove uvjete. Mediji imaju profesionalno pravo informiranja javnosti o pitanjima od javnog interesa, pa su tako poznati izgubili pravo prigovora.[20] S etičke strane gledišta, jasno je da je zona privatnosti javnih osoba uža od one običnih ljudi, no „to ne znači da oni moraju žrtvovati svu privatnost i predati svu autonomiju nad svojim ličnim životom.“[21] Novinari argumentiraju kako poznate osobe baš zbog svojeg publiciteta nisu iskrene i zapravo žele da se o njima piše, što i je opravdano, ali tanka je linija između legitimnog članka i nepodobnog upada u tuđu privatnost.

[19] L.A. Day: Etika u medijima, Klub PLUS, Beograd, str. 161

[20] A. McStay: Privacy and the media, SAGE Publications Ltd., London, 2017., str. 25-30

[21] L.A. Day: Etika u medijima, Klub PLUS, Beograd, str. 144

4.3. Medijska odgovornost

Medijska odgovornost prema javnosti ima prednost nad bilo kojom drugom odgovornošću. Novinarstvo je profesija koja zahtijeva vrijeme, resurse i sredstva kako bi se njome bavilo, a to je sve bitno za njezinu neovisnost.

Opća deklaracija o ljudskim pravima u članku 19. navodi smjernice ponašanja novinara u istraživanju, uređivanju, prijenosu, širenju i komentiranju vijesti i informacija, te u opisu događaja, u svim medijima.

1. Prva dužnost novinara je poštivanje činjenica i prava javnosti na istinu.

2. U skladu s ovom dužnošću, novinar će u svakom trenutku braniti načela slobode u poštenom prikupljanju i objavljivanju vijesti te prava na pošten komentar i kritiku. Pobrinut će se da jasno razlikuje činjenične podatke od komentara i kritika.

3. Novinar će izvještavati samo u skladu s činjenicama za koje zna podrijetlo. Novinar ne smije potiskivati bitne informacije niti krivotvoriti bilo koji dokument. Pažljivo će reproducirati vjerodostojne izjave i druge materijale koje osobe koje nisu javne objavljuju na društvenim medijima.

4. Novinar će koristiti samo poštene metode za dobivanje informacija, fotografija, dokumenata i podataka te će uvijek prijaviti svoj status novinara i suzdržati se od korištenja skrivenih snimaka slika i zvukova, osim ako je nemoguće prikupljati podatke koji su izrazito u javnom interesu. Tražit će slobodan pristup svim izvorima informacija i pravo da slobodno istražuje sve činjenice od javnog interesa.

5. Pojam hitnosti ili neposrednosti u širenju informacija neće imati prednost nad provjerom činjenica, izvora i/ili ponudom odgovora.

6. Novinar će učiniti sve kako bi ispravio pogreške ili objavljene informacije za koje se utvrdi da su netočne na pravodoban, eksplicitan, potpun i transparentan način.

7. Novinar mora čuvati profesionalnu tajnu u vezi s izvorom informacija dobivenih u povjerenju.

8. Novinar će poštivati privatnost. On će poštivati dostojanstvo imenovanih i/ili zastupanih osoba te obavijestiti ispitanika je li razgovor i drugi materijal namijenjen objavljivanju. On/ona će pokazati posebnu pažnju neiskusnim i ranjivim sugovornicima.

9. Novinari će osigurati da širenje informacija ili mišljenja ne doprinosi mržnji ili predrasudama i učinit će sve da spriječe širenje diskriminacije na temelju zemljopisnog, društvenog ili etničkog podrijetla, rase, spola, spolne orijentacije, jezika, religije, invaliditeta, političkih i drugih mišljenja.

10. Novinara će se smatrati ozbiljnim profesionalnim prekršiteljem u slučaju da učini nešto od sljedećeg: plagijat, iskrivljavanje činjenica, klevetu, neutemeljene optužbe.

11. Novinar će se suzdržati od djelovanja kao pomoćnik policije ili drugih sigurnosnih službi. Od njega će se tražiti samo da dostavi podatke koji su već objavljeni u medijima.

12. Novinar će pokazati solidarnost sa svojim kolegama, ne odričući se slobode istrage, dužnosti informiranja i prava na kritiku, komentare, satiru i uredničkI izbor.

13. Novinar neće koristiti slobodu tiska za služenje drugim interesima i neće se suzdržati od primanja bilo kakve nepravedne prednosti ili osobne koristi zbog širenja ili nerasprostiranja informacija. On/ona će izbjeći ili prekinuti svaku situaciju koja bi ga mogla dovesti do sukoba interesa u obavljanju svoje profesije. Izbjeći će zabunu između svojih aktivnosti i aktivnosti oglašavanja ili propagande. On/ona će se suzdržati od bilo kakvog oblika *insajderske* trgovine i tržišne manipulacije.

14. Novinar neće poduzimati nikakve aktivnosti ili angažmane koji bi mogli ugroziti njegovu neovisnost. On/ona će poštovati metode prikupljanja/širenja informacija koje je slobodno prihvatio, pod uvjetom da su obveze jasne i neupitne.

15. Novinari vrijedni imena smatrat će svojom dužnošću vjerno poštivati gore navedena načela. Ne smiju se prisiljavati na obavljanje profesionalnog čina ili na izražavanje mišljenja koje je protivno njegovom/njezinom profesionalnom uvjerenju ili savjesti.

16. U okviru općeg zakona svake zemlje, novinar će u pitanjima profesionalne časti priznati nadležnost neovisnih samoregulativnih tijela otvorenih za javnost, isključujući svaku vrstu uplitanja vlada ili drugih.[22]

4.4. Invazija na privatnost

Autor Prosser privatnost razdvaja na četiri delikta. Invazija, odnosno fizičko ili drugačije upadanje u tuđu samoću na vrlo uvredljiv način predstavlja prvi delikt. Drugi delikt se odnosi na objavljivanje vrlo uvredljivih privatnih podataka o nekome u javnosti. Treći delikt naziva se lažno svjetlo i pod njim se podrazumijeva objavljivanje lažnog i uvredljivog dojma o nekome. Prisvajanje je četvrti delikt koji predstavlja korištenje tuđeg imena ili neke sličnosti u korist nečega, bez pristanka onog drugog.[23]

[22] https://www.ifj.org/who/rules-and-policy/global-charter-of-ethics-for-journalists.html, dostupno 30.07.2021.

[23] W. L. Prosser, Privacy: California Law Review, br. 3/48, kolovoz 1960., str. 389

Prosser prvi i drugi delikt povezuje sa slobodom od mentalnih tegoba obzirom da iznenađujuće invazije na privatnost mogu dovesti do cijelog niza negativnih osjećaja, poput anksioznosti, depresije i sl. Treći delikt poistovjećuje sa zabrinutošću zbog vlastitog ugleda, jer se čovjek uvijek nastoji prikazati u što boljem svjetlu, pa lažne informacije, klevete i tračevi mogu loše odraziti na cjelokupnu sliku o nekome. Prosser privatnost smatra izvedenim etičkim i pravnim načelima, što znači da je nastala iz nekog od prethodnih postojećih prava (npr. sloboda, vlasništvo, kleveta i sl.). S druge strane, možda je privatnost krovna kategorija navedenih prava, pa kad osjećamo da je naša privatnost povrijeđena jer je netko nešto sramotno objavio o nama, iz toga proizlaze mnoge emocije poput iziritiranosti, bijesa ili potrebe za osvetom.[24]

Autor Rusbridger predložio je pet točki po kojima se tumači invazija na privatnost od strane medija:

I. mora postojati dovoljan razlog uz prethodnu procjenu štete za pojedince i obitelj,
II. integritet motiva i opravdanje da će uslijediti javno dobro,
III. metode trebaju biti proporcionalne priči i stupnju javnog interesa, dok invazija treba biti svedena na minimum,
IV. invaziju bi trebalo nadzirati nadležno tijelo,
V. moraju postojati dobri temelji priče kako bi uspjela.[25]

On smatra kako je budućnost privatnosti komplicirana. Za početak, niti trenutno ju ne možemo točno definirati, stoga prvi scenarij predviđa kako se neće mnogo toga promijeniti. Elitne novine i znanstvenici mogu zauvijek govoriti o implikacijama ljudskih prava i prijetećoj moći kompjutorskih algoritama, ali duh privatnosti se nikada neće vratiti u svoju bocu. Drugi je scenarij da će doći do neke vrste *techlasa*, pri čemu će potrošači sve više mijenjati svoje postavke privatnosti - i stvarne i metaforične. Treći scenarij mogao bi vidjeti postupnu promjenu ponašanja pri ulasku novih igrača na tržište, zajedno s novim tehnologijama koje omogućuju bolje upravljanje osobnim podacima.

