

Zaštita privatnosti i osobnih podataka, s posebnim osvrtom na profiliranje i bihevioralno oglašavanje

Radošević, Lukrecija

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Law / Sveučilište u Zagrebu, Pravni fakultet**

Permanent link / Trajna poveznica: <https://urn.nsk.hr/urn:nbn:hr:199:039026>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-08-08**



Repository / Repozitorij:

[Repository Faculty of Law University of Zagreb](#)



Sveučilište u Zagrebu
Pravni fakultet u Zagrebu
Katedra za pravo informacijskih tehnologija i pravnu informatiku

Lukrecija Radošević

ZAŠTITA PRIVATNOSTI I OSOBNIH PODATAKA, S
POSEBNIM OSVRTOM NA PROFILIRANJE I
BIHEVIORALNO OGLAŠAVANJE

diplomski rad

Mentor : prof. dr. sc. Hrvoje Lisičar

Zagreb, 2022.

Izjava o izvornosti

Ja, Lukrecija Radošević, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiva autorica diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristila drugim izvorima do onih navedenih u radu.

Lukrecija Radošević, v. r.

SADRŽAJ

1.	UVOD	1
1.1.	Predmet i cilj rada	1
1.2.	Izvori podataka i metode prikupljanja	1
1.3.	Sadržaj i struktura rada	1
2.	PRAVO NA PRIVATNOST	3
2.1.	Pojam i sadržaj prava	3
2.2.	Zaštita osobnih podataka	5
2.3.	Pravni okvir zaštite privatnosti i osobnih podataka	7
2.3.1.	Općenito	7
2.3.2.	Genealogija tumačenja zaštite osobnih podataka u zakonodavstvu	8
2.3.3.	Ujedinjeni narodi	10
2.3.4.	Vijeće Europe	11
2.3.2.1.	Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda	11
2.3.2.2.	Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108)	14
2.3.5.	Europska unija	15
2.3.4.1.	Povelja Europske unije o temeljnim pravima	15
2.3.5.3.	Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća uredba o zaštiti podataka, GDPR)	17
2.3.6.	Republika Hrvatska	21
2.3.6.1.	Ustav Republike Hrvatske	21
2.3.6.2.	Zakon o provedbi Opće uredbe o zaštiti osobnih podataka (NN br. 42/18)	22
3.	INFORMACIJSKA I KOMUNIKACIJSKA TEHNOLOGIJA	23
3.1.	Općenito	23
3.2.	Utjecaj informacijske i komunikacijske tehnologije na pravo privatnosti	25
3.3.	Profiliranje i bihevioralno oglašavanje	26
3.3.1.	Profiliranje	27

3.3.2. Bihevioralno oglašavanje	29
3.3.3. Pravno uređenje obrade osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja	30
3.3.3.1. Općenito	30
3.3.3.2. Pravna osnova obrade osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja	31
3.3.3.3. Prava ispitanika osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja	36
4. IZAZOVI BUDUĆNOSTI	38
5. ZAKLJUČAK	40
LITERATURA	42

Sažetak: Rad pruža pregled teorija o pojmu i sadržaju prava na privatnost i prava na zaštitu osobnih podataka. Zatim donosi pregled razvoja zakonskog uređenja zaštite tih prava, uz osobit naglasak na Opću uredbu Europske unije o zaštiti osobnih podataka. Razvoj informacijske i komunikacijske tehnologije donosi brojne izazove i rizike za zaštitu ovih prava, a rad posebno razmatra profiliranje i bihevioralno oglašavanje. Zaključno, raspravlja se o stavovima i ponašanjima pojedinaca o zaštiti privatnosti u digitalnoj sferi.

Summary: The paper provides an overview of theories on the concept and content of the right to privacy and the right to the protection of personal data. It then provides an overview of the development of the legal regulation of the protection of these rights, with special emphasis on the General Regulation of the European Union on the protection of personal data. The development of information and communication technology brings numerous challenges and risks for the protection of these rights, and the paper especially considers profiling and behavioral advertising. In conclusion, the attitudes and behaviors of individuals regarding the protection of privacy in the digital sphere are discussed.

Ključne riječi: privatnost, zaštita osobnih podataka, Opća uredba o zaštiti osobnih podataka, informacijska i komunikacijska tehnologija, profiliranje, bihevioralno oglašavanje

Keywords: privacy, personal data protection, General Regulation on Personal Data Protection, information and communication technology, profiling, behavioral advertising

1. UVOD

1.1. Predmet i cilj rada

U ovom radu se analizira pojam i povijesni razvoj zaštite privatnosti i osobnih podataka te izazovi koje otvara korištenje suvremenih tehnologija, s posebnim naglaskom na profiliranje i bihevioralno oglašavanje. Ova tema je posljednjih godina dobila veliku pozornost jer brzi razvoj digitalnih tehnologija neprestano dovodi do novih mogućnosti ugrožavanja temeljnih ljudskih prava i sloboda. U radu će se obrađivati dvije problematike vezane uz ovu temu koje su čest predmet diskursa u javnosti. Unatoč rizicima za privatnost, moderne tehnologije snažno utječu na razvoj suvremenog društva. Obradu osobnih podataka je danas gotovo nemoguće izbjeći te je stoga izrazito važno strogo zakonsko reguliranje te materije. Imajući to u vidu, rad nudi pregled zakonskog uređenja pitanja obrade osobnih podataka u svrhu profiliranja i oglašavanja.

1.2. Izvori podataka i metode prikupljanja

Osim znanstvene i stručne literature, u radu se razmatraju relevantne odredbe Opće uredbe o zaštiti osobnih podataka i drugi dokumenti Europske unije o toj temi, s obzirom na važnost europskog uređenja za hrvatski pravni sustav.

1.3. Sadržaj i struktura rada

Rad je strukturiran u pet glavnih cjelina. U drugoj cjelini razmatramo pojam prava na privatnost i pojam prava na zaštitu osobnih podataka i nudimo kratki pregled različitih pristupa definiranju ovih pojmova. U ovom se poglavlju također prikazuje pravni okvir uređenja prava na privatnost i zaštitu osobnih podataka kroz povijesni razvoj u različitim državama i međunarodnim organizacijama te kroz suvremeno uređenje u Europskoj uniji i Republici Hrvatskoj.

Treća cjelina se bavi izazovima i rizicima koje pred zaštitu privatnosti i osobnih podataka postavlja suvremeni nagli razvoj informacijske i komunikacijske tehnologije. Posebno se razmatra profiliranje i bihevioralno oglašavanje, s obzirom na to da se radi o aktivnostima koje se provode obradom osobnih podataka na globalnoj razini i koje je u današnjem društvu teško izbjeći. Također, u ovom su poglavlju prikazane pravne osnove koje takvi postupci moraju imati da bi bili zakoniti te druge relevantne pravne odredbe koje nude pregled prava korisnika u kontekstu takvih obrada.

U četvrtom poglavlju, nudi se završni osvrt na stanje zaštite privatnosti i osobnih podataka kroz stavove i ponašanja pojedinaca i digitalne ciljeve koje Europska unija postavlja za naredno desetljeće.

2. PRAVO NA PRIVATNOST

2.1. Pojam i sadržaj prava

Društveni poretci moderne zapadne civilizacije njeguju individualizam te osobni i obiteljski privatni život kao osobito važne vrijednosti¹. Privatnost i njena zaštita česte su teme rasprave, kako na međunarodnoj i nacionalnoj zakonodavnoj razini, tako i u svakodnevnom životu u medijima i među pojedincima. Pitanje zaštite privatnosti osobito dobiva na značenju u kontekstu informacijskih i komunikacijskih tehnologija², čije je korištenje sveprisutno i gotovo neophodno u suvremenom društvu. “Tek je u posljednje vrijeme zloupotreba modernih tehnologija osvijetlila značenje i važnost tog subjektivnog prava, a ukazala je i na problem definiranja njegovog sadržaja. Pritisak koji nosi moderni način života čini pravo na privatni život važnijim nego što je to bilo za prethodne generacije.”³

Međutim, nema općeprihvaćene definicije pojma privatnosti, ni suglasnosti u pogledu sadržaja prava na privatnost⁴. Značajnom se smatra definicija američkog profesora prava Westina koji pod pojmom privatnosti smatra “pravo pojedinaca da sami odrede kada, kako i u kojoj mjeri će se informacije o njima priopćiti drugima. U pogledu sudjelovanja pojedinca u društvu, privatnost je dobrovoljno i privremeno fizičko ili psihičko povlačenje pojedinca iz šireg društva u stanje samoće, intimnost manje grupe ili anonimnost i rezerviranost u većim grupama.”⁵ U francuskoj pravnoj teoriji nalazimo da je pravo na privatni život “pravo pojedinca na tajnost života, iz kojeg može isključiti sve ostale osobe te pravo na poštovanje privatnosti njegove osobe.”⁶ Jedna od definicija iz talijanske pravne književnosti privatni život definira kao “bitnu

¹ Dropulić, Julijano, *Pravo na privatni život i društveni integritet*, Zagreb, 2002., str. 45.

² Informacijska i komunikacijska tehnologija (*Information and Communications Technology, ICT*) je djelatnost i oprema koja čini tehničku osnovu za sustavno prikupljanje, pohranjivanje, obradbu, širenje i razmjenu informacija različita oblika, tj. znakova, teksta, zvuka i slike. Začetak predstavlja izum tiskarskog stroja, a procvat doživljava pojavom računala te razvojem mikroelektronike i telekomunikacija. Danas se primjenjuje gotovo u svakoj grani gospodarstva te u svim njegovim glavnim segmentima. Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. Pristupljeno 9. 1. 2022. <<http://www.enciklopedija.hr/Natuknica.aspx?ID=27406>>.

³ Dropulić, *ibid.*, str. 54

⁴ Dragičević, D.; Gumzej, N.; Jurić, M.; Katulić, T.; Lisićar, H.: *Pravna informatika i pravo informacijskih tehnologija*, Narodne Novine, Zagreb, 2015., https://www.pravo.unizg.hr/download/repository/FIN_Cjelovito_poglavlje_5_knjige_PIT%5B3%5D.pdf, str. 2.

⁵ Westin, Alan, *Privacy and Freedom*, Atheneum, New York, 1967, str. 7., navedeno u Brezak, Milan, *Pravo na osobnost*, Nakladni zavod matice Hrvatske, Zagreb, 1998., str. 22.

⁶ Carbonnier, Jean, *Droit civil I*, Pariz, 1965., str. 239, navedeno u Dropulić, *op. cit.* (bilj.1), str. 55.

pretpostavku da netko egzistira kao osoba, a sastoji se od mogućnosti isključenja saznanja trećih onih činjenica koje se odnose isključivo na tu osobu i koje nisu namijenjene drugima.”⁷

Hrvatski pravnik Nikola Gavella navodi: “Pravo na privatnost je osobno neimovinsko pravo, koje osobi daje apsolutnu privatnu vlast glede vođenja vlastitog života te ovlast da svakoga isključi od protupravnog zadiranja u nj”⁸. Osobno, neimovinsko pravo je subjektivno pravo koje pravo priznaje osobi na njenim osobnim, neimovinskim dobrima kao što su život, sloboda, čast i dr.⁹ Gavella dalje iznosi da je to definicija privatnosti u svom najužem smislu, no ponekad se o privatnosti govori i u širem smislu, na način da obuhvaća i neke interese čija je zaštita predmet drugih ljudskih prava, primjerice časti, ugleda, tajnosti pisama i drugih osobnih zapisa, vlastitog lika. Takvu definiciju u širem smislu nalazimo u *Deklaraciji o sredstvima javnog priopćivanja i ljudskim pravima* iz 1970. : “Pravo na poštivanje privatnosti sastoji se prvenstveno u mogućnosti da se živi prema vlastitom nahodjenju uz minimalna uplitanja. Odnosi se na privatni, obiteljski i kućni život, fizički i moralni integritet, čast i ugled, ne predstavljanje pod krivim svjetlom, neobjavljivanje nepotrebnih i neugodnih podataka, neovlašteno objavljivanje privatnih fotografija, na zaštitu od špijunaže i neopravdanih ili neprihvatljivih indiskrecija, na zaštitu od zlonamjernog korištenja privatnih razgovora, na zaštitu od širenja informacija priopćenih ili primljenih od pojedinca u povjerenju.”¹⁰ Gavella zauzima stav da je taj opis ilustrativan, premda ponešto preširok jer nema razgraničenja od drugih ljudskih prava¹¹

U većini navedenih definicija uočavamo da sadržaj prava na privatnost čine dvije komponente: ovlast slobodnog upravljanja osobnim životom i ovlast isključiti treće iz svog privatnog života. Istu podjelu možemo uočiti u različitom razvoju zaštite prava na privatnost u angloameričkoj i europskoj pravnoj praksi. Naime, u pravu SAD-a pojam privatnosti shvaćen je uže nego u europskom pravu te se tumači primarno kao negativna vrijednost koja ograničava uplitanje drugih osoba u privatnu sferu pojedinca.¹² Taj pristup je izražen sintagmom “pravo biti ostavljen na miru” (*right to be let alone*) u smislu u kojem je to izrazio američki vrhovni sudac Louis Brandeis u izdvojenom mišljenju u prvom sudskom slučaju o telefonskom prisluškivanju i povredi prava na privatni život: “Prepoznali su (tvorci američkog Ustava) značaj čovjekove

⁷ Carnelutti, Francesco, *Diritto alla vita privata*, 1995., str. 3., navedeno u Dropulić, op. cit. (bilj.1), str. 55.

⁸ Gavella, Nikola, *Osobna prava*, Pravni fakultet Zagreb, Zagreb 2000., str. 211.

⁹ Ibid., str. 13.

¹⁰ Deklaracija o slobodi izražavanja i informiranja je u Republici Hrvatskoj prihvaćena Zaključcima o prihvaćanju akata Savjeta Europe o slobodi izražavanja i informiranja, NN 7/91.

¹¹ Gavella, op.cit. (bilj. 8.), str. 216.