Konačni scenarij je regulacija. Europa je prednjačila s GDPR-om. Ranije se pretpostavljalo da će SAD polako ići ovim putem, ali bilo je beznačajno pa je u siječnju 2020. uveden Kalifornijski zakon o zaštiti potrošača koji označava značajnu promjenu u načinu na koji se zapadna obala nalazi. Naš stvarni gubitak privatnosti datira prije 2019. godine, ali to je bila

[24] A. McStay: Privacy and the media, SAGE Publications Ltd., London, 2017., str. 34

[25] Ibid., str. 33

godina kada smo pokazali naivnost u pogledu razmjera gubitka. Kao i uvijek u digitalnom svijetu, budućnost je nespoznatljiva. Možemo nastaviti kao da se ništa nije dogodilo ili bi se sve moglo poremetiti u tren oka. "Konkurenti koji se usklade sa stvarnim potrebama ljudi i normama tržišne demokracije, vjerojatno će privući gotovo svaku osobu na Zemlji kao svog kupca." [26]

[26] https://www.theguardian.com/commentisfree/2020/feb/02/will-we-just-accept-our-loss-of-privacy-or-has-the-techlash-already-begun, dostupno 01.08.2021.

5. GDPR- Opća uredba o zaštiti osobnih podataka

Pravo na privatnost dio je Europske konvencije o ljudskim pravima iz 1950. godine koja kaže da „svatko ima pravo na poštivanje svog privatnog i obiteljskog života, doma i dopisivanja[27]“. Na temelju toga, Europska unija nastojala je zakonom osigurati zaštitu ovog prava. Kako su tehnologija i internet napredovali, EU je prepoznala potrebu za suvremenom zaštitom. Tako je 1995. godine donijela Europsku direktivu o zaštiti podataka, uspostavljajući minimalne standarde privatnosti i sigurnosti podataka, na kojima je svaka država članica temeljila svoj provedbeni zakon. Prvi *banner* oglas na internetu se pojavio 1994. godine. Većina financijskih institucija nudila je internet bankarstvo 2000. godine. *Facebook* je otvoren za javnost 2006. godine, a 2011. godine je *Googleov* korisnik tužio tvrtku zbog skeniranja njegovih e-mailova. Dva mjeseca nakon toga, europsko tijelo za zaštitu podataka izjavilo je da je Europskoj uniji potreban sveobuhvatan pristup zaštiti osobnih podataka i počeli su raditi na ažuriranju direktive iz 1995. godine.[28] Počela je priprema Europe za digitalno doba: „Digitalna budućnost Europe može se graditi samo na povjerenju. Uz čvrste zajedničke standarde za zaštitu podataka, ljudi mogu biti sigurni da kontroliraju svoje osobne podatke.“[29] GDPR je stupio na snagu 2016. nakon zasjedanja Europskog parlamenta, a aktivno se primjenjuje u svim članicama EU od 25. svibnja 2018. godine.[30]

Opća uredba o zaštiti podataka je jedinstveni skup pravila vezanih uz zaštitu osobnih podataka koji se primjenjuje u svim zemljama Europske unije i koja građanima EU-a osigurava jednaku razinu zaštite podataka, a tvrtkama jamči pravnu sigurnost. Odnosi se na sve tvrtke koje posluju u EU, koje prikupljaju podatke o građanima, ali i na tvrtke u inozemstvu koje prodaju svoje proizvode/usluge građanima EU.[31] GDPR detaljno definira niz pravnih pojmova. Neki od najvažnijih su:

- osobni podaci - svi podaci koji se odnose na pojedinca kojega se može izravno ili neizravno identificirati: ime i prezime, broj osobne iskaznice, lokacijski podaci,

[27] https://narodne-novine.nn.hr/clanci/medunarodni/1999_05_6_142.html, dostupno 15.08.2021.

[28] https://gdpr.eu/what-is-gdpr/, dostupno 15.08.2021.

[29] https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/, dostupno 15.08.2021.

[30] https://gdpr.eu/what-is-gdpr/, dostupno 15.08.2021.

[31] https://zimo.dnevnik.hr/clanak/gdpr-uredba-koja-ce-napokon-zastititi-vase-osobne-podatke---504349.html, dostupno 16.08.2021.

podaci s kreditnih kartica, zdravstveni karton (npr. povijest bolesti), biometrijski podaci (npr. otisci prsta), genetski podaci (npr. DNA), etnička pripadnost, seksualna orijentacija i spolni život, vjerska i filozofska uvjerenja, ekonomsko stanje, članstvo u sindikatu, , IP adrese, osobne poruke e-maila, kolačići u pregledniku, pseudonimizirani podaci[32],

- obrada podataka - bilo koja radnja izvedena na podacima, bilo automatska ili ručna,
- subjekt podataka - osoba čiji se podaci obrađuju,
- voditelj obrade podataka - osoba koja odlučuje zašto i kako će se osobni podaci obrađivati,
- izvršitelj obrade podataka - treća strana koja obrađuje osobne podatke u ime voditelja obrade podataka.[33]

Voditelji obrade podataka (eng. Data Protection Officer, u daljnjem tekstu: DPO) su tvrtke koje pribavljaju osobne podatke, a naredbe za obradu podataka daju izvršiteljima obrade podataka. U većini slučajeva, ista tvrtka će biti i voditelj i izvršitelj, ali to pravilo ne vrijedi uvijek.[34] Tvrtka mora imenovati službenika za zaštitu podataka ako provodi opsežnu obradu posebnih kategorija podataka, provodi opsežno praćenje pojedinaca poput praćenja ponašanja ili je javno tijelo. Ne postoje postavljeni kriteriji o tome tko bi trebao biti DPO ili koje kvalifikacije treba imati, ali prema Uredu povjerenika za informacije, oni bi trebali imati profesionalno iskustvo i zakon o zaštiti podataka razmjeran onome što organizacija provodi.[35]

Tvrtke trebaju imenovati DPO-a u slučaju da redovito ili sustavno prati pojedince ili obrađuje posebne kategorije podataka, ako je obrada podataka temeljna poslovna aktivnost tvrtke i ako tvrtka obrađuje velik broj podataka.[36]

[32] https://gdprinformer.com/hr/vodic-kroz-gdpr, dostupno 16.08.2021.

[33] https://gdpr.eu/what-is-gdpr/, dostupno 16.08.2021.

[34] https://gdprinformer.com/hr/vodic-kroz-gdpr, dostupno 16.08.2021.

[35] https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/, dostupno 17.08.2021.

[36] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm, dostupno 17.08.2021.

5.1. AZOP – Agencija za zaštitu osobnih podataka

Agencija za zaštitu osobnih podataka (u daljnjem tekstu: AZOP) je krovna organizacija za zaštitu podataka u Republici Hrvatskoj. Započela je s radom 2004. godine, a temeljena je na Zakonu o zaštiti osobnih podataka iz 2003. godine. Organizacijska struktura AZOP-a dijeli se na Službu za zaštitu osobnih podataka, Službu za nadzor i središnji registar te Službu za međunarodnu suradnju, EU i pravne poslove.

Pravni okvir djelovanja AZOP-a sastoji se od EU i nacionalnih zakonodavstava te međunarodnih ugovora.