¹² Jurić, Marko, *Pravo na poštovanje privatnog života i zaštitu osobnih podataka*, u Kregar, Josip et. al., *Ljudska prava: uvod u studij*, Zagreb, 2014., str. 63

duhovne prirode, njegovih osjećaja i njegova intelekta. ... Nastojali su zaštititi Amerikance u njihovim uvjerenjima, njihovim mislima, emocijama i osjećajima. Oni su dodijelili, u odnosu na vladu, pravo biti ostavljen na miru - najopsežnije pravo i pravo koje civilizirani ljudi najviše cijene. Kako bi se zaštitilo to pravo, svako neopravdano zadiranje vlade u privatnost pojedinca, bez obzira na korištena sredstva, mora se smatrati kršenjem Četvrtog amandmana.”¹³ Izrazio je to i sudac T. M. Cooley: “Pravo na vlastitu osobu se može izraziti kao pravo potpunog imuniteta - biti ostavljen na miru.”¹⁴

Drugačiji je slučaj sa zaštitom privatnosti u europskom pravnom krugu gdje se ona ne percipira samo negativno, kao mogućnost pojedinca da se izolira od društva, nego i kao pozitivna vrijednost povezana sa slobodom i autonomijom pojedinca te njegovim pravom na samoodređenje.¹⁵ Kao što je Vrhovni sud SAD-a svojim presudama odlučujuće utjecao na formiranje pojma privatnosti u Americi, tako možemo uočiti i ulogu presuda Europskog suda za ljudska prava (dalje: ESLJP) na području Europe. Iz sljedećeg je primjera očito šire poimanje privatnosti koje obuhvaća i pravo na društvene odnose. “Sud ne smatra mogućim niti potrebnim iscrpno definirati pojam "privatni život". Međutim, bilo bi previše restriktivno ograničiti taj pojam na "unutarnji krug" u kojem pojedinac može živjeti vlastitim osobnim životom kako odabere i od toga potpuno isključiti vanjski svijet koji nije obuhvaćen tim krugom. Poštivanje privatnog života također mora u određenoj mjeri sadržavati pravo na uspostavljanje i razvijanje odnosa s drugim ljudskim bićima.”¹⁶

2.2. Zaštita osobnih podataka

Pravo na zaštitu osobnih podataka nije oduvijek bilo posebno temeljno pravo te se o njemu razmatralo kroz druga ljudska prava, prvenstveno privatnost.¹⁷ Prvi pravni propisi europskog

¹³ Vrhovni sud SAD-a, *Olmstead v. US*, 277 U.S. 438, 1928, <https://www.law.cornell.edu/supremecourt/text/277/438> (10.1.2022.)

¹⁴ Cooley, Thomas M. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*. Chicago, 1879., <https://repository.law.umich.edu/books/11/> (10.1.2022.)

¹⁵ Jurić, loc.cit. (bilj.12.)

¹⁶ ESLJP, *Niemietz v. Germany*, 72/1991/324/396, 1992, <https://www.refworld.org/cases,ECHR,3f32560b4.html> (10.1.2022.)

¹⁷ Bukovac Puvača, Maja; Demark, Armando, *Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede*, 2019., *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*. 40, 287-315., str. 291

prava o pravu na zaštitu osobnih podataka¹⁸ su pravo na zaštitu osobnih podataka shvaćali kao skup posebnih interesa obuhvaćenih širim pojmom privatnosti ili su ju poistovjećivali s pravom na privatnost, kao 'twin-right'.¹⁹

U pravnoj literaturi potkraj dvadesetog stoljeća bilo je uobičajeno shvaćanje da se pravo na privatnost s vremenom razvilo na način da sada uključuje i pravo na zaštitu osobnih podataka.²⁰

U takvoj konceptualnoj modernizaciji je pravo na zaštitu osobnih podataka gledano samo kao jedna od dimenzija privatnosti, i to njena informacijska dimenzija.²¹ Takav se razvoj uzima kao 'povijesna prekretnica u poimanju privatnosti, od tajnosti prema kontroli' ('historical shift: from secrecy to control').²² Smatra se da je ta evolucija privatnosti izravno inspirirana sudskom praksom ESLJP-a, koji je u tumačenje prava na privatnost iz čl. 8. Europske konvencije o ljudskim pravima i temeljnim slobodama, progresivno inkorporirao elemente zaštite osobnih podataka iz Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka iz 1981.²³ Tako je ESLJP u svojoj praksi prepoznao da obrada osobnih podataka ulazi u doseg zaštite privatnog života (Leander protiv Švicarske, 1987; Kopp protiv Švicarske, 1998; Amann protiv Švicarske, 2000).²⁴

Ipak, zaštita osobnih podataka se pokazala kao kompleksna materija, osobito s obzirom da se razvojem tehnologije sve više razvijala i obrada osobnih podataka, što je rezultiralo definiranjem te zaštite kao samostalnog temeljnog prava.²⁵ Pravni teoretičari novijeg doba govore o zaštiti osobnih podataka kao o pravu temeljno različitom od privatnosti, pozivajući se na različitost njihovih ciljeva izraženu terminima "transparentnost" i "neprozirnost". ('transparency vs opacity').²⁶ Cilj zaštite privatnosti je uspostava pravila koja će 'sakriti' pojedince od neopravdanih zadiranja u njihovu privatnost, poput neprozirnog štita, dok je cilj

¹⁸ 'Riječ je o Rezoluciji Vijeća Europe o zaštiti privatnosti pojedinaca u vezi s elektroničkim bankama podataka u privatnom sektoru iz 1973. i Rezoluciji Vijeća Europe o zaštiti privatnosti pojedinaca u vezi s elektroničkim bankama podataka u javnom sektoru iz 1974.', *ibid.* fusnota 25, str. 291.

¹⁹ *ibid.*, str. 291

²⁰ Gonzalez Fuster; Gloria; Gutwirth, Serge, Opening up personal data protection: a conceptual controversy, *Computer Law & Security Review*, 2013, vol. 29, 531-539, str. 8.

²¹ *ibid.*

²² *ibid.*

²³ *ibid.*, str. 8, bilj. 47.

²⁴ Jurić, op. cit. (bilj. 12), str. 68.

²⁵ *ibid.*

²⁶ Gonzalez; Gutwirth, op. cit. (bilj. 20), str. 9.

zaštite osobnih podataka pojačati transparentnost obrade osobnih podataka, učiniti ju vidljivijom, propisivanjem kakva ona mora biti da bi bila zakonita.²⁷

Postoje dvije različite konceptualizacije prava na zaštitu osobnih podataka: prohibitivna i permisivna.²⁸ Po prohibitivnoj koncepciji je obrada osobnih podataka u principu zabranjena, a dozvoljena je iznimno ako su ispunjeni određeni uvjeti.²⁹ Struktura prava je binarna, sastoji se od zabrane uparene s vrlo specifičnim uvjetima za ukidanje te zabrane.³⁰ Srž prava na zaštitu osobnih podataka je preskriptivna jer se radi o pukoj zabrani uz iznimke za njeno ograničenje.³¹ S druge strane, po permisivnoj koncepciji je obrada osobnih podataka dozvoljena pod određenim uvjetima.³² Ovdje uvjeti nisu iznimke nego dio samog prava, i to njegove supstancijalne komponente.³³ Struktura prava je jedinstvena jer su baš ti uvjeti preduvjet za poštivanje samog prava, stoga je ovdje srž prava afirmativna.³⁴ Korijene različitog razumijevanja sadržaja prava na zaštitu osobnih podataka možemo uočiti u povijesti zakonodavstva o zaštiti osobnih podataka, o čemu će biti riječi u sljedećem poglavlju.

2.3. Pravni okvir zaštite privatnosti i osobnih podataka

2.3.1. Općenito

Zakonodavna djelatnost na području komunikacijske i informacijske privatnosti počinje od sedamdesetih godina prošlog stoljeća. Zaštita podataka u Europi započela je kada su u nekim državama doneseni propisi vezani za regulaciju obrade osobnih podataka koju provode javna tijela i velika društva.³⁵ Njemačka savezna država Hessen donijela je 1970. prvi zakon o zaštiti podataka, koji se primjenjivao samo u toj saveznoj državi, a prvi nacionalni zakon o zaštiti

²⁷ *ibid.*

²⁸ *ibid.*, str. 2.

²⁹ *ibid.*

³⁰ *ibid.*, str. 3.

³¹ *ibid.*, str. 2.

³² *ibid.*, str. 3.

³³ *ibid.*

³⁴ *ibid.*

³⁵ Priručnik o europskom zakonodavstvu o zaštiti podataka, str. 20. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_hr.pdf, 2.2.2022.,

podataka donijela je Švedska 1973. Do kraja 1980-ih nekoliko je europskih država (Francuska, Njemačka, Nizozemska i Ujedinjena Kraljevina) također donijelo zakone o zaštiti podataka.³⁶

U tom su procesu vidljiva dva različita pristupa regulaciji: opći i područni pristup.³⁷ Države koje su regulaciji pristupile opće, su donijele jedan zakon o cijeloj materiji zaštite osobnih podataka temeljenog na Smjernicama OECD-a o zaštiti privatnosti i prekograničnog protoka osobnih podataka iz 1980. i Konvenciji o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (dalje: Konvencija br. 108) Vijeća Europe iz 1981.³⁸ Osim europskih zemalja, takvim su se pristupom vodile i Australija, Novi Zeland, Hong Kong i Kanada. Karakteristike ovog pristupa su stroga pravila o prikupljanju, obradi i prijenosu podataka i povjerenik (ombudsman) koji brine o provođenju zakona. Ipak nije isključeno donošenje posebnih propisa za specifična područja.³⁹ Nasuprot tome, u SAD-u se zaštiti pristupilo područno, što je karakterizirano donošenjem posebnih zakona za posebna područja ili djelatnosti za koje se smatra da mogu osobito ugroziti privatnost i osobne podatke, te nepostojanje posebnog javnog službenika koji bi nadgledao provođenje zakona.⁴⁰ Osim zakonodavne aktivnosti država i međunarodnih organizacija, možemo govoriti o samoregulaciji kao uspostavljanju pravila ponašanja i standarda koje mogu donijeti tvrtke, udruženja proizvođača, davatelji usluga te udruge kupaca i drugih korisnika usluga.⁴¹ Osobito bitna je tehnička samopomoć koja obuhvaća korištenje kriptografskih proizvoda, usluga za anonimnost korisnika i besplatnih programa za zaštitu privatnosti.⁴²

2.3.2. Genealogija tumačenja zaštite osobnih podataka u zakonodavstvu

Prvi zakon o zaštiti osobnih podataka bio je *Hessische Datenschutzgesetz* iz 1970. godine kojim je njemačka pokrajina Hessen regulirala pitanje informacija pohranjenih tijekom automatizirane obrade.⁴³ Taj zakon definira pojam *Datenschutz* kao obvezu da podaci u bazama

³⁶ *ibid.*, str. 20., fusnota 2

³⁷ Dragičević et. al., *op.cit.* (bilj. 4), str. 14.

³⁸ v. *infra*

³⁹ Dragičević et. al., *op.cit.* (bilj. 4), str. 14.

⁴⁰ *ibid.*

⁴¹ *ibid.*

⁴² *ibid.*

⁴³ Brezak, Milan, *Pravo na osobnost*, Nakladni zavod Matice Hrvatske, Zagreb, 1998., str. 82.

podataka i rezultati obrade tih podataka budu pribavljeni, prenošeni i pohranjeni na način da ne mogu biti dostupni, mijenjani, vađeni ili uništeni od strane neovlaštene osobe.⁴⁴ Taj je pojam kasnije korišten u njemačkom pravu kako bi označio regulaciju korištenja podacima pohranjenim u bazama podataka.⁴⁵ Zakon je bio temeljen na principu ‘confidentiality by default’ pri čemu je obrada podataka iznimka, a ne pravilo.⁴⁶ Pravilo je da je obrada podataka zabranjena, dakle radilo se o prohibitivnoj zaštiti.⁴⁷ Ista je koncepcija u prvom njemačkom federalnom zakonu o zaštiti osobnih podataka, *Bundesdatenschutzgesetz* iz 1977. godine.⁴⁸ Obrada osobnih podataka je generalno zabranjena, uz široke iznimke.⁴⁹ Isto u austrijskom zakonu iz 1978. godine koji izjednačuje zaštitu osobnih podataka s tajnošću osobnih podataka.⁵⁰ Do redefinicije srži zaštite osobnih podataka u Njemačkoj dolazi putem sudske prakse.⁵¹ Njemački ustavni sud je 1983. iznio novu ideju o pravu na informacijsko samoodređenje (*informationelle Selbstbestimmung, informational self determination*) po kojoj se tijekom cijele obrade osobnih podataka moraju uzimati u obzir prava pojedinaca, s obzirom da bi im obradom mogle biti ugroženo dostojanstvo i sloboda.⁵² ‘Zbog toga slobodan razvoj osobe u uvjetima automatske obrade osobnih podataka podrazumijeva zaštitu pojedinca protiv neograničena prikupljanja, pohranjivanja, uporabe i priopćavanja osobnih podataka. ... Temeljno pravo jamči svakome ovlaštenje odlučiti o uporabi osobnih podataka koji se na njega odnose.’⁵³ Odluka se odnosila na popis stanovništva kao najtemeljitiji instrument države za prikupljanje osobnih podataka.⁵⁴ Sud kao glavne elemente prava na zaštitu osobnih podataka utvrđuje strogo ograničenje svrhe korištenja osobnih podataka i zabranu korištenja podataka koja su inkompatibilna s originalnom svrhom prikupljanja podataka.⁵⁵ Ovakvo tumačenje zaštite pretpostavlja obradu osobnih podataka, dakle radi se o usvajanju permisivnog koncepta.

S druge strane, u SAD-u je regulacija automatizirane obrade osobnih podataka promatrana kroz pojam kontrole nad osobnim informacijama, a ta ideja kontrole je podrazumijevala afirmativna

⁴⁴ Gonzalez et al., loc. cit. (bilj. 20), str. 4.

⁴⁵ ibid.

⁴⁶ ibid.

⁴⁷ ibid.

⁴⁸ Brezak, op. cit. (bilj. 36.), str. 83.

⁴⁹ Gonzalez et al., loc. cit. (bilj. 20), str. 5.

⁵⁰ Brezak, op. cit. (bilj. 36.), str. 85.

⁵¹ Gonzalez et al., loc. cit. (bilj. 20), str. 6.

⁵² ibid., str. 6.

⁵³ Odluka Saveznog ustavnog suda (BVerfG), broj 65, 1(40), NJW, broj 8, Frankfurt, 1984, str. 419 u Brezak, loc. cit. (bilj. 36), str. 57.

⁵⁴ Brezak, str. 56.

⁵⁵ Gonzalez et al., loc. cit. (bilj. 20), str. 6.

prava.⁵⁶ Stoga je usvojena doktrina *fair information practices* koja je utvrđivala što mora biti učinjeno kod obrade osobnih podataka, za razliku od zabrane obrade.⁵⁷ Ta je doktrina formalno inkorporirana u američko pravo kada je donesen *Privacy Act* 1974.⁵⁸

Drugi primjer permisivne koncepcije zaštite osobnih podataka nalazimo u francuskom zakonu. Objekt zakona nisu osobni podaci, nego sama obrada i za koju propisuje uvjete, što podrazumijeva da je obrada dozvoljena.⁵⁹ Iznimno je zabranjena obrada nekih kategorija osobnih podataka koji se odnose na rasno ili etničko podrijetlo, političku, filozofsku ili religijsku orijentaciju, članstvo u sindikatu, zdravlje ili seksualni život.⁶⁰ Ova je odredba kasnije inspirirala kategoriju 'osjetljivih podataka'.⁶¹

Prevlast permisivne koncepcije zaštite osobnih podataka u međunarodnom pravu, a indirektno i u nacionalnim pravima država stranaka, nastupa donošenjem Konvencije Vijeća Europe o zaštiti i pojedinaca pri automatskoj obradi osobnih podataka 1981. (Konvencija br. 108) u kojoj je pravo na zaštitu osobnih podataka uređeno pravilima duboko utemeljenim na *fair information practices* doktrini.⁶²

2.3.3. Ujedinjeni narodi

U okviru međunarodnih organizacija, pravo na privatnost utvrđeno je u čl. 12. Opće deklaracije UN-a o ljudskim pravima iz 1948.: "Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada."⁶³ Deklaracija je neobvezujući dokument, no u okviru UN-a je Međunarodnim paktom o građanskim i političkim pravima iz 1976. propisana obveza zemalja potpisnica da poštuju i jamče u njemu utvrđena građanska prava, među kojima je i pravo na privatnost: "Nitko ne smije biti podvrgnut

⁵⁶ Miller, Arthur, *The Assault on Privacy*, 1972, u Gonzalez et al., loc. cit. (bilj. 20.), str. 5.

⁵⁷ Gonzalez et al., loc. cit. (bilj. 20.), str. 5.

⁵⁸ ibid.

⁵⁹ ibid., loc. cit. (bilj. 20.), str. 5.

⁶⁰ *Loi informatique et libertés*, 1978, čl. 8., u Gonzalez et al., loc. cit. (bilj. 20.), str. 5.

⁶¹ Gonzalez et al., loc. cit. (bilj. 20.), str. 5.

⁶² ibid.

⁶³ Opća deklaracija o ljudskim pravima, rezolucija br. 217 /III, čl. 12.

samovoljnom ili nezakonitom miješanju u njegov privatni život, obitelj ili dopisivanje, niti nezakonitim napadima na njegovu čast ili ugled.”⁶⁴

Opća skupština UN-a je 2013. godine donijela rezoluciju o pravu na privatnost u digitalnom dobu, potaknuta razvojem digitalnih tehnologija i objavom informacija zviždača Edwarda Snowdena o masovnom nadzoru koji su provodile obavještajne agencije. Rezolucija je kasnije više puta revidirana. Uvažavajući globalnu i otvorenu narav Interneta i brzi razvoj informacijskih i komunikacijskih tehnologija kao pokretačke sile bržeg napretka, potvrđuje da ljudska prava koja su ljudima zajamčena ‘offline’, moraju također biti zaštićena ‘online’, osobito pravo na privatnost.⁶⁵ Pozivaju se države članice da poštuju i štite pravo na privatnost u kontekstu digitalnih komunikacija te da ponovno razmotre svoju praksu i zakonodavstvo o nadzoru i presretanju komunikacija, osobito o masovnom nadzoru te o prikupljanju osobnih podataka kako bi osigurale potpunu implementaciju svih međunarodnih obaveza o zaštiti ljudskih prava.⁶⁶ Osim osude masovnog nadzora, rezolucije su potaknule političku raspravu koja je dovela do imenovanja posebnog izvjestitelja UN-a za pitanja prava na privatnost s posebnim zadacima prikupljanja informacija o nacionalnim praksama i izazovima, te utvrđivanja najboljih praksi i preporuka.⁶⁷ Revidiranom rezolucijom iz 2016. je dodano da se pozivaju i privatna poduzeća na odgovornost za poštivanje ljudskih prava i potiče ih se da obavještavaju korisnike o prikupljanju, korištenju, dijeljenju i zadržavanju njihovih podataka koje bi moglo utjecati na pravo na privatnost te da uspostave transparentna pravila.⁶⁸

2.3.4. Vijeće Europe

2.3.2.1. Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda

Pravo na poštovanje privatnog i obiteljskog života je uređeno u Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda (dalje: EKLJP), donesenoj 1950. godine u okviru Vijeća

⁶⁴ Međunarodni pakt o građanskim i političkim pravima, rezolucija br. 2200 A /XXI, čl. 17.

⁶⁵ Rezolucija o pravu na privatnost u digitalnom dobu, A/RES/68/167, 2013., str. 2.

⁶⁶ Revidirani nacrt Rezolucije o pravu na privatnost u digitalnom dobu, A/C.3/69/L.26/Rev. 1, 2014., str. 4.

⁶⁷ Priručnik o europskom zakonodavstvu o zaštiti podataka, https://www.echr.coe.int/documents/handbook_data_protection_hrv.pdf, (1.6.2022.), str. 24.

⁶⁸ Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/ Rev. 1, New York, 16. studenoga 2016

Europe, na sljedeći način: “Svatko ima pravo na poštovanje svog privatnog i obiteljskog života, doma i dopisivanja.⁶⁹ Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih. (čl. 8., st. 1. EKLJP)”⁷⁰

Dakle javna vlast može ograničiti pravo na poštivanje privatnog života ako to ograničenje kumulativno ispunjava tri uvjeta: zakonito je, služi ostvarenju legitimnog cilja i nužno je u demokratskom društvu.⁷¹ Ograničenje je zakonito ako se temelji na pravnoj osnovi, koja mora pojedincima biti dostupna i iz koje mogu razumno predvidjeti posljedice svog ponašanja te ako imaju na raspolaganju pravno sredstvo protiv takvih ograničenja.⁷² Zatim, ograničenje mora služiti ispunjavanju nekog od taksativno navedenih legitimnih ciljeva: državna sigurnost, javni red i mir, gospodarska dobrobit zemlje, sprječavanje nereda ili zločina, zaštita zdravlja ili morala te zaštita prava i sloboda drugih.⁷³ I na kraju, ograničenje mora biti nužno u demokratskom društvu, što znači da za njim mora postojati ‘prijeka društvena potreba’.⁷⁴ Kod utvrđivanja nužnosti je važno paziti na ravnotežu između interesa države i prava podnositelja zahtjeva.⁷⁵ Važno je da ograničenje poštuje načelo razmjernosti te da se pravo ograničava samo koliko je nužno za ostvarenje legitimnog cilja.⁷⁶

Posebnost članka 8. EKLJP se očituje u tome što on ne jamči pravo na privatni život, obitelj, dom ili dopisivanje, nego definira pravo na ‘poštovanje’ navedena četiri specifična interesa.⁷⁷ Države članice su u početku tumačile ‘poštovanje’ kao negativnu obvezu nezadiranja u prava pojedinca.⁷⁸ Međutim ESLJP nije prihvatio takvo tumačenje te je na tom primjeru prvi puta utvrdio koncept pozitivne konvencijske obveze.⁷⁹ Tako u presudi Marckx protiv Belgije iz

⁶⁹ Konvencija za zaštitu ljudskih prava i temeljnih sloboda, MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, čl. 8. st. 1.

⁷⁰ EKLJP, čl. 8. st. 1. i 2.

⁷¹ Jurić, op. cit. (bilj. 12.), str. 69.

⁷² ibid.

⁷³ ibid., str. 70.

⁷⁴ ibid.

⁷⁵ Vodič kroz članak 8. Konvencije – Pravo na poštovanje privatnog i obiteljskog života, 2020. <https://uredzastupnika.gov.hr/UserDocsImages/dokumenti/Edukacija/Vodi%C4%8D%20kroz%20%C4%8Dlana k%208.%20Konvencije.pdf>, str. 11.

⁷⁶ ibid.

⁷⁷ Batistić Kos, Vesna, Pozitivne obveze prema Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda, Narodne novine, Zagreb, 2012., str. 203.

⁷⁸ ibid., str. 206.

⁷⁹ ibid., str. 207.

1979.: 'Sud nadalje potvrđuje da, dok je temeljni predmet članka 8. zaštita pojedinaca od arbitrarnog miješanja od strane javnih vlasti, on se ne zaustavlja samo na zahtjevu da se država suzdrži od takvog miješanja. Dodatno na takvo negativno poduzimanje, može postojati pozitivna obveza inherentna u učinkovitom poštovanju privatnog i obiteljskog života.'⁸⁰

Za razliku od navedenog tumačenja 'poštovanja', sam predmet te obveze nije precizno definiran pa se opseg pojedinog interesa definira pomoću smjernica iz sudske prakse, koje su utvrđivane od slučaja do slučaja.⁸¹ U kontekstu prava na privatni život, opseg prava obuhvaća najrazličitije interese pojedinaca, povezane i s drugim ljudskim pravima kao što su dostojanstvo i sloboda, a koji zajedno predstavljaju izvorne vrijednosti slobodnog društva.⁸² Prema sudskoj praksi, ti interesi obuhvaćaju: fizički i moralni integritet osobe (X i Y protiv Nizozemske, 1985 gdje napadnutoj osobi nije pružena adekvatna zaštita od strane zakonodavstva; Wainwright protiv Ujedinjenog kraljevstva, 2006. gdje je osoba skinuta do gola tijekom pretraživanja pri zatvorskom posjetu; Y.F. protiv Turske, 2003. gdje je žena prisilno podvrgnuta ginekološkom pregledu; Glass protiv Ujedinjenog kraljevstva, 2004. i Storck protiv Njemačke, 2006, gdje su osobama davani lijekovi bez pristanka; Brüggemann i Scheuten protiv Njemačke, 1976., Tysiąc protiv Poljske, 2007. o pravu na pobačaj), fizički i društveni identitet pojedinca (Mikulić protiv Hrvatske, 2002. o pravu djeteta na saznanje vlastitog podrijetla; Shofman protiv Rusije, 2005. o pravu muškarca na utvrđivanje da nije otac djeteta; Burghartz protiv Švicarske, 1994 i Guillot protiv Francuske, 1996. o pravu na izbor prezimena odnosno imena), uključujući seksualni identitet (B protiv Francuske, 1994 gdje je ženi uskraćeno posvojenje zbog seksualne orijentacije), pravo na osobni razvoj i ispunjenje, pravo na sakupljanje i korištenje informacija (Gaskin protiv Ujedinjenog Kraljevstva, 1989. gdje je osobi uskraćen pristup podacima o obiteljima pod čijom je skrbi bio kao maloljetnik; X protiv Hrvatske, 2008. gdje majka lišena poslovne sposobnosti nije bila obaviještena o postupku posvojenja svoga djeteta), seksualni život (Smith i Grady protiv Ujedinjenog kraljevstva, 1999. gdje su vojnici otpušteni iz službe zbog homoseksualnog života), društveni život i odnosi u smislu prava na odnose s drugim ljudskim bićima u vanjskom svijetu (Silvenko protiv Latvije, 2003. gdje je osoba prisiljena napustiti svoju državu).⁸³

⁸⁰ Marckx protiv Belgije, A31 (1979) u Batistić Kos, loc. cit. (bilj. 43)

⁸¹ Batistić Kos, op. cit. (bilj. 70), str. 203.

⁸² ibid., str. 204.

⁸³ Sistematizacija prema Jurić, op. cit. (bilj.12.), str. 64., 65., 66. i 67. i Batistić Kos, op. cit. (bilj. 70.), str. 204 i bilješke 591, 592, 593, 594

Države potpisnice EKLJP su obvezne poštovati ju u izvršavanju svih svojih aktivnosti i ovlasti te su bile dužne ugraditi ili provesti EKLJP u svoja nacionalnim zakonodavstvima.⁸⁴ U Europskoj uniji, pitanja nacionalne sigurnosti ne podliježu aktima te organizacije, no to nije slučaj s Vijećem Europe.⁸⁵ Stoga su države stranke Konvencije dužne poštovati ju i u aktivnostima o nacionalnoj sigurnosti. Nadzor nad izvršavanjem konvencijskih obveza provodi Europski sud za prava čovjeka (dalje: ESLJP).⁸⁶ Pojedinci su donošenjem Protokola uz EKLJP iz 1998. dobili široka prava obraćanja Sudu, pa tako to može učiniti svaki pojedinac, država stranka EKLJP, nevladina organizacija ili pravna osoba ako smatra da su joj prekršena konvencijskih prava.⁸⁷ Pojedinci to pravo imaju prema svim državama strankama EKLJP, to više ne ovisi o prihvatu države sudbenosti ESLJP-a, ni o državljanstvu pojedinca.⁸⁸ Međutim prije toga je potrebno iscrpiti sva raspoloživa domaća pravna sredstva.⁸⁹ Stoga je to sudski nadzor supsidijarnog karaktera, jer je i provođenje i nadzor prvenstveno odgovornost države te se računa na njihovo aktivno djelovanje za zaštitu konvencijskih prava.⁹⁰

2.3.2.2. Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108)

Jedini međunarodnopravno obvezujući pravni akt s temeljnim načelima zaštite osobnih podataka je *Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka* (dalje Konvencija br. 108) iz 1981. godine.⁹¹ Republika Hrvatska ju je potpisala 2003. godine, a ratificirala 2005. godine zajedno s *Dodatnim protokolom u vezi nadzornih tijela i međunarodne razmjene podataka*.⁹² Konvencija br. 108 primjenjuje se na svaku obradu podataka u privatnom i u javnom sektoru te štiti pojedince od zlouporaba prilikom obrade osobnih podataka i regulira prekogranične prijenose osobnih podataka.⁹³ Konvenciji br. 108 mogu pristupiti i države koje

⁸⁴ Priručnik o europskom zakonodavstvu o zaštiti podataka op..cit. (bilj. 28.), str. 25.

⁸⁵ v. infra

⁸⁶ Andrassy, Juraj; Seršić, Maja, Vukas, Branimir, Međunarodno pravo 1, Školska knjiga, Zagreb, str. 391

⁸⁷ ibid, str. 392.

⁸⁸ ibid.

⁸⁹ ibid.