Dokumenti koji se odnose na EU zakonodavstva su sljedeći:

- Ugovor o funkcioniranju Europske Unije, u članku 16. nalaže kako svatko ima pravo na zaštitu svojih osobnih podataka. „Europski parlament i Vijeće, odlučujući u skladu s redovnim zakonodavnim postupkom, utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu osobnih podataka u institucijama, tijelima, uredima i agencijama Unije te u državama članicama kada obavljaju svoje aktivnosti u području primjene prava Unije i pravila o slobodnom kretanju takvih podataka. Poštovanje tih pravila podliježe nadzoru neovisnih tijela. Pravila usvojena na temelju ovog članka ne dovode u pitanje posebna pravila utvrđena u članku 39. Ugovora o Europskoj uniji.“[37]
- Povelja Europske unije o temeljnim pravima u članku 7. kaže kako svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i dopisivanja. U članku 8. iznosi kako svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose. „Takvi podaci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje.“[38]
- Uredba (EZ) 1987/2006 Europskog parlamenta i Vijeća od 20. prosinca 2006. o uspostavi, djelovanju i korištenju druge generacije Schengenskog informacijskog sustava (u daljnjem tekstu: SIS II). „SIS II je informacijski sustav koji omogućava nacionalnim tijelima provedbu zakona te pravosudnim i upravnim tijelima obavljanje određenih zadaća zajedničkim korištenjem odgovarajućih podataka. Europske

[37] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A12016ME%2FTXT, dostupno 18.08.2021.

[38] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P, dostupno 18.08.2021.

agencije EUROPOL i EUROJUST također imaju ograničene pogodnosti pristupa ovom sustavu.“[39] Kategorije obrađenih informacija odnose se na osobe koje se traži zbog uhićenja, nestanka i sl. ili za osobe izvan granica EU koje pokušavaju ući ili boraviti u schengengskom prostoru bez prava na to; ili na stvari poput vozila, putnih isprava, kreditnih kartica i sl.

- 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 u Općoj uredbi za zaštitu podataka donosi se utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka.[40]
- Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija u Direktivi o privatnosti i elektroničkim komunikacijama ima za cilj povećati povjerenje u digitalne usluge i njihovu sigurnost. „Povjerljivost komunikacija zajamčena je u skladu s međunarodnim instrumentima koji se odnose na ljudska prava, posebno Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda, te ustavima država članica.“[41]
- Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP tvrdi da su „načela i pravila o zaštiti pojedinaca u vezi s obradom njihovih osobnih podataka trebala bi poštovati njihova temeljna prava i slobode, a posebno njihovo pravo na zaštitu osobnih podataka, bez obzira na nacionalnost ili boravište pojedinaca. Ovom Direktivom želi se doprinijeti uspostavi područja slobode, sigurnosti i pravde.“[42]

---

[39] https://azop.hr/wp-content/uploads/2020/12/sisii-vodic-hr.pdf, dostupno 18.08.2021.

[40] https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN, dostupno 18.08.2021.

[41] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002L0058, dostupno 18.08.2021.

[42] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L0680, dostupno 18.08.2021.

- Direktiva (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije o putnicima (u daljnjem tekstu: PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela za cilj jamči sigurnost, zaštitu života i sigurnost osoba te uspostava pravnog okvira za zaštitu podataka iz PNR-a u pogledu njihove obrade koju provode nadležna tijela.[43]

Dokumenti koji se odnose na nacionalno zakonodavstvo su sljedeći:

- Ustav RH koji u članku 37. kaže kako je svakom zajamčena sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.[44]
- Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka primjenjuje se na automatizirane zbirke podataka i automatiziranu obradu osobnih podataka u javnom i u privatnom sektoru.[45]
- Zakon o potvrđivanju izmjena i dopuna Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (ETS br. 108) koje Europskim zajednicama omogućavaju pristupanje.
- Zakon o elektroničkim komunikacijama „uređuje područje elektroničkih komunikacija, i to korištenje elektroničkih komunikacijskih mreža i pružanje elektroničkih komunikacijskih usluga, pružanje univerzalnih usluga te zaštita prava korisnika usluga, gradnja, postavljanje, održavanje i korištenje elektroničke komunikacijske infrastrukture i povezane opreme, uvjeti tržišnog natjecanja te prava i obveze sudionika na tržištu elektroničkih komunikacijskih mreža i usluga, adresiranje, numeriranje i upravljanje radiofrekvencijskim spektrom, digitalni radio i televizija, zaštita podataka i sigurnost elektroničkih komunikacija te obavljanje

[43] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L0681, dostupno 18.08.2021.

[44] https://narodne-novine.nn.hr/clanci/sluzbeni/2001_05_41_705.html, dostupno 18.08.2021.

[45] https://narodne-novine.nn.hr/clanci/medunarodni/2005_05_4_38.html, dostupno 18.08.2021.

inspekcijskog i stručnog nadzora i kontrole u elektroničkim komunikacijama, kao i osnivanje nacionalnog regulatornog tijela za elektroničke komunikacije i poštanske usluge, njegovo ustrojstvo, djelokrug i nadležnosti te postupak donošenja odluka i rješavanja sporova u elektroničkim komunikacijama.“[46]

- Zakon o provedbi Opće uredbe o zaštiti podataka donosi uredbe o nadležnom tijelu (AZOP), obradu osobnih podataka u posebnim slučajevima, postupke koji su u nadležnosti AZOP-a te pravne lijekove, prekršajne odredbe i upravne novčane kazne.[47]
- Zakon o prijenosu i obradi podataka o putnicima u zračnom prometu u svrhu sprječavanja, otkrivanja, istraživanja i vođenja kaznenog postupka za kaznena djela terorizma i druga teška kaznena djela.
- Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija.
- Zakon o potvrđivanju Protokola kojim se mijenja i dopunjuje Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka.[48]
- Uredba o Hrvatskom viznom informacijskom sustavu (u daljnjem tekstu: HVIS) uključuje osobne i biometrijske podatke, a uređuje podatke o podnesenim zahtjevima za vizu, izdanim, produljenim, odbijenim, poništenim i ukinutim vizama i razmjena tih podataka između viznih tijela, postupak uzimanja biometrijskih podataka te način čuvanja i korištenja zbirke podataka zahtjeva za vizu.[49]
- Kriteriji za obročnu otplatu i uvjete za raskid obročne otplate upravne novčane kazne Agencije za zaštitu osobnih podataka.[50]

Međunarodni ugovori:

- Konvencija za zaštitu ljudskih prava i temeljnih sloboda u članku 8. navodi kako „svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i

[46] https://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, dostupno 18.08.2021.

[47] https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html, dostupno 18.08.2021.

[48] https://azop.hr/pravni-okvir/, dostupno 18.08.2021.

[49] https://narodne-novine.nn.hr/clanci/sluzbeni/2013_03_36_657.html, dostupno 18.08.2021.

[50] https://azop.hr/pravni-okvir/, dostupno 18.08.2021.

dopisivanja. 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 spriječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih."[51]

- Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka ima svrhu svakoj fizičkoj osobi, bez obzira na njezino državljanstvo i boravište, na području svake stranke, osigurati poštovanje njezinih prava i temeljnih sloboda, a osobito njezino pravo na privatnost glede automatizirane obrade osobnih podataka koji se na nju odnose. Primjenjuje se na automatizirane zbirke podataka i automatiziranu obradu osobnih podataka u javnom i u privatnom sektoru.[52]

5.2. Obveze i zahtjevi GDPR-a

Zahtjevi GDPR-a obuhvaćaju ukupno 99 članaka. Bilo koje poduzeće koje pohranjuje ili obrađuje osobne podatke o građanima EU-a unutar država EU-a mora se pridržavati GDPR-a, čak i ako nemaju poslovnu prisutnost u EU-u. Tvrtke podliježu GDPR-u ako:

- je tvrtka prisutna i posluje u zemlji EU-a,
- tvrtka koja obrađuje osobne podatke europskih stanovnika nema prisutnost u EU-u,
- poduzeće ima više od 250 zaposlenih,
- obrada podataka utječe na prava i slobode ispitanika, čak i ako tvrtka ima manje od 250 zaposlenika.[53]

Obveze i zahtjevi koje GDPR donosi su:

- zakonitost, pravičnost i transparentnost - obrada mora biti zakonita, poštena i transparentna za ispitanika,
- ograničenje svrhe – podaci se obrađuju u legitimne svrhe navedene izričito subjektu podataka kada su prikupljene,

[51] https://narodne-novine.nn.hr/clanci/medunarodni/1999_05_6_142.html, dostupno 18.08.2021.

[52] https://narodne-novine.nn.hr/clanci/medunarodni/2005_05_4_38.html, dostupno 18.08.2021.