⁹⁰ Batistić Kos, op. cit. (bilj. 70), str. 10

⁹¹ Dragičević et al., op. cit. (bilj. 4.), str. 16

⁹² Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola; NN MU 4/2005

⁹³ Priručnik o europskom zakonodavstvu o zaštiti podataka, op. cit. (bilj. 28.), str. 26.

nisu članice Vijeća Europe⁹⁴, a zbog takvog otvorenog karaktera i potencijala da služi kao univerzalni standard, predstavlja temelj globalnog promicanja zaštite podataka.⁹⁵ Konvencija br. 108 je modernizirana i dopunjena donošenjem Protokola o izmjeni 2018. godine.⁹⁶ Hrvatska ga je unijela u svoje zakonodavstvo 2019. godine.⁹⁷

Konvencija br. 108 uređuje način postupanja s osobnim podacima koji su predmet automatizirane obrade na sljedeći način: moraju biti pribavljeni zakonito i u dobroj vjeri, pohranjeni u određene i zakonite svrhe te ne smiju biti uporabljani na način nespojiv s tim svrhama, moraju biti odgovarajući, mjerodavni i ne suvišni u odnosu na svrhe u koje su pohranjeni, moraju biti točni i ažurni te sačuvani u obliku koji omogućuje identifikaciju subjekata podataka tijekom razdoblja koje nije duže nego što to nalaže svrha u koju su pohranjeni.⁹⁸ Također, posebne kategorije podataka ne mogu se uopće automatizirano obrađivati ako unutarnje pravo ne predviđa primjerenu razinu zaštite.⁹⁹ Takvi posebni osobni podaci su oni koji otkrivaju rasno podrijetlo, politička mišljenja, vjerska ili druga uvjerenja ili se tiču zdravlja ili spolnog života, kao i oni koji se odnose na kaznene presude.¹⁰⁰ Također propisuje iznimke i ograničenja navedenih prava kada je to predviđeno pravom stranke i ako je nužno u demokratskom društvu za zaštitu državne sigurnosti, javne sigurnosti, monetarnih interesa države ili suzbijanja kaznenih djela ili pak zaštite subjekta podataka ili prava i slobode drugih.¹⁰¹

2.3.5. Europska unija

2.3.4.1. Povelja Europske unije o temeljnim pravima

⁹⁴ Do sada je 51 zemlja potpisala Konvenciju br. 108. Među njima su sve države članice Vijeća Europe (47 zemalja), Urugvaj (prva neeuropska zemlja koja je pristupila Konvenciji), 2013., te Mauricijus, Senegal i Tunis, 2016. i 2017., *ibid.*

⁹⁵ *ibid.*, str. 28.

⁹⁶ *ibid.*, str. 19.

⁹⁷ Zakon o potvrđivanju Protokola kojim se mijenja i dopunjuje Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, NN 8/2019

⁹⁸ Rajko, Alen, *Informacijsko upravno pravo*, TEB poslovno savjetovanje, Zagreb, 2011., str. 122.

⁹⁹ *ibid.*

¹⁰⁰ *ibid.*

¹⁰¹ *ibid.*

Povelja Europske unije o temeljnim pravima (dalje: Povelja EU)¹⁰² utvrđuje poštovanje privatnog i obiteljskog života u čl. 7: ‘Svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja.’ Povelja također utvrđuje zaštitu osobnih podataka kao samostalno temeljno pravo u čl. 8. st. 1.: ‘Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose.’ U vezi zaštite osobnih podataka Povelja dalje propisuje: ‘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. Poštovanje tih pravila podliježe nadzoru neovisnog tijela’¹⁰³

Pod zaštitom Povelje su temeljna prava svakog pojedinca u Europskoj uniji, čime su umanjene potencijalne opasnosti za zaštitu prava koje proizlaze iz različitih interpretacija prava na privatnost i prava na zaštitu osobnih podataka među državama članicama.¹⁰⁴ Neovisno kako neka država članica tumači tu materiju, njeni se državljani i pred nacionalnim sudovima od tada mogu pozvati na Povelju.¹⁰⁵ Naime europski zakonodavac je zbog izrazite važnosti tih prava, odlučio unificirati regulaciju te bi se moglo reći da je time pravo na zaštitu osobnih podataka potpuno „europizirano“.¹⁰⁶ Za jedinstveno tumačenje i primjenu prava Europske unije zadužen je Sud Europske unije osnovan 1952. godine sa sjedištem u Luksemburgu.¹⁰⁷

Povelja unosi dvije temeljne promjene u pravo EU: uvodi pojam ‘zaštite osobnih podataka’ nasuprot ‘zaštiti podataka’¹⁰⁸ i utvrđuje pravo na zaštitu osobnih podataka kao zasebno temeljno pravo, odvojeno od privatnosti.¹⁰⁹ Posljednja glava Povelje donosi opće odredbe o tumačenju i primjeni Povelje.¹¹⁰ Primjerice u članku 52. se utvrđuje opseg i tumačenje prava i načela Povelje: ‘Svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju

¹⁰² Povelja Europske unije o temeljnim pravima (2016/C 202/02)

¹⁰³ Povelja EU, čl. 8. st. 2. i 3.

¹⁰⁴ Bukovac; Puvača, op. cit. (bilj. 17), str. 293

¹⁰⁵ *ibid.*

¹⁰⁶ *ibid.*

¹⁰⁷ Sud Europske unije, <http://www.vsrh.hr/EasyWeb.asp?pcpid=1050>, (1.6.2022.)

¹⁰⁸ Terminološka razlika je uočljivija u nekim drugim europskim jezicima, npr. njemačkom (*Schutz personenbezogener Daten* umjesto *Datenschutz*) ili švedskom (*Skydd av personuppgifter* umjesto *Dataskydd*), Gonzalez, op. cit. (bilj. 20), str. 7., bilj. 39.

¹⁰⁹ *ibid.*

¹¹⁰ Povelja EU, glava VII

ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.¹¹¹

2.3.5.3. Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća uredba o zaštiti podataka, GDPR)

Najvažniji izvor EU za zaštitu osobnih podataka je *Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ* (Opća uredba o zaštiti podataka, GDPR).¹¹² Opća uredba se počinje primjenjivati od 25. svibnja 2018. godine kada je zamijenila *Direktivu 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o njihovom slobodnom protoku*.¹¹³ Za razliku od te Direktive, Opća uredba je horizontalni izvor prava zaštite osobnih podataka, što znači da je potpuno obvezujuća i da se izravno primjenjuje u svim državama članicama.¹¹⁴ Namjera je novih pravila maksimalno ujednačiti dotadašnja pravna pravila domaćih zakonodavstava, koja su se temeljem Direktive mogla znatno razlikovati. Također, iz načina na koji je uređeno teritorijalno područje primjene Uredbe proizlazi potencijalni globalni učinak njenih odredaba, osobito za pitanja online poslovanja gdje su predmet obrade osobni podaci građana EU.¹¹⁵

Naime, 'teritorijalno područje primjene Opće uredbe obuhvaća obradu osobnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne, ali i obradu osobnih podataka ispitanika u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji'.¹¹⁶ Uvjet za potonje je da su aktivnosti obrade povezane s nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje, ili praćenjem njihova ponašanja, dokle god se njihovo ponašanje odvija unutar Unije.¹¹⁷ Na zaključak da voditelj ili izvršitelj obrade

¹¹¹ Povelja čl. 52, st. 1.

¹¹² Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119/1

¹¹³ Direktiva 95/46/EZ europskog parlamenta i vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281/31

¹¹⁴ Gumzej, Nina, Uredba o zaštiti osobnih podataka, 2017., projekt "Novi hrvatski pravni sustav" Pravnog fakulteta Sveučilišta u Zagrebu, str. 2.

¹¹⁵ ibid.

¹¹⁶ GDPR, čl. 3., st. 1. i 2.

¹¹⁷ ibid.

namjerava ponuditi usluge ispitanicima koji se nalaze u jednoj ili više država članica Unije, izvjesno upućuju okolnosti poput korištenja jezikom ili valutom koji su općenito u uporabi u jednoj ili više država članica s mogućnošću naručivanja robe i usluga na tom drugom jeziku, ili spominjanje kupaca ili korisnika koji se nalaze u Uniji.¹¹⁸ Međutim nije dovoljna puka dostupnost internetskih stranica voditelja obrade, izvršitelja obrade ili posrednika u Uniji ili adrese elektroničke pošte i drugih kontaktnih podataka ili korištenje jezikom koji je općenito u uporabi u trećoj zemlji u kojoj voditelj obrade ima poslovni nastan.¹¹⁹ Na taj je način europski pravni okvir zaštite osobnih podataka u velikoj mjeri proširen.¹²⁰ Opća uredba se primjenjuje i na obradu osobnih podataka koju obavlja voditelj obrade koji uopće nema poslovni nastan u Uniji, nego na mjestu gdje se pravo neke države članice primjenjuje na temelju međunarodnog javnog prava (npr. u diplomatskom ili konzularnom predstavništvu).¹²¹

'Materijalno područje primjene Opće uredbe obuhvaća obradu osobnih podataka koja se u cijelosti obavlja automatizirano te neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.'¹²² Opća uredba sadrži definicije pojmova važnih za tumačenje njenog polja primjene. Tako definira osobne podatke kao 'sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi odnosno osobu koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.'¹²³ Novine koje uvodi ova Opća uredba su uvođenje pojma mrežnog identifikatora u definiciju osobnog podatka te, u daljnjem tekstu, po prvi put zakonsko definiranje i uređenje genetskih i biometrijskih podataka kao osobnih podataka.¹²⁴ 'Genetski podaci predstavljaju osobne podatke koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca'¹²⁵, a biometrijski podaci su osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima,

¹¹⁸ *ibid.*, recital 23.

¹¹⁹ *ibid.*

¹²⁰ Gumzej, op. cit. (bilj. 106), str. 14.

¹²¹ *ibid.*, str. 22.

¹²² GDPR, čl.2. st.1.

¹²³ *ibid.*

¹²⁴ Čizmić, Jozo; Boban, Marija, Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 377-410 (2018), str. 382.

¹²⁵ GDPR., čl. 4., st. 13.

fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.¹²⁶ Je li moguće utvrditi identitet pojedinca iz određenog podatka procjenjuje se s obzirom na sva sredstva koja voditelj obrade ili bilo koja druga osoba mogu za to upotrijebiti, a je li izgledno da se ta sredstva zaista upotrebljavaju za identifikaciju, prosuđuje se s obzirom na objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, tehnologija dostupna u vrijeme obrade i tehnološki razvoj.¹²⁷ Time je kodificiran relativni kriterij razumnog korištenja iz mišljenja nezavisnog odvjetnika u predmetu Breyer pred Sudom EU.¹²⁸

Po Općoj Uredbi, 'obrada osobnih podataka je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.'¹²⁹ Definicija je otvorena i samo primjerice navodi slučajeve obrade, jer bi se taksativnim navođenjem omogućilo zaobilazanje odredaba i otežala prilagodljivost tehnološkom razvoju.¹³⁰ Neautomatizirana je ona obrada koju provode samo ljudi, bez upotrebe tehnoloških pomagala, a automatizirana obrada se provodi automatiziranim tehnologijama.¹³¹ Da bi neautomatizirana obrada osobnih podataka bila pokrivena Općom uredbom, mora biti dio nekog sustava pohrane.¹³² Po Općoj uredbi, to je strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, koji mogu biti centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.¹³³ Što se tiče, automatizirane obrade, posebno je istaknuta izrada profila. Definirana je kao 'svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima,

¹²⁶ *ibid.*, čl. 4, st. 14.

¹²⁷ *ibid.*, recital. 26.

¹²⁸ Mišljenje Nezavisnog odvjetnika Manuela Camposa Sanchez-Bordone od 12. svibnja 2016. u predmetu C-582/14, Breyer, EU:C:2016:339, para.68.

¹²⁹ GDPR, čl. 4., st. 2.

¹³⁰ Mišćenić, Emilia; Kunda, Ivana; Petrić, Silvija; Butorac Malnar, Vlatka; Vrbljanac, Danijela; Winkler, Sandra, *Europsko privatno pravo - posebni dio*, Školska knjiga, Zagreb, 2021., str. 294.

¹³¹ *ibid.*

¹³² *ibid.*

¹³³ GDPR, čl. 4., st. 6.

interesima, pouzdanosti, ponašanjem, lokacijom ili kretanjem tog pojedinca.¹³⁴ Takva obrada omogućava automatizirano pojedinačno donošenje odluka, tehnološkim putem bez sudjelovanja ljudi, što u nekim društvenim aspektima pojedincima nije poželjno.¹³⁵

Opća uredba, kao akt EU, se ne primjenjuje na obradu osobnih podataka tijekom aktivnosti koje izlaze iz opsega prava EU, poput nacionalne sigurnosti, ni na obradu koju obavljaju države članice u aktivnostima povezanim sa zajedničkom vanjskom i sigurnosnom politikom EU (glava V, poglavlje 2, *Ugovora o Europskoj uniji*).¹³⁶ Također, pojedina područja su uređena pravnim aktima EU koji posebno uređuju ta područja te stoga ne ulaze u polje primjene Opće Uredbe, primjerice *Direktiva 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*¹³⁷, zatim *Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka*¹³⁸. Međutim, iako je i *Direktiva o privatnosti i elektroničkim komunikacijama*¹³⁹, takav posebni akt, Opća uredba se primjenjuje na sva pitanja zaštite temeljnih prava i sloboda u obradi osobnih podataka koja nisu uređena posebnim obvezama s istim ciljem iz te Direktive.¹⁴⁰

Opća uredba se ne primjenjuje ni na obradu koju provode fizičke osobe isključivo tijekom osobnih ili kućnih aktivnosti.¹⁴¹ To su one aktivnosti koje nisu nikako povezane s profesionalnom ili komercijalnom djelatnošću, primjerice korespondencija, posjedovanje adresa, društveno umrežavanje te druge internetske aktivnosti poduzete u kontekstu takvih aktivnosti.¹⁴² Međutim, i tada se primjenjuje na voditelje ili izvršitelje obrade koji pružaju

¹³⁴ ibid., čl. 4., st. 4.

¹³⁵ ibid.

¹³⁶ Gumzej, op.cit. (bilj.106), str. 11

¹³⁷ 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, SL L 119/89

¹³⁸ Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL L 008/1

¹³⁹ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL L 105, 54

¹⁴⁰ Gumzej, op. cit.(bilj. 106), str. 13.

¹⁴¹ GDPR., čl. 2, st. 2., t. c

¹⁴² ibid., recital 18.

sredstva za obradu osobnih podataka za takve osobne ili kućne aktivnosti, tj. na davatelje usluga društvenih mreža i drugih relevantnih online usluga.¹⁴³

Da bi obrada osobnih podataka bila zakonita, sukladno Općoj uredbi, potrebno je da je utemeljena na jednoj od šest pravnih osnova: ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha, obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora, radi poštovanja pravnih obveza voditelja obrade, kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe, za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade ili za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.¹⁴⁴ Potonje se ne odnosi na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća.