[53] https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=26cdd9cb55e5, dostupno 20.08.2021.

- minimiziranje podataka - prikuplja se i obrađuje samo onoliko podataka koliko je apsolutno potrebno za navedene svrhe,
- točnost – podaci moraju biti točni i ažurni,
- ograničenje pohrane – podaci za osobnu identifikaciju mogu se pohraniti samo onoliko dugo koliko je potrebno za navedenu svrhu,
- integritet i povjerljivost - obrada se mora obaviti na takav način da se osigura odgovarajuća sigurnost, integritet i povjerljivost (npr. pomoću šifriranja),
- odgovornost - voditelj obrade podataka odgovoran je za mogućnost dokazivanja usklađenosti s GDPR-om sa svim ovim načelima.[54]

Odgovornost GDPR-a nalaže mogućnost dokazivanja da je poslovanje bilo koje tvrtke u skladu s GDPR-om. Kako bi se dokazivanje lakše provelo, zaposlenicima je potrebno objasniti koje su odgovornosti za zaštitu podataka te ih obučiti kako bi uspješno prošli tehničke i organizacijske sigurnosne mjere i arhivirati svu dokumentaciju podataka koji se prikupljaju te kako se koriste i tko je odgovoran za njih. Tehničke mjere podrazumijevaju zahtjeve zaposlenika za npr. dvofaktorsku provjeru autentičnosti na računima na koje se pohranjuju osobni podaci i sl. Organizacijske mjere su sve one olakšavajuće mjere za zaposlenike kako bi radili u skladu s GDPR-om. To podrazumijeva obuku zaposlenika, priručnik za zaposlenike s pravilima o zaštiti podataka ili ograničenje pristupa osobnim podacima za one zaposlenike kojima je to potrebno. Ako tvrtka surađuje s drugom tvrtkom koja radi obradu podataka umjesto njih, potrebno je definirati ugovorom na koji način se podaci obrađuju.[55]

Obrada podataka dopuštena je kada:

- tvrtka ima privolu predmetnog pojedinca za obradu osobnih podataka,
- su osobni podaci potrebni za ispunjavanje ugovorne obveze prema pojedincu,
- su osobni podaci potrebni za ispunjenje zakonske obveze,
- su osobni podaci potrebni za zaštitu životnog interesa pojedinca,
- se osobni podaci obrađuju u okviru zadaće javnog interesa,
- tvrtka djeluje u ime legitimnih interesa pod uvjetom da nisu ozbiljno narušena temeljna prava i slobode pojedinca čiji se podaci obrađuju. Osobni podaci se ne mogu

[54] https://gdpr.eu/what-is-gdpr/, dostupno 20.08.2021.

[55] Ibid.

obrađivati ako prava pojedinca imaju prevagu u odnosu na interese tvrtke koja obrađuje podatke.[56]

5.3. Pseudonimizacija

Pseudonimizacija znači zamjenu svih informacija koje bi se mogle koristiti za identifikaciju pojedinca s pseudonimom ili, drugim riječima, vrijednost koja ne dopušta izravnu identifikaciju pojedinca. Prema GDPR-u, definirana je kao „obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom nositelju podataka bez korištenja dodatnih podataka, pod uvjetom da se ti dodatni podaci čuvaju odvojeno i podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne pripisuju identificiranoj fizičkoj osobi.“[57]

	Ime studenta	**Matični broj studenta**	**Kolegij**
Izvorni podaci	Hrvoje Horvat	1234567890	Etika
Pseudonimizirani podaci	Kandidat 1	XXXXXXXXXX	Etika

Tablica 2. Primjer pseudonimiziranih podataka

Pseudonimizacija olakšava obradu osobnih podataka, smanjujući rizik izlaganja osjetljivih podataka neovlaštenom osoblju i zaposlenicima. Primjer je slanje plaće zaposlenika u *excel* listama putem e-maila. Iako su pošiljatelj i primatelj e-maila ovlašteni pristupiti tim podacima, IT podrška također ima pristup tim e-mailovima.

Kada su podaci pseudonimizirani, postoji mnogo manja šansa za otkrivanje osobnih podataka, jer čini zapis neidentificiranim, a ostaje prikladan za obradu i analizu podataka. U tom kontekstu, pseudonim je identifikator koji je povezan s pojedincem. Baš kao što pisci koriste pseudonime kako bi prikrili svoj identitet i zaštitili svoju privatnost, pseudonimi se koriste u istu svrhu u zaštiti podataka.

[56] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm, dostupno 20.08.2021.

[57] https://gdpr-info.eu/art-4-gdpr/, dostupno 22.08.2021.

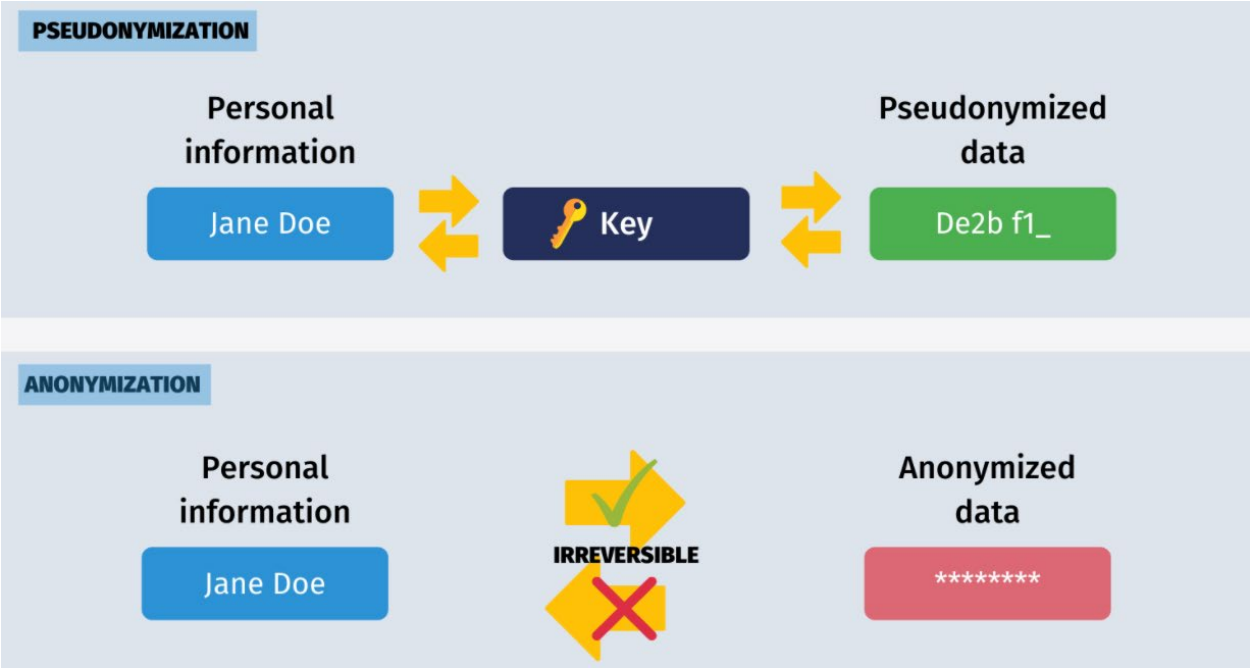
Pseudonim može biti broj, slovo, poseban znak ili bilo koja kombinacija onih koji su vezani za određene osobne podatke ili pojedinca i stoga podatke čini sigurnijima za upotrebu u poslovnom okruženju.[58]

Postoje i anonimizirani podaci koji ne zadovoljavaju kriterije potrebne za kvalifikaciju kao osobni podaci i stoga ne podliježu istim ograničenjima koja se postavljaju na obradu osobnih podataka prema GDPR-u. Podaci se mogu smatrati anonimiziranima kada se pojedinci više ne mogu identificirati. Važno je napomenuti da se osoba ne mora imenovati da bi se mogla identificirati. Ako postoje drugi podaci koji omogućuju povezivanje pojedinca s podacima o njima, a koji se ne mogu odnositi na nekog drugog u grupi, oni se ipak mogu identificirati. U tom je kontekstu je važno razmotriti koji su identifikatori (dijelovi informacija koji su usko povezani s određenom osobom, a koji bi se mogli koristiti za njihovo izdvajanje) sadržani u pohranjenim informacijama. Tamo gdje su podaci anonimizirani, izvorne podatke treba sigurno izbrisati kako bi se spriječilo preokretanje procesa anonimizacije. U većini slučajeva, ako se to brisanje ne dogodi, tada se podaci klasificiraju kao pseudonimizirani, a ne kao anonimizirani te se i dalje smatraju osobnim podacima. Zakon o zaštiti podataka ne propisuje nikakvu posebnu tehniku anonimizacije, pa je na pojedinim voditeljima obrade da osiguraju da je bilo koji postupak anonimizacije koji odaberu dovoljno robustan.[59]

Iako se pseudonimizacija i anonimizacija koriste za zaštitu identiteta pojedinca, one nisu sinonimi. To se može protumačiti na Slici 2.

[58] https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/, dostupno 22.08.2021.

[59] https://www.dataprotection.ie/en/dpc-guidance/anonymisation-pseudonymisation, dostupno 22.08.2021.

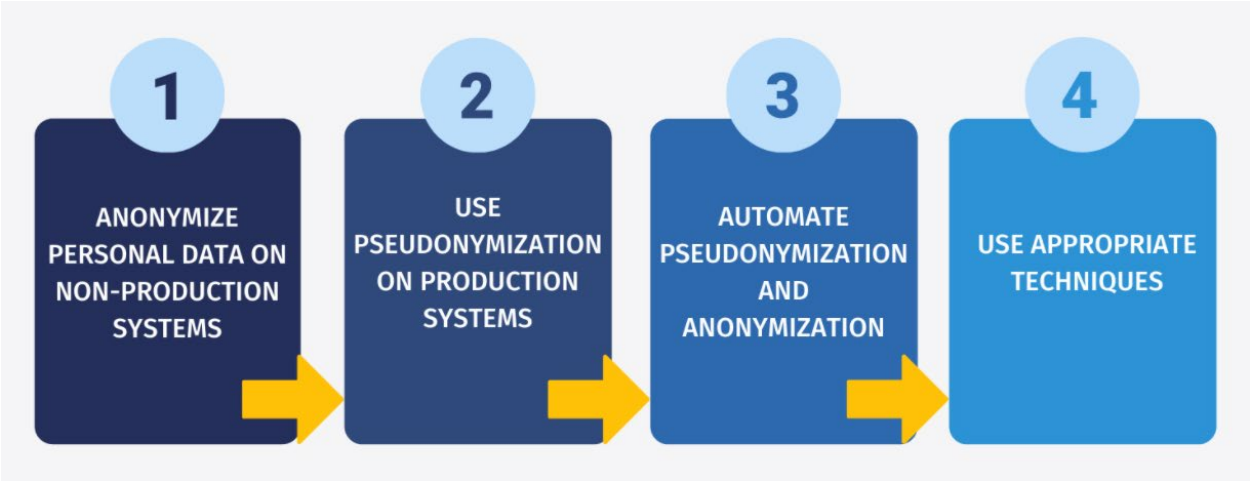


Slika 2. Razlika između pseudonimizacija i anonimizacije

Za osoblje ovlašteno pristupiti pseudonimiziranim podacima postoji ključ koji omogućuje poništenje identifikacije podataka. Anonimizacija je tehnika koja nepovratno mijenja podatke pa se pojedinac više ne može izravno ili neizravno identificirati. Obje su metode jednako preporučljive. Izbor će ovisiti o mnogim čimbenicima (slučaj upotrebe, stupanj rizika, način obrade podataka unutar tvrtke itd.). Najbolja metoda odabira određena je svrhom obrade, vrstom podataka koja se obrađuje i rizikom od kršenja podataka koje se nameće. U usporedbi s anonimizacijom, pseudonimizacija je mnogo sofisticiranija opcija jer ostavlja ključ za otkrivanje podataka. Na taj se način podaci ne smatraju izravnim identifikacijskim podacima, a ni anonimiziranima, pa ne gube izvornu vrijednost.[60]

Preporuke za pseudonimizaciju vide se na Slici 3.

[60] https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/, dostupno 23.08.2021.



Slika 3. Preporuke za pseudonimizaciju

Anonimizacija se preporučuje u neproizvodnim organizacijama. Skupovi podataka s anonimiziranim osobnim podacima i dalje su izvrsni za razvoj, statistiku i analitiku. Pseudonimizacija se preporučuje u proizvodnim organizacijama. Na taj će način samo ovlašteni korisnici imati pristup osobnim podacima ispitanika. Kad više ne postoji zakonita osnova za obradu osobnih podataka nositelja podataka, sustav će izbrisati pseudonim i učiniti subjekt podataka anonimiziranim (zaboravljenim). Automatizacijom pseudonimizacije i anonimizacije smanjuje se mogućnost ljudske pogreške. Odabir odgovarajućih tehnika propisala je u izvješću o „Tehnikama i najboljim praksama pseudonimizacije“ Agencija Europske unije za kibersigurnost (eng. The European Union Agency for Cybersecurity, u daljnjem tekstu: ENISA). Vodič raspravlja o kriterijima za odabir odgovarajućih tehnika pseudonimizacije, kao što su zaštita podataka, skalabilnost i oporavak. Vodič također razmatra specifične slučajeve uporabe različitih identifikatora, poput IP adrese ili e-maila. U izvješću je zaključeno da ne postoji samo jedno rješenje ili jedan način za operacionalizaciju pseudonimizacije koji funkcionira za sve industrije ili sve scenarije. “… Ne postoji jedno jednostavno rješenje za pseudonimizaciju koje odgovara svim pristupima u svim mogućim scenarijima. Naprotiv, potrebna je visoka razina kompetencije kako bi se primijenio robustan proces pseudonimizacije, moguće smanjivši prijetnju od diskriminacije ili napada na ponovnu identifikaciju, uz održavanje stupnja korisnosti potrebne za obradu pseudonimiziranih podataka.”[61]

[61] Ibid.

5.4. Povrede osobnih podataka i sankcije

U slučaju da dođe do bilo kakve zlouporabe osobnih podataka, tvrtka je dužna obavijestiti nadležno nadzorno tijelo, a u nekim slučajevima i samog pojedinca čiji su podaci povrijeđeni. Organizacije su dužne prijaviti sve povrede koje bi mogle rezultirati rizikom po prava i slobode pojedinaca i dovesti do diskriminacije, štete ugledu, financijskom gubitku, gubitku povjerljivosti ili bilo kojeg drugog ekonomskog ili društvenog nepovoljnog položaja. Drukčije rečeno, ako se prekrši ime, prezime, adresa, podaci o rođenju, zdravstveni karton, bankovni podaci ili bilo koji privatni ili osobni podaci o pojedincu, tvrtka je dužna obavijestiti povrijeđene osobe, kao i regulatorno tijelo, kako bi se učinilo sve što je moguće za ograničenje nastale štete.

Takve povrede priopćuju se putem obavijesti o kršenju koja se izravno dostavlja povrijeđenicima. Obavijest se ne smije prenositi u priopćenjima za javnost, na društvenim mrežama ili na web stranici tvrtke. Kršenje se mora prijaviti nadležnom nadzornom tijelu u roku od 72 sata nakon što je tvrtka za to prvi puta saznala. U međuvremenu, ako je kršenje dovoljno ozbiljno da znači da se korisnici ili javnost moraju obavijestiti, GDPR zakonodavstvo kaže da se korisnici moraju smatrati odgovornima bez „nepotrebnog odgađanja“.[62]

Nepoštivanjem GDPR-a nastupaju visoke novčane kazne. Raspon kazni se kreće do 4% globalnog prometa tvrtke, a maksimalna kazna iznosi 20 milijuna eura. Niža kazna od 10 milijuna eura ili 2% globalnog prometa bit će primijenjena na tvrtke koje na drugi način zloupotrebljavaju podatke. Oni uključuju propuste u prijavi povrede podataka, neuspjeh u izgradnji privatnosti prema dizajnu i osiguravaju da se zaštita podataka primjenjuje u prvoj fazi projekta te da budu usklađeni imenovanjem službenika za zaštitu podataka. Kazne ovise o ozbiljnosti povrede te o tome smatra li se da je tvrtka dovoljno ozbiljno preuzela usklađenost i propise vezane uz sigurnost osobnih podataka. [63]

Procjena učinka na zaštitu osobnih podataka je obvezna u slučajevima sustavne i opsežne procjene osobnih aspekata temeljenih na automatiziranoj obradi kojom se donose odluke pravnih učinaka za pojedince, u slučaju opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima, u slučajevima sustavnog praćenja javno dostupnog područja u velikoj mjeri. Nadzorno tijelo dužno je javno objaviti popis vrste

[62] https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/, dostupno 24.08.2021.