Jedna od najvećih novosti iz Opće uredbi je uvođenje obveze procjene učinka obrade osobnih podataka na zaštitu osobnih podataka prije same obrade, ako je vjerojatno da bi neka vrsta obrade mogla biti visokorizična za prava i slobode pojedinaca, osobito ako se provodi putem novih tehnologija, i pritom vodeći računa o prirodi, opsegu, kontekstu i svrsi te obrade.¹⁴⁵ Također, potrebno je imati na umu kako se jedna procjena može odnositi na više sličnih postupaka obrade koji predstavljaju slične visoke rizike.¹⁴⁶ Ova obveza ukazuje na posebnu važnost koju Uredba pridaje zaštiti osobnih podataka, namećući voditeljima obrade zakonodavnu obvezu da paze kako obrada podataka koju vrše utječe na pojedince.

2.3.6. Republika Hrvatska

2.3.6.1. Ustav Republike Hrvatske

¹⁴³ Gumzej, op.cit. (bilj. 106), str. 14.

¹⁴⁴ GDPR, čl. 3., st. 1.

¹⁴⁵ ibid., čl. 35. st. 1.

¹⁴⁶ Čizmić; Boban, op. cit. (bilj. 116.), str. 403.

Ustav Republike Hrvatske štiti pravo na privatnost u čl. 35.: ‘Svakom se jamči štovanje i pravna zaštita njegova osobnog i obiteljskog života, dostojanstva, ugleda i časti.’¹⁴⁷ Samostalno pravo na zaštitu osobnih podataka utvrđeno je u čl. 37.: ‘Svakom se jamči 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.’¹⁴⁸

Ustav također propisuje uvjete za ograničenje ustavnih prava u čl.16.: ‘Slobode i prava mogu se ograničiti samo zakonom da bi se zaštitila sloboda i prava drugih ljudi te pravni poredak, javni moral i zdravlje. Svako ograničenje slobode ili prava mora biti razmjerno naravi potrebe za ograničenjem u svakom pojedinom slučaju.’¹⁴⁹ Također u čl. 17.: ‘U doba ratnog stanja ili neposredne ugroženosti neovisnosti i jedinstvenosti države, te velikih prirodnih nepogoda pojedine slobode i prava zajamčena Ustavom mogu se ograničiti. O tome odlučuje Hrvatski sabor dvotrećinskom većinom svih zastupnika, a ako se Hrvatski sabor ne može sastati, na prijedlog Vlade i uz supotpis predsjednika Vlade, Predsjednik Republike. Opseg ograničenja mora biti primjeren naravi pogibelji, a za posljedicu ne može imati nejednakost osoba s obzirom na rasu, boju kože, spol, jezik, vjeru, nacionalno ili socijalno podrijetlo. Niti u slučaju neposredne opasnosti za opstanak države ne može se ograničiti primjena odredbi Ustava o pravu na život, zabrani mučenja, surovog ili ponižavajućeg postupanja ili kažnjavanja, o pravnoj određenosti kažnjivih djela i kazni, te o slobodi misli, savjesti i vjeroispovijedi.’¹⁵⁰

2.3.6.2. Zakon o provedbi Opće uredbe o zaštiti osobnih podataka (NN br. 42/18)

U Republici Hrvatskoj je *Zakon o provedbi Opće uredbe o zaštiti osobnih podataka*¹⁵¹ stupio na snagu 25.5.2018. te zamijenio dotadašnji *Zakon o zaštiti osobnih podataka*¹⁵² i podzakonske propise koji su se temeljili na tom zakonu.¹⁵³ *Agencija za zaštitu osobnih podataka* (AZOP), osnovana je 2004. godine kao pravna osoba s javnim ovlastima na temelju ranijeg *Zakona o*

¹⁴⁷ Ustav Republike Hrvatske, NN 85/2010, čl. 35.

¹⁴⁸ Ustav RH, čl.37.

¹⁴⁹ Ustav RH, čl. 16.

¹⁵⁰ *ibid.*, čl. 17.

¹⁵¹ Zakon o provedbi Opće uredbe o zaštiti osobnih podataka, NN 42/2018

¹⁵² Zakon o zaštiti osobnih podataka, NN 103/03, 118/06, 41/08, 130/11, 106/12

¹⁵³ Dragičević et al., *op.cit.* (bilj. 4), str. 61

zaštiti osobnih podataka, a novim se zakonom utvrđuje kao neovisno državno nadzorno tijelo u smislu Opće uredbe, koje je u svom radu samostalno i neovisno i za svoj rad odgovara Hrvatskom saboru.¹⁵⁴ Ona obavlja nadzor nad primjenom Opće Uredbe, Zakona za provedbu opće Uredbe i *Direktive EU 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.*¹⁵⁵

AZOP ima ovlast pokretanja i sudjelovanja u kaznenim, prekršajnim, upravnim i drugim sudskim i izvansudskim postupcima zbog povrede Opće uredbe i Zakon o njejoj provedbi (kada je propisao posebnim zakonom) i pokretanja i vođenja postupaka protiv odgovornih osoba.¹⁵⁶ Ako se utvrde povrede navedenih propisa, AZOP ima ovlast izricanja upravne novčane kazne.¹⁵⁷ Nadalje, AZOP je ovlašten obustaviti upravni postupak i predmet uputiti Visokom upravnom sudu RH u određenim posebnim slučajevima međunarodnog prijenosa osobnih podataka, a taj sud se može obratiti Sudu EU.¹⁵⁸ AZOP može izdavati stručna mišljenja iz područja zaštite osobnih podataka na pisani zahtjev fizičkih ili pravnih osoba te stručna mišljenja o prijedlozima zakona i drugih propisa iz materije obradi osobnih podataka.¹⁵⁹

3. INFORMACIJSKA I KOMUNIKACIJSKA TEHNOLOGIJA

3.1. Općenito

Početkom devedesetih se smatralo da će kritično pitanje masovnog komuniciranja u budućnosti biti ugrožavanje privatnosti prisluškivanjem mobitela, nadzorom elektroničke pošte, centraliziranjem osobnih podataka, obradom potrošačkih navika i dr.¹⁶⁰ Osim ugroze privatnosti, govorilo se o 'opasnosti od fragmentacije društva i izolacije pojedinca jer mediji sve više ciljaju na specijalizirane publike, potičući na selektivniji odabir sadržaja i formiranje sve manjih i manjih interesnih skupina koje bi tako mogle postati neupućene u ostala svjetska

¹⁵⁴ *ibid.*

¹⁵⁵ 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, SL L 119/89

¹⁵⁶ Dragičević et al., *op.cit.* (bilj. 4), str. 63.

¹⁵⁷ *ibid.*

¹⁵⁸ *ibid.*

¹⁵⁹ *ibid.*

¹⁶⁰ Rajko, *op. cit.* (bilj. 91), str. 29.

pitanja.¹⁶¹ U sociologiji se taj fenomen naziva 'učinak čahure', gdje se ljudi okružuju samo političkim i društvenim informacijama koje odgovaraju njihovim interesima i svjetonazorima, stvarajući tako oko sebe informacijski balon koji ne mora odgovarati stvarnosti.¹⁶² Zatim se ističe pitanje informacijske zasićenosti s obzirom da vijesti, podaci i zabava postaju glavni proizvod društva i preopterećuju pojedinca prevelikim mogućnostima izbora u svakom segmentu. I na kraju, rasla je zabrinutost da će zbog sve veće sličnosti medijske stvarnosti sa životom, ljudi sve više tražiti bijeg od stvarnosti u medijskom svijetu.¹⁶³ U današnje smo doba svjedoci opravdanosti ovih bojazni.

S druge strane, primjenom novih tehnologija se pokreće društveni i gospodarski razvoj i napredak svake zemlje.¹⁶⁴ U svim ekonomskim i društvenim aktivnostima se koriste informacijske i komunikacijske tehnologije za brzo i jednostavno prikupljanje, pohranu, obradu, prenošenje, razmjenu, pristup i korištenje različitih podataka i informacija, a sve veći zahtjevi i potražnja za velikim brojem informacija dovodi do stvaranja niza zbirki uglavnom osobnih podataka.¹⁶⁵ Takvim se zbirkama podataka služe gotovo sva tijela s kojima suvremeni građani svakodnevno dolaze u doticaj, kao što su državna tijela, agencije i institucije, tvrtke, neprofitne organizacije, kulturne i sportske institucije...¹⁶⁶ Stoga nije osobito vjerojatno da bi osoba mogla na bilo koji način funkcionirati u društvu, a da izbjegne obradu svojih osobnih podataka.¹⁶⁷ Brojne prednosti obrade uključuju 'profitabilnije, jednostavnije i brže poslovanje, uspjeliji nastup na domaćem i inozemnom tržištu, kvalitetnije programe prilagođene stvarnim potrebama pojedinca i zajednice, sniženje troškova, bolji standard i sigurnije okruženje s obzirom na zaštitu okoliša, održiv razvoj i učinkovitiju obranu od terorizma i kriminala.¹⁶⁸ Možemo pretpostaviti da će u budućnosti tehnologija postati još sveprisutnija i još sofisticiranija nego danas.¹⁶⁹

¹⁶¹ ibid.

¹⁶² ibid., bilješka 57., str. 29.

¹⁶³ ibid.

¹⁶⁴ Sudar-Kulčar, Mirna, Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni (direktni) marketing, *Politička misao*, vol. XLII, 2005., br. 4, str. 97.

¹⁶⁵ ibid., str. 98.

¹⁶⁶ ibid.

¹⁶⁷ Jurić, op. cit. (bilj. 12), str. 67.

¹⁶⁸ Sudar-Kulčar, loc.cit. (bilj. 158), str. 98.

¹⁶⁹ ibid.

Naime moderni je život predvidljiviji i sigurniji nego ikad prije, upravo iz razloga što je vrlo organiziran.¹⁷⁰ Organiziranost suvremenog društva je rezultat planiranja i usmjeravanja načina rada i ponašanja ljudi od strane institucija.¹⁷¹ Takvu razinu organizacije života i društva omogućava sustavno prikupljanje informacija o ljudima i njihovim aktivnostima.¹⁷² U kontekstu navedenog, možemo reći da je rutinski nadzor preduvjet uspješne društvene organizacije suvremenog doba.¹⁷³

3.2. Utjecaj informacijske i komunikacijske tehnologije na pravo privatnosti

Utjecaj informacijskih tehnologija na privatnost kroz povijest počinje od otkrića tiska u 15. stoljeću, preko druge informacijske revolucije na prijelazu iz 19. u 20. stoljeće pojavom radija i televizije te širenjem njihove dostupnosti upotrebom komunikacijskih satelita u devedesetima, a vrhunac dostiže informatičkom revolucijom s pojavom računala i interneta.¹⁷⁴ Taj je utjecaj doveo do brojnih pogodnosti, ali i brojnih rizika i izazova za privatnost i ljudska prava općenito. Pozitivnim se smatra olakšana dostupnost podataka, informacija i znanja, promicanje ljudskih prava i sloboda, jačanje svijesti o važnosti zaštite tih prava, veća transparentnost vlasti koja omogućuje javnosti lakše praćenje javnih politika i izražavanje svog neslaganja.¹⁷⁵

Po drugačijem stajalištu, tehnološki napredak nije pomogao u riješiti stare probleme, već su se postojeći problemi uvijek odgađali ili zamjenjivali novima.¹⁷⁶ U tom smislu su ljudskih prava pojavom novih tehnologija postala još ugroženija nego prije, zbog novih mogućnosti njihovog ugrožavanja.¹⁷⁷ Među negativnim utjecajima razvoja tehnologije na privatnost ističe se lakše dezinformiranje i manipuliranje javnošću, promicanje nemoralnih i nezakonitih ciljeva, ideja i

¹⁷⁰Webster, F., *Theories of the information society*, 1995, str. 53., u Boban, Marija, *Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu*, Zbornik radova Pravnog fakulteta u Splitu, 49, 3/2012, str. 593.

¹⁷¹ *ibid.*

¹⁷² *ibid.*

¹⁷³ *ibid.*

¹⁷⁴ Dragičević et al., *op.cit.* (bilj. 4), str. 6

¹⁷⁵ *ibid.*

¹⁷⁶ Tuđman, Miroslav, *Uvod u informacijsku znanost*, str. 177., u Boban, loc. cit. (bilj. 164), str. 592.

¹⁷⁷ Boban, loc. cit. (bilj. 164.), str. 592.

sadržaja, masovni nadzor, cenzura neistomišljenika, poticanje na nasilje, rasnu ili vjersku mržnju itd.¹⁷⁸

U današnjem tzv. 'dobu velikih podataka (Big Data)', osobni podaci se smatraju novom naftom interneta i novom valutom digitalnog svijeta.¹⁷⁹ To je stvarnost koju moramo prihvatiti zato što su tako odabrali internetski korisnici, masovno pristajući na prikupljanje osobnih podataka u svrhu oglašavanja u zamjenu za besplatne internetske usluge.¹⁸⁰ *'Internet is an advertisement supported service and the development of marketing based on profiling and personal data is what makes it go round.'*¹⁸¹ U korak s razvojem visokih tehnologija javljaju se različite mogućnosti obrade osobnih podataka, što je ojačalo tržište osobnih podataka.¹⁸² Međutim, temelj uspješnog funkcioniranja takvog tržišta je povjerenje korisnika da će se s njihovim osobnim podacima zakonito postupati i da će se poduzeti zaštitne mjere protiv njihove zloupotrebe, te je stoga osobito važno osigurati jamstva pravne zaštite obrade osobnih podataka korisnika.¹⁸³

'Elektroničke komunikacije sve više postaju temeljna infrastruktura za obavljanje i zadovoljavanje najrazličitijih poslovnih i osobnih potreba poput informiranja, obrazovanja, elektroničke trgovine, zabave i društvenog života.'¹⁸⁴ Tehnološkim razvojem na tom području javljaju se novi izazovi za pravno područje privatnosti i zaštite osobnih podataka kao što su profiliranje, bihevioralno oglašavanje, cookies, Internet stvari (Internet of Things - IOT), usluga računarstva u oblaku (cloud computing), biometrija, DNA identifikacija, identifikacija putem radiofrekvencije (RFID).¹⁸⁵

3.3. Profiliranje i bihevioralno oglašavanje

¹⁷⁸ Dragičević et al., op.cit. (bilj. 4), str.7.

¹⁷⁹ Kuneva, Meglena, Roundtable on Online Data Collection, Targeting and Profiling, 2009., https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156, (29.5.2022.)

¹⁸⁰ ibid.

¹⁸¹ ibid.

¹⁸² Gumzej, Nina, Challenges of the digital environment for personal data privacy and security, DIT 2014, Dr. Juraj Plenković, str. 707.

¹⁸³ ibid.

¹⁸⁴ ibid.

¹⁸⁵ ibid., str. 708.