[63] Ibid.

postupaka obrade podložne zahtjevu za procjenu učinka na zaštitu osobnih podataka. Procjena učinka sadrži:

- sustavan opis predviđenih postupaka obrade te svrhu obrade,
- procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama,
- procjenu rizika za prava i slobode ispitanika,
- mjere predviđene za rješavanje rizičnih problema (zaštitne mjere, sigurnosne mjere, mehanizmi za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s Uredbom).[64]

5.5. Značenje GDPR-a za građane EU

Započnimo ovo potpoglavlje sami od sebe – posjedujemo pametne telefone, prijenosne tablete ili laptope. Na tim uređajima sigurno smo registrirani barem na jednu društvenu mrežu gdje se povezujemo s prijateljima, ali upoznajemo i nove ljude. Sigurno smo registrirani i na neku od web-trgovina, obzirom da sve češće naručujemo stvari s interneta, umjesto da ih kupujemo u fizičkim trgovinama. Kako bismo uopće kupili nešto, potrebna nam je bankovna kartica, pa su sada i naši financijski podaci negdje na internetu, kako bismo lakše provjerili svoje financijsko stanje. Sve ovo govori kako smo povezani s mnogobrojnim tvrtkama i da naše podatke netko drugi sigurno vidi. Svi ti podaci danas su uvelike u opasnosti, jer su lako dostupni hakerima. Jedna od glavnih promjena koja je došla s GDPR-om je ta da građani imaju pravo znati kada su njihovi podaci hakirani. Tvrtke su obavezne obavijestiti odgovarajuća nacionalna tijela što je prije moguće, kako bi građani bili u mogućnosti poduzeti sve odgovarajuće mjere protiv zloupotrebe vlastitih podataka. Građanima se također obećava lakši pristup vlastitim osobnim podacima u smislu načina na koji se oni obrađuju, a tvrtke su dužne na jasan i razumljiv način detaljno objasniti kako koriste podatke o korisnicima.[65]

GDPR je građanima donio sljedeće promjene:

[64] J. Čizmić, M. Boban: Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Rijeka, 2018., str. 388

[65] https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/, dostupno 25.08.2021.

- širi opseg – odnosi se na sve tvrtke kojima smo dali svoje podatke, bile one registrirane na području EU-a ili ne, tako da građani EU-a budu sigurni u zaštitu svojih podataka, bez obzira od koga kupuju ili se registriraju radi nečeg drugoga na neku od inozemnih web stranica,
- privola – građani imaju slobodu odlučiti pružiti ili povući privolu za određene usluge. Ona mora biti slobodna, specifična, informativna i nedvosmislena,
- pravo na pristup osobnim podacima – građani imaju pravo saznati od DPO-a obrađuju li se njihovi osobni podaci, gdje i u koju svrhu. Dozvoljeno im je zatražiti i besplatnu kopiju osobnih podataka te izmjeniti podatke u slučaju da su netočni. Sve to znači da potrošači imaju pravo znati koji se osobni podaci o njima prikupljaju i kako ih njihovi davatelji usluga obrađuju,
- prijenos osobnih podataka – građani imaju pravo zatražiti od svog davatelja usluga da podrži prijenos njihovih osobnih podataka drugom davatelju usluga kada je to potrebno,
- pravo na zaborav – daje građanima pravo da DPO obriše njihove osobne podatke, prestanu s daljnjim otkrivanjima podataka i ako postoje treće strane obrađivača podataka, oni trebaju učiniti isto.[66]

U osnovi, građani EU-a nakon uvođenja GDPR-a imaju više moći nad svojim osobnim podacima nego su imali prije. Možda neki ove zakone nikada nećete koristiti, ali činjenica da ih se tvrtke moraju pridržavati znači da vode više računa o osobnim podacima, što nikako ne može biti loše.

[66] https://www.pwc.in/consulting/cyber-security/blogs/gdpr-what-it-means-for-individuals-and-consumers.html, dostupno 25.08.2021.

6. Anketno istraživanje

Za potrebe ovog rada, autor je proveo kvantitativno istraživanje u obliku ankete na društvenoj mreži *Facebook*.

Istraživanje je provedeno na slučajnom uzorku od 132 ispitanika različitog spola, dobi i statusa obrazovanja.

6.1. Cilj istraživanja

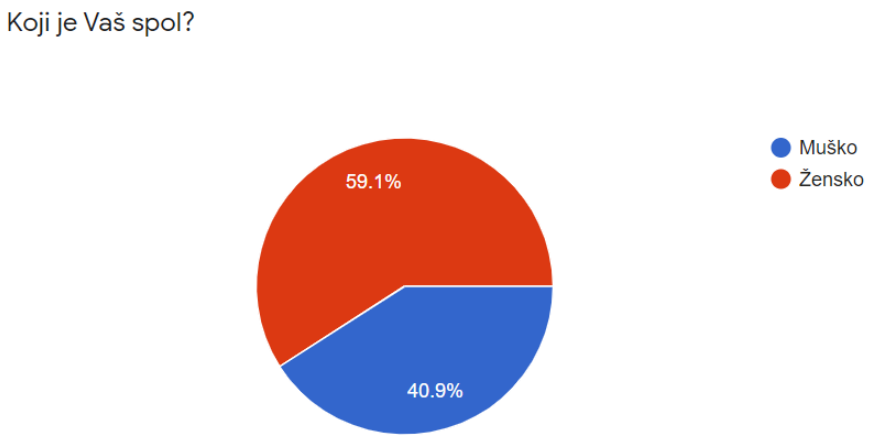
Anketa sadrži pitanja vezana uz pojedine teze postavljene u radu, kako bi se dokazala ili opovrgnula njihova istinitost, gledajući s etičke strane, od strane ispitanika. Stoga je cilj ankete usporediti takva etička stajališta sa svim poglavljima ovoga rada.

6.2. Metoda i nacrt istraživanja

Anketa sadrži ukupno 11 pitanja. Devet pitanja tiču se same teme ovog rada – percepcije privatnosti, utjecaja tehnologije i medija na privatnost te na GDPR, a ostala tri pitanja tiču se demografije ispitanika, kako bismo uvidjeli imaju li jednake dobne skupine ili ispitanici jednakog obrazovnog stupnja jednaka ili različita stajališta.

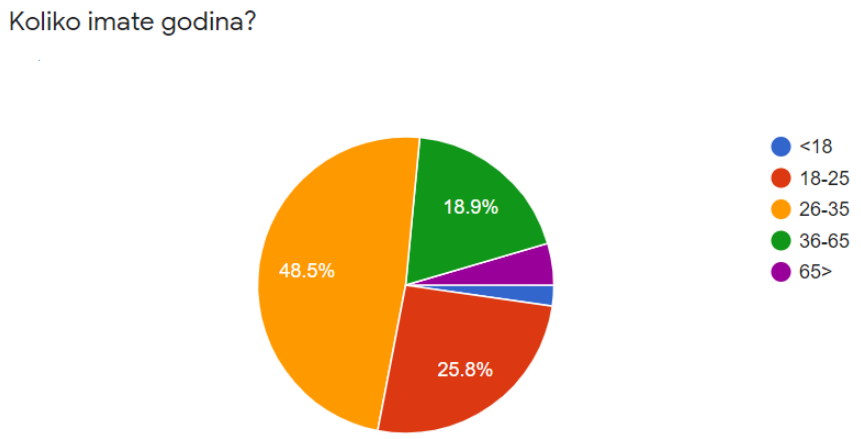
6.3. Analiza istraživanja

Započnimo analizu ankete s demografskim podacima ispitanika. Anketu je ispunilo 132 ispitanika, od kojih žene čine 59,1%, a muškarci 40,9%.