3.3.1. Profiliranje

'Tehnološki razvoj u području elektroničkih komunikacija i informacijskih i komunikacijskih tehnologija omogućio je identifikaciju, praćenje i analizu ponašanja korisnika pohranom podataka koji se generiraju samim korištenjem elektroničkih komunikacija i komunikacijskih usluga.¹⁸⁶ Visoko kompetitivna ekonomija digitalnog tržišta nudi sve veći broj personaliziranih usluga i proizvoda, zasnovanih na individualnim navikama i željama korisnika kako bi se što je moguće točnije ciljale njihove potrebe i interesi.¹⁸⁷ To se postiže praćenjem i profiliranjem korisnika.

S obzirom da većina pojedinaca svakodnevno koristi Internet za većinu svojih životnih aktivnosti, ponašanje korisnika na internetu pruža idealnu osnovu za stvaranje individualnog profila osobe. Praćenjem njegovog ponašanja na internetu, možemo profilirati pojedinca po navikama, interesima i osobnosti.¹⁸⁸ Međunarodna radna skupina za zaštitu podataka u telekomunikacijama, poznata kao Berlin grupa, definira praćenje (*web tracking*) kao prikupljanje, naknadno zadržavanje, korištenje ili dijeljenje podataka o korisničkoj aktivnosti na mreži preko više posjećenih web stranica korištenjem kolačića (*cookies*), *JavaScripta* ili bilo koje vrste identifikacije uređaja (*device fingerprinting*), a tehnologije praćenja omogućuju neprestani tok podataka o korisniku u stvarnom vremenu, primjerice podatke o registraciji, aktivnosti pretraživanja, statistike posjećivanja web stranica i podatke o reakciji korisnika na individualne ponude.¹⁸⁹

'Profiliranje u najširem smislu uključuje rudarenje (*data mining*) velike količine podataka koji se prikupljaju u postupku skladištenja podataka (*data warehousing*) da bi se potom donijeli zaključci o poveznicama između određenih sadržaja koji se odnose na konkretne osobe kako bi se postigao određeni cilj (npr. da se osoba ponaša na željeni način).¹⁹⁰ Drugim riječima, to je proces stvaranja profila (*profile generation*) i proces tretiranja korisnika u svjetlu tog profila

¹⁸⁶ *ibid.*, str. 707

¹⁸⁷ *ibid.*

¹⁸⁸ *ibid.*

¹⁸⁹ International Working Group on Data Protection in Telecommunications: Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2013/2013-WP-Webtracking-en.pdf, (29.5.2022.)

¹⁹⁰ Dragičević et. al., op. cit. (bilj. 4), str. 9.

(*profile application*).¹⁹¹ Za profiliranje se koriste različite moderne tehnologije, primjerice nadzor i praćenje putem GPS tehnologije, dubinsko pregledavanje sadržaja paketa prometa koji se prenose mrežom (*Deep pocket inspection*, DPI), video nadzor i dr.¹⁹²

Prvi korak u profiliranju je prikupljanje podataka korištenjem tehnologija praćenja.¹⁹³ Najčešća tehnologija korištena za bihevioralno praćenje su kolačići (*cookies*). To su 'tekstualne datoteke koje sadrže malu količinu informacija koja se preuzima na uređaj prilikom posjećivanja web-stranice.¹⁹⁴ Nakon toga web-preglednik šalje kolačiće natrag izvornoj web-stranici prilikom svakog posjećivanja stranice ili nekoj drugoj web-stranici koja prepoznaje ove kolačiće.¹⁹⁵ Mogu biti postavljeni od strane operatora web stranice (*first party cookies*) ili od strane trećih osoba (*third party cookies*).¹⁹⁶ Drugi primjer tehnologije korištene za praćenje su web-pratilice (*web beacons*, poznate i kao 'piksel oznake' ili 'jasni GIF-ovi'), malene grafičke slike koje se obično koriste kako bi prikazale da je korisnik pristupio određenoj web-stranici, kliknuo na neki sadržaj ili ga pročitao, u svrhu analize korištenja web-stranica.¹⁹⁷ Praćenje se može odvijati i putem identifikacije uređaja (*device fingerprinting*), tj. pomoću različitih informacijskih elemenata koji identificiraju uređaj ili određeni slučaj njegove primjene.¹⁹⁸ Tome mogu poslužiti brojne informacije koje zajedno tvore individualni otisak uređaja, primjerice čak i specifičan način na koji pojedinac puni bateriju svog uređaja može stvoriti njegov jedinstveni profil.¹⁹⁹

Drugi korak profiliranja je stvaranje profila korisnika.²⁰⁰ Prikupljeni podaci se analiziraju korištenjem softwera za utvrđivanje statističke korelacije koji stvara profile kombinacijom tih podataka kroz analizu određenih uzoraka ponašanja.²⁰¹ Može se raditi o individualnim korisničkim profilima, ali najčešće se formiraju grupe profila korisnika sa zajedničkim preferencijama, lokacijom, kupnjama, hobijima, posjećenim stranicama, dobnom skupinom i

¹⁹¹ Kamara, Irene; Kosta, Eleni, Do Not Track initiatives: regaining the lost user control, *International Data Privacy Law*, vol. 6., issue 4, 2016, str. 5.

¹⁹² Dragičević et al., loc. cit. (bilj. 184)

¹⁹³ Kamara; Kosta, op. cit. (bilj. 185.), str. 6..

¹⁹⁴ All about cookies, <https://allaboutcookies.org/> (29.5.2022.)

¹⁹⁵ *ibid.*

¹⁹⁶ Kamara; Kosta, op.cit. (bilj. 185.), str. 6..

¹⁹⁷ *ibid.*, bilj. 16., str. 6.

¹⁹⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, 2014., str. 4.

¹⁹⁹ 'Article 29 Working Party targets device fingerprinting', <https://www.osborneclarke.com/insights/artikel-29-datenschutzgruppe-nimmt-device-fingerprinting-ins-visier> (29.5.2022.)

²⁰⁰ Kamara; Kosta, loc.cit. (bilj. 185), str. 7.

²⁰¹ *ibid.*

sl.²⁰² Grupe profila se označuju na način koji olakšava rad oglašivačima, primjerice 'ljubitelji nogometa' ili 'entuzijasti za tekuća zbivanja'.²⁰³

3.3.2. Bihevioralno oglašavanje

U današnjem iznimno kompetitivnom potrošačkom društvu, oglašavanje postaje vrlo važna poslovna aktivnost. Velike baze osobnih podataka i profiliranje korisnika imaju ogroman komercijalni potencijal te oglašivači koriste blagodati novih tehnologija kako bi poboljšali svoje marketinške strategije. Za razliku od reklama upućenih široj javnosti, bihevioralno oglašavanje je upućeno izravno korisniku na temelju nekih njegovih karakteristika. 'Izravni (direktni) marketing je specifičan marketinški sustav u kojem marketer na temelju baze podataka uspostavlja izravni odnos s krajnjim korisnikom (potrošačem), bez posrednika, putem interaktivne komunikacije gdje potencijalni kupac ima mogućnost trenutne reakcije (narudžba putem telefona, pošte, elektronička trgovina).'²⁰⁴ Za uspješno izravno oglašavanje je važno prikupljanje podataka o potencijalnim i sadašnjim potrošačima kako bi se stvorila kvalitetna baza podataka i pomoću nje uspješna kampanja ciljanog oglašavanja.²⁰⁵ Prije zabrane korištenja osobnih podataka korisnika bez njihove privole, tzv. 'tvrtke sastavljača adresa (compilers)' su prikupljale osobne podatke građana iz različitih javnih dokumenata i sastavljale baze podataka te ih prodavale različitim kompanijama koje su ih koristile za formiranje kampanja izravnog marketinga.²⁰⁶ S obzirom na veći naglasak na zaštiti osobnih podataka u suvremenom dobu, ovakav tip oglašavanja danas mora počivati na dopuštenju korisnika. Tzv. 'dopušteni marketing (permission marketing)' temelji se na privoli korisnika za dostavu promotivnih poruka i materijala ili kontaktiranje telefonom ili elektroničkom poštom ili druge metode izravnog oglašavanja.²⁰⁷

AZOP navodi primjer online bihevioralnog oglašavanja: 'Posrednik podataka (eng. data broker) u ime svojih klijenata ili za vlastite potrebe prikuplja podatke iz različitih javnih i privatnih izvora kako bi izradio profile o pojedincima i razvrstava ih u određene kategorije u skladu s

²⁰² ibid.

²⁰³ ibid.

²⁰⁴ Sudar-Kulčar, op. cit. (bilj. 158), str. 104.

²⁰⁵ ibid., str. 105

²⁰⁶ ibid., str. 107.

²⁰⁷ ibid., str. 112.

njihovim interesima.²⁰⁸ Te profile prodaje poduzeću koje potom ciljano oglašava svoje robe i usluge na društvenim mrežama točno određenoj kategoriji kupaca za koje smatraju da će biti zainteresirani za kupnju (npr. prikazivanje oglasa za luksuzne ženske torbe ženama u dobi od 35-45 godina više platežne moći).²⁰⁹

3.3.3. Pravno uređenje obrade osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja

3.3.3.1. Općenito

Opća uredba sadrži specifične odredbe koje se odnose na tehnologije praćenja i profiliranja. U recitalu 72 stoji da izrada profila podliježe pravilima Uredbe kojima se uređuje obrada osobnih podataka, kao što su pravna osnova obrade ili načela zaštite podataka.²¹⁰ Nadalje Uredba detaljno pojašnjava: 'pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli, kao što su adrese internetskog protokola, identifikatori kolačića ili drugim identifikatorima poput oznaka za radiofrekvencijsku identifikaciju, a tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju.'²¹¹ Uredba eksplicitno navodi adrese internetskog protokola (IP adrese) kao mrežne identifikatore, čime rješava dugotrajnu debatu o tom pitanju, a uključuje i kolačiće i RFID tehnologiju.²¹² Također su navedeni kriteriji kada se obrada smatra praćenjem ponašanja (profiliranje): 'prati li se pojedinca na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova.'²¹³

²⁰⁸ AZOP: Što su izrada profila, automatizirano donošenje odluka i ciljano oglašavanje?, <https://azop.hr/najcesce-postavljena-pitanja/>, (1.6.2022.)

²⁰⁹ *ibid.*

²¹⁰ GDPR, recital. 72.

²¹¹ *ibid.*, recital 30.

²¹² Kamara; Kosta, *op.cit.* (bilj. 185.), str. 19.

²¹³ GDPR, recital 24.

3.3.3.2. Pravna osnova obrade osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja

Za pitanje obrade osobnih podataka putem kolačića je važno tzv. *cookie rule* u Direktivi EU o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija 2002. (E-Privacy Direktiva)²¹⁴, koje je značajno promijenjeno izmjenom 2009. (Citizens Rights Direktiva).²¹⁵ Odgovarajuće pravilo je preuzeto i u hrvatski *Zakon o elektroničkim komunikacijama* (ZEK).²¹⁶ Tzv. *cookie rule* uređuje pohranu i pristup informacijama pohranjenim na terminalnoj opremi korisnika, a smješteno je u E-Privacy direktivi kao jedan od članaka odredbe o povjerljivosti komunikacija. 'To je pravilo izazvalo znatnu pažnju javnosti zbog svog značajnog utjecaja na online poslovanje, osobito na praksu korištenja kolačića.'²¹⁷ Ono obvezuje države članice da osiguraju da je 'pohranjivanje podataka ili uspostavljanje pristupa već pohranjenim podacima na terminalnoj opremi pretplatnika ili korisnika, dozvoljeno samo pod uvjetom da je dotični pretplatnik ili korisnik dao svoj pristanak, nakon što je iscrpno i razumljivo, u skladu s Općom uredbom o zaštiti podataka, između ostalog obaviješten o namjeni postupka obrade.'²¹⁸ Upotreba kolačića stoga ovisi o pristanku korisnika kojem je pruženo kvalitetno objašnjenje namjene obrade. 'Navedeno ne sprečava nikakav oblik tehničke pohrane ili pristupa samo u svrhu izvršavanja prijenosa komunikacije putem elektroničke komunikacijske mreže ili ako je to strogo potrebno, kako bi operator usluge informacijskog društva mogao pružiti uslugu koju je izričito zatražio pretplatnik ili korisnik.'²¹⁹ Dakle, izuzev navedenih slučajeva, za upotrebu kolačića je potreban informirani pristanak.²²⁰ Preciznije, mora se raditi o privoli koja zadovoljava uvjete iz Opće uredbe u smislu dobrovoljnosti, posebnosti, informiranosti i nedvosmislenosti.²²¹ 'Unatoč spomenutom fokusu

²¹⁴ Direktiva 2002/58/EZ Europskog parlamenta i vijeća od 12. srpnja 2002., o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)

²¹⁵ Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/58/EZ

²¹⁶ Zakon o elektroničkim komunikacijama („Narodne novine“ broj 73/08, 90/11, 132/12, 80/13, 71/14), čl. 100., st. 4.

²¹⁷ Gumzej, Nina; Dragičević, Dražen, *Convergence in Communications and E-Privacy Regulatory Challenges, With a Local Perspective*, 2015., u: Thomas Plank / IEEE (ur.) *Proceedings of the 13th International Conference on Telecommunications*, str. 3.

²¹⁸ Direktiva 2009/136/EZ, čl. 5. st. 3.

²¹⁹ *ibid.*

²²⁰ Gumzej, Dragičević, *loc.cit.* (bilj. 211.)

²²¹ GDPR, čl. 4., st. 11.

na kolačiće, osnovna namjena ovog pravila je zaštita terminalne opreme, a time i korisnikove privatne sfere, neovisno o korištenoj tehnologiji, što znači da odredba pokriva i device fingerprinting, malware i spyware.²²²

Po prijašnjem uređenju, do 2009. godine, je umjesto pristanka, bilo potrebno da se pretplatniku ili korisniku pruže jasne i sveobuhvatne informacije između ostalog, o svrsi obrade te da ima pravo odbiti takvu obradu.²²³ Ova promjena od prava na odbijanje do obveznog davanja pristanka je potpuno promijenila praksu internetskih pretraživača koji su automatski (by default) pohranjivali kolačiće na računala i mobitele korisnika, pružajući im mogućnost da to promijene u postavkama pretraživača.²²⁴ U današnjem uređenju je važno da su informacije koje se pružaju korisnicima jasne i sažete te da se javljaju prije svakog njihovog djelovanja koje bi moglo dovesti do pohranjivanja ili davanja mogućnosti pristupa, te je osobito važno da su postavke privatnosti jednostavne za korištenje (*user-friendly*).²²⁵ 'Kada je to tehnički moguće i učinkovito, pristanak korisnika na obradu mogao bi se izraziti korištenjem odgovarajućih postavki na pregledniku ili drugim aplikacijama.'²²⁶

Opća uredba navodi privolu ispitanika kao jednu od pravnih osnova zakonite obrade podataka²²⁷ i definira ju kao 'svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.'²²⁸ Element dobrovoljnosti podrazumijeva da korisnik ima stvarni izbor te nema štetnih posljedica u slučaju ne davanja privole.²²⁹ Pri procjeni je li privola bila dobrovoljna uzima se u obzir neravnoteža ovlasti između voditelja obrade i ispitanika, npr. kad je voditelj tijelo javne vlasti, i postojanje odnosa koji uključuje slabiju stranu, npr. radnopravni odnos.²³⁰ U takvim situacijama nije vjerojatno da je privola dana dobrovoljno,²³¹ međutim nije posve isključena te može iznimno biti pravna osnova obrade.²³² Također, uzima se u obzir je li izvršenje ugovora, uključujući pružanje usluge, uvjetovano

²²² Gumzej, Dragičević, loc.cit. (bilj. 211.)