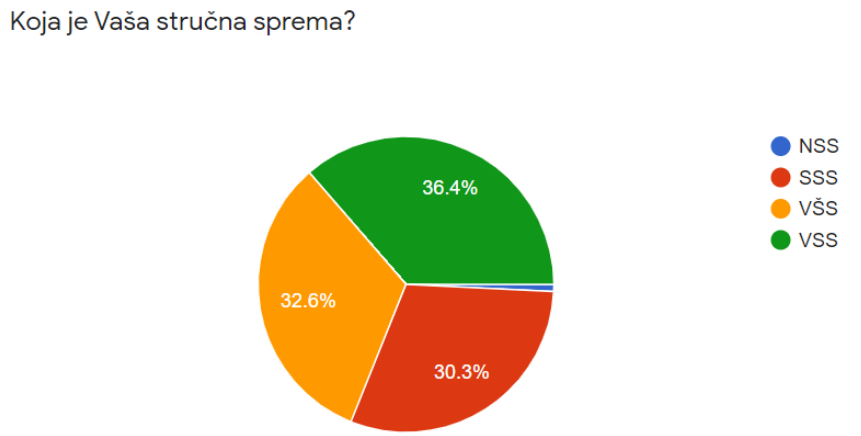
Graf 1. Spol ispitanika

Od ukupnog broja ispitanika, 48,5% je u dobi između 26 i 35 godina, 25,8% je u dobi između 18 i 25 godina, 18,9% čine ispitanici u dobi između 36 i 65 godina, 4,5% čine ispitanici koji imaju više od 65 godina, a 2,3% ispitanici koji su mlađi od 18 godina.



Graf 2. Dob ispitanika

Posljednje demografsko pitanje tiče se stupnja obrazovanja ispitanika. Tako je najviše ispitanika, njih 36,4% visoke stručne spreme, 32,6% ima višu stručnu spremu, 30,3% ima srednju stručnu spremu, a 0,8% ima nisku stručnu spremu.



Graf 3. Stupanj obrazovanja ispitanika

Prvo pitanje koje je ispitanicima postavljeno bilo je smatraju li privatnost važnom sastavnicom svojega života. Velika većina ispitanika, njih 89,3% odgovorilo je da je, dok je samo 10,7% odgovorilo da nije.

Graf 4. Važnost privatnosti za ispitanike

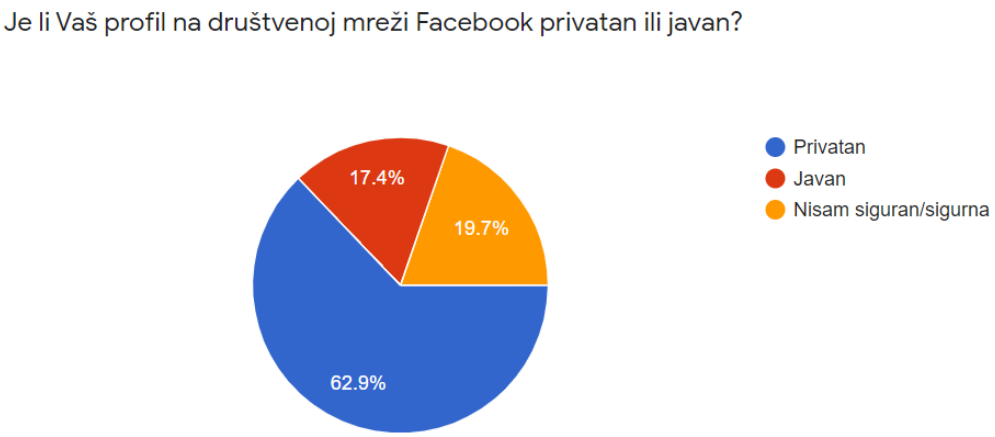
Drugo pitanje bilo je čitaju li ispitanici pravila privatnosti pri registraciji na različite portale, web-trgovine i društvene mreže. Iako im je većini privatnost važna stavka, ipak ih većina od 85,6% ne čita, dok samo 14,4% čita pravila privatnosti.

Graf 5. Informiranje ispitanika o pravilima privatnosti pri registraciji na portale, društvene mreže ili web-trgovine

Sljedeće pitanje bilo je vjeruju li ispitanici tvrtkama da neće zloupotrebljavati njihove podatke nakon njihove privole na pravila privatnosti. Većina od 62,1% ih ne vjeruje, dok 37,9% ipak vjeruje.

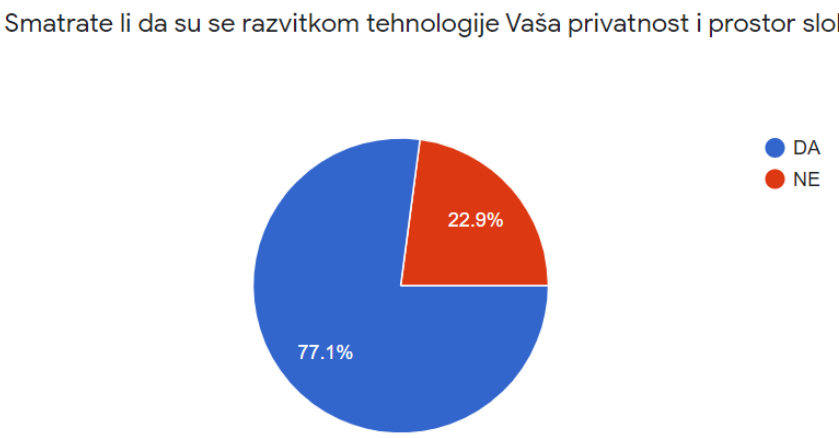
Graf 6. Povjerenje u organizacije pri davanju privole na korištenje osobnih podataka

Obzirom da je anketa provedena na društvenoj mreži *Facebook*, ispitanici su upitani je li njihov profil privatan ili javan. Da je privatan, odgovorilo je 62,9%, javan profil ima 17,4%, a 19,7% nije sigurno kakve postavke su postavili što se tiče njihovog profila.



Graf 7. Privatnost profila društvene mreže Facebook ispitanika

Zatim su ispitanici upitani smatraju li da su se razvojem tehnologije njihova privatnost i prostor slobode smanjili. 77,1% smatra da je, dok 22,9% smatra kako njihova privatnost i prostor slobode nisu narušeni tehnološkim napretkom.



Graf 8. Utjecaj razvitka tehnologije na privatnost i prostor slobode ispitanika

Sljedeće pitanje također se ticalo tehnologije i privatnosti. Ispitanici su upitani misle li da je kreiranje ponude „samo za vas“, od strane trgovaca i marketinških stručnjaka, u redu. Većina od 66,7% smatra da takvo korištenje njihovih osobnih podataka nije u redu, a 33,3% smatra da je.

Graf 9. Preferencija ispitanika o korištenju njihovih osobnih podataka u svrhu kreiranja ponude „samo za vas“

Pitanje vezano uz medije i privatnost ticalo se stajališta ispitanika o iznošenju stvari iz privatnog života slavnih osoba. 63,6% ispitanika smatra da mediji krše privatnost poznatih kada objavljuju neprimjeren sadržaj o njima, poput neobrađenih fotografija ili tračeva, dok 36,4% smatra da to nije kršenje njihove privatnosti.

Graf 10. Stav ispitanika o iznošenju stvari iz privatne sfere života javnih osoba u medijima

Što se tiče povjerenja ispitanika u GDPR, 67,4% smatra da njihova privatnost nije sigurnija otkako je GDPR stupio na snagu, dok samo 32,6% vjeruje da je.

Graf 11. Povjerenje ispitanika u GDPR

Zadnje pitanje u anketi ticalo se zloupotrebe osobnih podataka. 65,2% ispitanika izjavilo je kako nisu imali problema sa zloupotrebom osobnih podataka, dok je 34,8% izjavilo da je, bilo to krađa identiteta, fotografija ili hakiran profil.

Graf 12. Zloupotreba osobnih podataka ispitanika

Detaljnijom analizom ove ankete utvrđeno je kako privatnost nevažnom smatraju više muškarci nego žene, podjednakih statusa obrazovanja. Pravila privatnosti čita 7 muškaraca i 12 žena, a većina ih ima viši ili visoki status obrazovanja. Da tvrtke neće iskorištavati njihove osobne podatke u druge svrhe osim onih koji su navedeni u pravilniku o zaštiti podataka, žene vjeruju duplo više od muškaraca. *Facebook* profili su kod većine ispitanika privatni, a oni koji su javni, u podjednakom su broju i kod muškaraca i kod žena. Žene u većem broju smatraju kako tehnologija nije smanjila njihov prostor slobode i privatnost od muškaraca, ali podjednaki broj i muškaraca i žena smatra kako je u redu što trgovci i marketinški stručnjaci koriste njihove osobne podatke za stvaranje ponude „samo za vas“. 27 žena i 19 muškaraca smatra kako mediji ne krše privatnost javnih osoba kada objavljuje stvari iz njihovih privatnih života. I žene i muškarci su u podjednakom broju imali iskustva sa zloupotrebom osobnih podataka. Većina muškaraca i žena je izjavila kako ne vjeruje da GDPR štiti njihovu privatnost, bez obzira na stupanj njihovog obrazovanja.

7. Zaključak

Kroz ovaj rad detaljno su se analizirali brojni pojmovi vezani uz privatnost. U prvom dijelu rada govorilo se kako su je brojni teoretičari tumačili u početku te kako je nastao model procesa privatnosti. U anketi koja je provedena na kraju rada utvrđeno je kako je većini ljudi privatnost važna, iako su skeptični prema tvrtkama koje rade na temelju njihovih osobnih podataka.

Tome je tako jer se privatnost razvijala u korak s tehnologijom. Svima je poznato koliko je tehnologija uznapredovala i vjerojatno bi se teško snalazili bez nje, obzirom na ubrzan stil života koji vodimo. Ispitanici su anketi potvrdili da se razvojem tehnologije smanjio njihov prostor slobode i privatnost, pa je iz tog razloga većina ljudi na društvenim mrežama svoje profile zaključalo za javnost. Isto su svjesni koliko web-trgovine i marketing koriste njihove podatke kako bi stvarali personalizirane ponude i poruke te većinski smatraju kako to ipak nije u redu.

Naravno, razvoj tehnologije utjecao je i na razvoj medija, pa novine više nisu što su nekada bile. Danas većina tiskovina ima i svoje portale i društvene mreže na kojima prenose puno više vijesti i dobivaju povratne informacije od svojih čitatelja. Medijske ličnosti su više nego ikada pod povećalom, što većina ljudi smatra neetičnim, obzirom na svjesnost o tome da su i oni ipak samo ljudi.

Upravo zbog invazije na privatnost od strane tehnologije i medija nastala je potreba za sve detaljnijim zakonima koji štite privatnost. Tako je nastao i GDPR, koji diktira zakone o privatnosti na području cijele EU, ali i šire. Ti zakoni su u provedbi tek nekoliko godina, pa ljudi još uvijek nisu stekli dovoljnu razinu povjerenja u njih. Više od trećine ispitanika ankete ovoga rada imalo je negativna iskustva sa zlouporabom osobnih podataka, pa su vjerojatno iz tog razloga još uvijek skeptični oko provedbe GDPR-a. S druge strane, pojedinci vjerojatno nisu dovoljno upućeni u zakone, jer da jesu, uvidjeli bi koliku zaštitu su dobili uvođenjem istoga i kakve kazne prijete prekršiteljima. Bilo kako bilo, budućnost koja dolazi bit će sigurno još kompleksnija nego je danas i možemo se samo nadati kako ćemo uspjeti održati korak s njom, i u pravnom i u etičkom smislu.

U Koprivnici, 01.09.2021., _____

8. Literatura

Knjige:

1. A. McStay: Privacy and the media, SAGE Publications Ltd., London, 2017.
2. L.A. Day: Etika u medijima, Klub PLUS, Beograd, 2008.
3. S. Garnett, S. Halft, M. Herz, J. M. Mönig: Media and Privacy, Stutz, Passau, 2014.

Časopisi:

1. A. D. Moore, Defining Privacy: Journal of Social Philosophy, br. 3, svezak 39, 2008., str. 411-428
2. G. T. Marx: Privacy and Techonology, Telektronikk, br. 1, svezak 96, 1996., str. 40-48
3. J. K. Burgoon, Privacy and Communication: Annals of the International Communication Association, br. 6, siječanj 1982., str. 206-243
4. L. D. Brandeis, S. D. Warren: The Right to Privacy, Harvard Law Review, br. 5, svezak 4, prosinac 1890.
5. L. M. Austin, Re-reading Westin: Theoretical Inquiries in Law, br. 53, svezak 20, 2019., str. 53-81
6. R. Gavison: Privacy and the Limits of Law, The Yale Law Journal, br. 3, svezak 89, siječanj 1890., str. 421-471
7. W. L. Prosser, Privacy: California Law Review, br. 3, svezak 48, kolovoz 1960., str. 383-423

Radovi na konferenciji:

1. J. Čizmić, M. Boban: Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj. Zbornik Pravnog fakulteta Sveučilišta u Rijeci, Rijeka, 2018., str. 377-410

Doktorski, magistarski i diplomski radovi:

1. A. Pavuna: Transformacija pojma prava na privatnost kao posljedica razvoja tehnologije i novih sigurnosnih izazova, Doktorska disertacija, Sveučilište u Zagrebu, Fakultet političkih znanosti, 2019.
2. T. Dienlin: The psychology of privacy: Analyzing processes of media use and interpersonal communication, Doktorski rad, University of Hohenheim, Hohenheim, 2016.

Internet izvori:

1. https://azop.hr/wp-content/uploads/2020/12/sisii-vodic-hr.pdf
2. https://azop.hr/pravni-okvir/

3. https://www.balticapprenticeships.com/blog/what-is-techlash-and-what-does-it-mean-for-the-digital-industry
4. https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/
5. https://www.dataprotection.ie/en/dpc-guidance/anonymisation-pseudonymisation
6. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A12016ME%2FTXT
7. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A12007P
8. https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN
9. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002L0058
10. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L0680
11. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L0681
12. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm
13. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hr.htm
14. https://www.experian.co.uk/business/glossary/data-minimisation/, 22.07.2021.
15. https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=26cdd9cb55e5
16. https://gdprinformer.com/hr/vodic-kroz-gdpr
17. https://gdpr.eu/what-is-gdpr/
18. https://www.theguardian.com/commentisfree/2020/feb/02/will-we-just-accept-our-loss-of-privacy-or-has-the-techlash-already-begun, 25.07.2021.
19. https://www.ifj.org/who/rules-and-policy/global-charter-of-ethics-for-journalists.html, 30.07.2021.
20. https://media.privacyinternational.org/w/7zVySBTDcJUpe3YqoAZK1x, dostupno 15.07.2021.
21. https://narodne-novine.nn.hr/clanci/medunarodni/1999_05_6_142.html
22. https://narodne-novine.nn.hr/clanci/sluzbeni/2001_05_41_705.html
23. https://narodne-novine.nn.hr/clanci/medunarodni/2005_05_4_38.html
24. https://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html
25. https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
26. https://narodne-novine.nn.hr/clanci/sluzbeni/2013_03_36_657.html
27. https://narodne-novine.nn.hr/clanci/medunarodni/1999_05_6_142.html
28. https://narodne-novine.nn.hr/clanci/medunarodni/2005_05_4_38.html
29. https://www.pwc.in/consulting/cyber-security/blogs/gdpr-what-it-means-for-individuals-and-consumers.html
30. https://techcrunch.com/2019/09/26/privacy-queen-of-human-rights-in-a-digital-world/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANGe4anGvggpEzq3aCd1eUa_DdFWyPpVkKwGV4vFhe50KEQxgoqnY3JEGnMIQ0khZM0t5O6Yd9P1pLuPoqrQ2VJCel-bFSGX6g_ZI7AT8TgCgAt8Db_A3hNcTSTOWPj8eewpKfy0cDQHnyVroIbFF3ahMvban7-uBja4xvtdGyS0, 21.07.2021.
31. https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/
32. https://zimo.dnevnik.hr/clanak/gdpr-uredba-koja-ce-napokon-zastititi-vase-osobne-podatke---504349.html

Popis slika

Popis tablica

Popis grafikona