²²³ Direktiva 2002/58/EZ, čl. 5., st. 3.

²²⁴ Kamara; Kosta, op. cit. (bilj. 185), str. 22.

²²⁵ Direktiva 2009/136/EZ, Recital 66.

²²⁶ ibid.

²²⁷ GDPR, čl. 6., st. 1., t. a

²²⁸ GDPR, čl. 4., st. 11.

²²⁹ Smjernice 5/2020 o privoli na temelju Uredbe 2016/679, Europski odbor za zaštitu podataka, 2020., str. 7.

²³⁰ ibid., str. 8.

²³¹ GDPR, recital 43.

²³² Smjernice 5/2020, op. cit. (bilj. 223), str. 9.

davanjem privole za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora.²³³ Smatra se da privola o kojoj ovisi izvršenje ugovora, a koja za to nije nužna, nije dana dobrovoljno.²³⁴ Primjerice 'ako mobilna aplikacija za uređivanje fotografija traži od korisnika aktivaciju GPS lociranja za korištenje njezinim uslugama i prikupljene podatke koristi u biheviorističke promidžbene svrhe, privola se ne može smatrati dobrovoljnom jer ju korisnici ne mogu upotrebljavati bez privole, a ni geolociranje ni biheviorističko oglašavanje nisu nužni za pružanje usluge obrađivanja fotografija.'²³⁵ Isto tako se 'ne smatra dobrovoljno dana privola u slučaju tzv. obveznog prihvaćanja kolačića gdje korisnik ne može pristupiti uslugama i funkcijama ako ne prihvati kolačiće, primjerice kada pružatelj internetskih stranica uvodi skriptu kojom se onemogućuje vidljivost sadržaja.'²³⁶ Nadalje, ako usluga uključuje višestruke postupke obrade osobnih podataka ili ako obrada ima višestruke svrhe, potrebno je zadovoljiti uvjet granularnosti, tj. dati privolu za svaki pojedini postupak obrade i za svaku pojedinu svrhu.²³⁷ Voditelj obrade mora dokazati da je moguće odbiti ili povući privolu bez štetnih posljedica.²³⁸ Primjer štetnih posljedica je slučaj mobilne aplikacije za životni stil koja nakon povlačenja privole za pristup akcelerometru telefona, iako nije nužan za rad aplikacije, radi samo u ograničenoj mjeri.²³⁹

Uvjet posebnosti privole označava da privola mora biti dana u posebno definiranu svrhu.²⁴⁰ Svrha mora biti jasna i dovoljno određena, a ne generalizirana, npr. 'poboljšanje iskustva korisnika' ili 'u svrhu budućih istraživanja'.²⁴¹ Time se korisnika štiti od kasnijeg tzv. širenja namjene nakon davanja pristanka za prikupljanje podataka.²⁴² Također, ako se radi o usluzi koja ima više svrha obrade podataka, za privolu je važan uvjet granularnosti, u smislu da se mora omogućiti davanje posebne privole za svaku svrhu zasebno i pružiti informacije odvojeno za svaku od tih svrha.²⁴³ Na taj način voditelj obrade omogućuje ispitaniku da sam izabere i pristane samo na postupke obrade s kojima se slaže.²⁴⁴

²³³ GDPR, čl. 7., st. 4.

²³⁴ *ibid.*, recital 43.

²³⁵ Smjernice 5/2020, op. cit. (bilj. 223), str. 8.

²³⁶ *ibid.*, str. 12.

²³⁷ GDPR, recital 32. i 43.

²³⁸ *ibid.*, recital 42.

²³⁹ Smjernice 5/2020, op. cit. (bilj. 223), str. 13.

²⁴⁰ Mišćenić et al., op. cit. (bilj. 105), str. 305.

²⁴¹ Smjernice 5/2020, op. cit. (bilj. 223), str. 14.

²⁴² *ibid.*

²⁴³ *ibid.*

²⁴⁴ *ibid.*, str. 15.

Uvjet informiranosti odnosi se na zahtjev da se ispitaniku pruže informacije i činjenice o obradi osobnih podataka prije davanja privole za obradu.²⁴⁵ Time mu se daje prilika da sam informirano odluči i procijeni želi li pristati na obradu svojih osobnih podataka i da razumije ono na što pristaje.²⁴⁶ Europski odbor za zaštitu podatak navodi minimalni sadržaj koji se mora pružiti ispitaniku u svrhu davanja informirane privole: 'identitet voditelja obrade, svrha svakog postupka obrade za koji se traži privola, vrsta podataka koji će se prikupljati, pravo na povlačenje privole, prema potrebi informacije o automatiziranom donošenju odluka i mogući rizici prijenosa podataka zbog nepostojanja odluke o prikladnosti i odgovarajućih zaštitnih mjera iz čl. 46. GDPR.'²⁴⁷

Uvjet nedvosmislenosti znači ispitanik mora dati privolu izjavom ili jasnom potvrdnom radnjom, dakle uvijek nekom aktivnom radnjom.²⁴⁸ To isključuje šutnju, neaktivnost ili unaprijed označen pristanak.²⁴⁹ Privola mora nesumnjivo ukazivati na namjeru ispitanika.²⁵⁰ U digitalnom kontekstu, obrada osobnih podataka je temelj brojnih usluga koje svakodnevno koristimo pa se tako ispitanici vrlo često nalaze u situaciji da moraju aktivno davati privolu na obradu.²⁵¹ Zbog toga dolazi do 'zamora u klicanju' pa ispitanici ni ne pročitaju pružene informacije i upozorenja, čime one gube svoju svrhu.²⁵² Za neke situacije je potrebna izričita privola, kada postoji osobito visok rizik ugrožavanja prava za zaštitu podataka te je potrebna pojačana pažnja ispitanika pri davanju privole, primjerice za automatizirano pojedinačno donošenje odluka, osobito izradu profila.²⁵³

Radna skupina WP29 daje odgovor na pitanje bi li nužnost za izvršenje ugovora ili predugovornih radnji (iz čl. 6. st. 1. t. b) mogla biti zakonita osnova za obradu osobnih podataka za internetsko oglašavanje na temelju obrazaca ponašanja: 'Ugovorna nužnost nije odgovarajuća pravna osnova za izradu profila ukusa i načina života korisnika na temelju toka klikova na mrežnim stranicama koje posjećuje i proizvoda koje kupuje, jer voditelj obrade nije

²⁴⁵ Mišćenić et al., op. cit. (bilj. 105), str. 305.

²⁴⁶ Smjernice 5/2020, op. cit. (bilj. 223), str. 15.

²⁴⁷ ibid., str. 16.

²⁴⁸ ibid., str. 18.

²⁴⁹ Mišćenić et al., op. cit. (bilj. 105), str. 305.

²⁵⁰ ibid.

²⁵¹ Smjernice 5/2020, op. cit. (bilj. 223), str. 19.

²⁵² ibid.

²⁵³ ibid., str. 20.

angažiran za izradu profila nego za isporuku određenih vrsta proizvoda i usluga.²⁵⁴ Obrada osobnih podataka za internetsko oglašavanje nije nužna za izvršenje ugovora za internetske usluge.²⁵⁵ Ne može se opravdati ni razlogom da oglašavanje neizravno financira pružanje usluge.²⁵⁶ 'S obzirom da je zaštita osobnih podataka temeljno pravo zajamčeno čl. 8. Povelje EU o temeljnim pravima te da je jedna od glavnih svrha GDPR-a pružanje kontrole ispitanicima nad podacima koji se odnose na njih, osobni podaci se ne mogu smatrati proizvodom kojim se trguje.²⁵⁷ Ispitanik može pristati na obradu osobnih prava, ali ne može trgovati temeljnim pravima.²⁵⁸ Navedeno je u skladu sa spomenutim pravilom Direktive o e-privatnosti o nužnosti prethodnog pristanka za postavljanje kolačića koji su nužni za uključivanje internetskog oglašavanja na temelju obrazaca ponašanja.

GDPR navodi da se kod izravnog marketinga može koristiti i pravnom osnovom legitimnog interesa.²⁵⁹ Može se smatrati da postoji legitiman interes kod obrade osobnih podataka provedene za potrebe izravnog marketinga.²⁶⁰ Međutim, za upotrebu legitimnog interesa kao pravne osnove potrebno je provesti test ravnoteže koji se sastoji od utvrđivanja tri činjenice, a postojanje legitimnog interesa je samo jedna od njih.²⁶¹ Drugi korak je utvrđivanje je li obrada osobnih podataka nužna kako bi se ostvario taj legitimni interes, što će biti slučaj ako ne postoji manje invazivno sredstvo kojim bi se mogla postići ista svrha.²⁶² Treći korak je utvrđivanje kako će takva obrada utjecati na temeljna prava i slobode ispitanika te može li on razumno predvidjeti obradu u takvu svrhu.²⁶³ Ovdje je osobito naglasak na prethodnim aktivnostima voditelja obrade pa se utvrđuju poduzete mjere za osiguravanje važnih načela obrade, poput proporcionalnosti, transparentnosti i ograničenja količine prikupljenih podataka, te dodatne mjere za sigurnost osobnih podataka ili osiguravanje mogućnosti ispitanicima da se isključe iz obrade ('opt-out').²⁶⁴

²⁵⁴ Mišljenje 06/2014 radne skupine o pojmu legitimnih interesa voditelja obrade u skladu s člankom 7. Direktive 95/46/EZ (WP217), 844/14/EN RD 217, str. 17.,

²⁵⁵ Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke b Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, Europski odbor za zaštitu podataka, 2019., str. 14.

²⁵⁶ *ibid.*, str. 15.

²⁵⁷ *ibid.*

²⁵⁸ *ibid.*

²⁵⁹ Mišćenić et al., op. cit. (bilj. 105), str. 311.

²⁶⁰ GDPR, recital 47.

²⁶¹ Mišćenić et al., op. cit. (bilj. 105), str. 310.

²⁶² *ibid.*

²⁶³ *ibid.*, str. 311

²⁶⁴ *ibid.*

3.3.3.3. Prava ispitanika osobnih podataka u svrhu profiliranja i bihevioralnog oglašavanja

Jedno od najvažnijih prava ispitanika je njegovo pravo da se usprotivi obradi svojih osobnih podataka ulaganjem prigovora. 'Ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega, kada je obrada temeljena na javnom interesu ili izvršavanju javne ovlasti ili legitimnom interesu voditelja ili treće osobe, uključujući izradu profila koja se temelji na tim odredbama.'²⁶⁵ Dakle ne može prigovoriti na profiliranje kada je pravna osnova obrade privola ili izvršenje ugovora ili druga osnova, što isključuje znatan broj slučajeva profiliranja.²⁶⁶ Međutim uvijek može prigovoriti profiliranju ako je povezano s izravnim marketingom.²⁶⁷ Nakon uloženog prigovora, voditelj više ne smije obrađivati njegove osobne podatke, 'osim ako ne dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.'²⁶⁸ Dakle teret dokaza je na voditelju obrade. U kontekstu služenja uslugama informacijskog društva, kako bi mu se olakšalo služenje svojim pravom na prigovor, 'ispitanik može ostvariti svoje pravo na prigovor automatiziranim putem koji se koristi tehničkim specifikacijama.'²⁶⁹

Nadalje, 'ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu.'²⁷⁰ Radi se o odluci ili mjeri za čije je donošenje potrebna procjena ispitanikovih osobnih karakteristika ili okolnosti, a koja se isključivo donosi tehnološkim putem bez ljudske intervencije, i koja proizvodi pravne učinke, poput automatskog odbijanja zahtjeva za kreditom putem interneta ili zapošljavanja putem interneta.²⁷¹ Iznimke od navedenog pravila predviđene su u slučaju da je 'odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, dopuštena pravom Unije ili pravom države članice kojem podliježe voditelj obrade te koje također

²⁶⁵ GDPR, čl. 21.

²⁶⁶ Kamar; Kosta, op.cit. (bilj. 185), str. 20.

²⁶⁷ GDPR, čl. 21. st. 2.

²⁶⁸ ibid., čl. 21., st. 1.

²⁶⁹ ibid., čl. 21., st. 5.

²⁷⁰ ibid., čl. 22, st. 1.

²⁷¹ ibid., recital 71.

propisuje odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika.²⁷²

Automatizirane odluke mogu se donositi uz upotrebu postupaka profiliranja ili bez njih, i naravno izrada profila ne rezultira nužno donošenjem automatiziranih odluka.²⁷³ Međutim, izrada profila i automatizirano donošenje odluka se mogu kasnije ispreplesti, ovisno o načinu korištenja podacima, pa je moguće da jednostavan postupak automatiziranog donošenja odluka preraste u postupak koji se temelji na izradi profila.²⁷⁴

U svakom slučaju takve obrade, potrebna je primjena zaštitnih mjera kao što su 'davanje određenih informacija ispitaniku i pravo na ljudsku intervenciju, pravo na izražavanje vlastitog stajališta, na dobivanje pojašnjenja odluke donesene nakon takve procjene i pravo na osporavanje odluke.'²⁷⁵ Od takvih bi postupaka trebalo isključiti djecu.²⁷⁶ Nadalje, voditelj obrade mora 'poduzeti odgovarajuće matematičke i statističke postupke za izradu profila, provesti odgovarajuće tehničke i organizacijske mjere kako bi se posebno osiguralo da budu ispravljeni čimbenici koji dovode do netočnosti u osobnim podacima i da se rizici od pojave pogrešaka svedu na minimum, te osobne podatke osigurati na način kojim se uzima u obzir potencijalne rizike za interese i prava ispitanika i kojim se, među ostalim, sprečavaju diskriminacijski učinci na pojedince na temelju rasnog ili etničkog porijekla, političkog mišljenja, vjere ili uvjerenja, članstva u sindikatu, genetskog ili zdravstvenog stanja ili spolne orijentacije, ili koji rezultiraju mjerama koje imaju takav učinak.'²⁷⁷ Opća uredba propisuje obvezno provođenje procjene učinka na zaštitu podataka iz čl. 35. GDPR-a u slučaju donošenja automatiziranih odluka, i osobito kod izrade profila.²⁷⁸ Automatizirane odluke i izrada profila na temelju posebnih kategorija osobnih podataka iz čl. 9. GDPR-a dopustive su samo pod posebnim uvjetima.²⁷⁹

Po GDPR-u, ako se osobni podaci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na takvu obradu, uključujući profiliranje, u mjeri u kojoj

²⁷² *ibid.*, čl. 22, st. 2.

²⁷³ AZOP: Što su izrada profila, automatizirano donošenje odluka i ciljano oglašavanje?, <https://azop.hr/najcesce-postavljena-pitanja/>, (1.6.2022.)

²⁷⁴ *ibid.*

²⁷⁵ GDPR., recital 71.

²⁷⁶ *ibid.*

²⁷⁷ *ibid.*

²⁷⁸ *ibid.*, čl. 35., st. 3., t. a

²⁷⁹ *ibid.*, recital 71.

postoji povezanost s izravnim marketingom.²⁸⁰ Za razliku od profiliranja, prigovoriti obradi podataka u svrhu izravnog oglašavanja je moguće neovisno o tome koja je pravna osnova obrade podataka.²⁸¹ Ako ispitanik uloži takav prigovor, osobni podaci se više ne smiju obrađivati u tu svrhu.²⁸²

4. IZAZOVI BUDUĆNOSTI

Zaštita privatnosti i osobnih podataka je vrlo aktualno pravo u današnje društvu. Digitalne tehnologije i nove mogućnosti obrade i korištenja osobnih podataka dodaju novu dimenziju problemu zaštite. Sve više korisnika izražava zabrinutost u kontekstu profiliranja i bihevioralnog oglašavanja. Oglas savršeno prilagođen našim trenutnim željama i potrebama, ponekad i trenutnom razgovoru, može biti koristan, ali i izazvati osjećaj nelagode.

Međutim, u ponašanju korisnika možemo vrlo lako uočiti 'tzv. paradoks privatnosti, tj. diskrepanciju između deklariranog izražavanja visoke zabrinutosti za privatnost i istovremenog manifestiranja ponašanja kojim se iskazuje nebriga za privatnost, osobito na internetu i društvenim mrežama.'²⁸³

To je posebno očito iz činjenice da su najčešće korištene tražilice, mail servisi i društvene mreže, redom Google, Gmail i Facebook, upravo one koje su najzloglasnije po obilatom korištenju osobnim podacima svojih korisnika.²⁸⁴ Facebook je osobito bio na meti kritičara te je bio predmet brojnih afera koje su ukazale na zabrinjavajuće načine upotrebe osobnih podataka, od dijeljenja podataka trećim stranama do utjecanja na birače, no i dalje je uobičajeno na Facebooku podijeliti svoje ime, fotografiju, podatke o školovanju i zaposlenju, religijsku i političku pripadnost, itd.²⁸⁵

Takve proturječnosti se različito tumače u teoriji. Po jednoj teoriji, danas živimo u 'društvu razotkrivanja' koje karakterizira 'novo političko i društveno stanje radikalno transformiranih

²⁸⁰ GDPR, čl. 21., st. 2.

²⁸¹ Mišćenić et. al., op. cit. (bilj.122), str. 321.

²⁸² ibid., čl. 21. st. 3.

²⁸³ Pavuna, Andro, Paradoks privatnosti: empirijska provjera fenomena, Politička misao, god. 56, br. 1, 2019., str. 132.

²⁸⁴ ibid. str. 150. i 151.

²⁸⁵ ibid., str. 152.

međuljudskih odnosa i nova virtualna transparentnost koja iznova dizajnira naš društveni krajolik i transformira pojam privatnosti.²⁸⁶

Prema teoriji kognitivne disonance, 'ljudi će prije prilagoditi svoja uvjerenja ponašanju nego što će promijeniti vlastito ponašanje.'²⁸⁷ U kontekstu privatnosti, pojedinci svjesni raširenog i nekritičkog nadzora, industrije obrade podataka te posljedičnih opasnosti će prije početi vjerovati kako su oni sami zapravo nebitni, kako se neće baš njima narušiti privatnost, što vodi to toga da sami nekritički i obilato dijele svoje osobne podatke.²⁸⁸

Ipak, činjenica je da je za razvoj digitalne ekonomije i gospodarstva u kojem su osobni podaci važna pokretačka snaga, ključno razvijati povjerenje korisnika. S time u vidu, EU želi pružiti zakonodavni okvir o zaštiti podataka koje će se temeljiti na antropocentričnom pristupu inovacijama.²⁸⁹ Europska komisija zato donosi Pravila o zaštiti podataka kao katalizator povjerenja u EU-u i izvan njega, kojima želi analizirati utjecaj Opće uredbe o zaštiti osobnih podataka na korisnike.

Jedan od ciljeva je poboljšati razinu poznavanja prava na zaštitu podataka. Pojedinci u EU su sve upoznatiiji s pravilima o zaštiti podataka i svojim pravima, pa tako po istraživanju Eurobarometra iz 2019.: 'ukupno 67% ispitanika je upoznato s Općom uredbom o zaštiti osobnih podataka, 73% zna barem jedno od prava iz Uredbe, a 57% ispitanika zna da postoji nacionalno tijelo za zaštitu podataka kojem se mogu obratiti za informacije ili podnijeti pritužbe.'²⁹⁰

Ipak postoji potreba da se nastavi raditi na razini svijesti građana o toj temi. Komisija EU je u tu svrhu 2019. pokrenula novu internetsku kampanju kako bi potaknula građane da čitaju izjave o zaštiti osobnih podataka i da optimiziraju svojih postavki privatnosti.²⁹¹

Europska komisija u svom Digitalnom kompasu 2030. ističe solidarnost, blagostanje i održivost te jačanje položaja građana i poduzeća te jamstvo sigurnosti i otpornosti europskih digitalnih

²⁸⁶ ibid., str. 154.

²⁸⁷ ibid., str. 156.

²⁸⁸ ibid.

²⁸⁹ Komunikacija Komisije Europskom parlamentu i Vijeću, Pravila o zaštiti podataka kao katalizator povjerenja u EU-u i izvan njega - analiza napretka, Bruxelles, 2019., COM(2019) 374 final, str. 2.

²⁹⁰ Prva godina primjene Uredbe o zaštiti podataka: 73 % Europljana zna za barem jedno od svojih prava, https://ec.europa.eu/commission/presscorner/detail/hr/IP_19_2956, (1.6.2022.)

²⁹¹ Komunikacija Komisije Europskom parlamentu i Vijeću, op. cit., (bilj. 292), str. 7.

ekosustava kao ciljeve za budućnost.²⁹² Tijekom pandemije COVID-19 posebno je došla do izražaja važnost digitalne tehnologije, s obzirom da su se svi aspekti života prebacili u digitalnu sferu. Europska komisija je utvrdila i slabe točke europskog digitalnog prostora koje su se tada razotkrile: 'ovisnost o ključnim tehnologijama koje su često izvan EU, ovisnost o nekoliko velikih tehnoloških poduzeća, porast priljeva krivotvorenih proizvoda i kiberkrađa, pojačan utjecaj dezinformacija na demokratska društva te novi digitalni jaz koji je ukazao na novi problem digitalnog siromaštva.'²⁹³ Sve su to izazovi s kojima se potrebno suočiti u budućnosti, a za njihovo će svladavanje biti potreban zajednički napor zakonodavstva i osobnog odgovornog ponašanja.

5. ZAKLJUČAK

Pravo na privatnost je kroz povijest raslo po važnosti i prilagođavalo svoj sadržaj društvenim okolnostima. Klasičnim sferama privatnosti kao što su dom, obitelj ili dopisivanje, dodaju se nova područja gdje osobe također očekuju zaštitu privatnosti, primjerice velike baze osobnih podataka. U pravnoj se teoriji mnogo raspravljalo o sličnostima i razlikama pojmova zaštite privatnosti i prava na zaštitu osobnih podataka. Različite zemlje su tom pitanju pristupale različito, no s obzirom na globalni karakter interneta, danas se sve više nastoji pronaći zajednički okvir.

Pojava interneta je posebno snažno utjecala na pravo na privatnost. On otvara dotad neslućene mogućnosti zlorabiranja privatnosti, istovremeno pružajući i brojne blagodati, zbog čega ulazi u sve pore života pojedinaca. Potonje je osobito vidljivo od početka korištenja interneta na mobitelima. Prosječni korisnik interneta može posvjedočiti koliko češće poseže za internetom otkad ima pristup u vlastitom džepu.

Internet tako postaje područje koje se koristi svakodnevno, kao drugi dom, i u određenim aspektima korisnici očekuju jednaku razinu zaštite privatnosti. Prateći tragove nečijeg ponašanja na internetu se često može doznati više o njemu nego pretraživanjem njegove sobe.

²⁹² Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Digitalni kompas 2030.: europski pristup za digitalno desetljeće, Bruxelles, 2021, COM (2021) 118 final, str. 2.

²⁹³ Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Digitalni kompas 2030.: europski pristup za digitalno desetljeće, Bruxelles, 2021, COM (2021) 118 final, str. 2.

S obzirom da se koristi gotovo neprestano i u najrazličitijim životnim situacijama, opravdana je bojazan da bi se zloupotrebom osobnih podataka mogla ozbiljno narušiti privatnost korisnika.

Osobit osjećaj nesigurnosti stvara strah od konstantnog nadzora. Pojam svevidećeg Velikog brata prelazi iz distopijskih romana i teorija zavjera u stvarnu mogućnost. Istovremeno, lako je podleći dojmju anonimnosti koji nam pruža internet i zanemariti oprez. Tako da će se ljudi često ophoditi opreznije sa svojim osobnim podacima u stvarnom životu, primjerice s nepoznatima na ulici, nego na internetu, primjerice pri ispunjavanju obrazaca za programe vjernosti ili nagradne igre.

U pristupu zaštiti privatnosti u digitalnom kontekstu svakako nije zanemariv ljudski faktor. Potrebno je njegovati kulturu ponašanja na internetu koja obuhvaća odgovorno ponašanje na društvenim mrežama i oprez pri davanju osobnih podataka. No i uz svo odgovorno ponašanje, naša je stvarnost takva da je nemoguće u potpunosti izbjeći svaku obradu osobnih podataka. Stoga je vrlo važno postojanje pravnih pravila koja će podrobno urediti uvjete obrade.

Pravo bi uvijek trebalo ići u korak s društvenim razvojem pa tako i u slučaju zaštite privatnosti i osobnih podataka. Prateći razvoj komunikacijskih i informacijskih tehnologija, njihovu primjenu u svakodnevnom životu i utjecaj na ljudska prava te potencijalne zlouporabe, potrebno je pravovremeno donositi zakonska rješenja. U ozračju pravne sigurnosti, korisnici interneta ne moraju strahovati od profiliranja i bihevioralnog oglašavanja, već mogu koristiti pogodnosti koje oni pružaju, pouzdajući se da će zlouporabe biti kažnjene.

LITERATURA

Andrassy, Juraj; Seršić, Maja; Vukas, Branimir, *Međunarodno pravo 1*, Školska knjiga, Zagreb, 2010.

Batistić Kos, Vesna, *Pozitivne obveze prema Europskoj konvenciji za zaštitu ljudskih prava i temeljnih sloboda*, Narodne novine, Zagreb, 2012

Boban, Marija, *Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu*, Zbornik radova Pravnog fakulteta u Splitu, 49, 3/2012,

Brezak, Milan *Pravo na osobnost*, Nakladni zavod Matice Hrvatske, Zagreb, 1998.

Čizmić, Jozo; Boban, Marija, Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 39, br. 1, 2018.

Dragičević, Dragan; Gumzej, Nina; Jurić, Marko; Katulić, Tihomir; Lisičar, Hrvoje: *Pravna informatika i pravo informacijskih tehnologija*, Narodne Novine, Zagreb, 2015

Dropulić, Julijano, *Pravo na privatni život i duševni integritet*, Vizura, Zagreb, 2002.

Gavella, Nikola, *Osobna prava*, Pravni fakultet Zagreb, Zagreb 2000

Gonzalez Fuster; Gloria; Gutwirth, Serge, *Opening up personal data protection: a conceptual controversy*, Computer Law & Security Review, vol. 29, 2013.

Gumzej, Nina, *Challenges of the digital environment for personal data privacy and security*, DIT 2014, Dr. Juraj Plenković, 2014.

Gumzej, Nina; Dragičević, Dražen, *Convergence in Communications and E-Privacy Regulatory Challenges, With a Local Perspective*, 2015., u: Thomas Plank / IEEE (ur.)Proceedings of the 13th International Conference on Telecommunications, 2015.

Gumzej, Nina, *Uredba o zaštiti osobnih podataka*, 2017., projekt "Novi hrvatski pravni sustav" Pravnog fakulteta Sveučilišta u Zagrebu, 2017.

Jurić, Marko, *Pravo na poštovanje privatnog života i zaštitu osobnih podataka*, u Kregar, Josip et. al., *Ljudska prava: uvod u studij*, Zagreb, 2014.

Kamara, Irene; Kosta, Eleni, *Do Not Track initiatives: regaining the lost user control*, *International Data Privacy Law*, vol. 6., issue 4, 2016

Mišćenić, Emilia; Kunda, Ivana; Petrić, Silvija; Butorac Malnar, Vlatka; Vrbljanac, Danijela; Winkler, Sandra, *Europsko privatno pravo - posebni dio*, Školska knjiga, Zagreb, 2021

Pavuna, Andro, *Paradoks privatnosti: empirijska provjera fenomena*, *Politička misao*, god. 56, br. 1, 2019

Puvača, M. B., & Demark, A. (n.d.). *Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede*, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*. 40, 2019.

Rajko, Alen, *Informacijsko upravno pravo*, TEB poslovno savjetovanje, Zagreb, 2011.

Sudar-Kulčar, Mirna, *Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni (direktni) marketing*, *Politička misao*, vol. XLII, br. 4, 2005.

Propisi i dokumenti međunarodnih organizacija:

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*, 2014.

Deklaracija o slobodi izražavanja i informiranja je u Republici Hrvatskoj prihvaćena Zaključcima o prihvaćanju akata Savjeta Europe o slobodi izražavanja i informiranja, NN 7/91.

Direktiva 2002/58/EZ Europskog parlamenta i vijeća od 12. srpnja 2002., o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)

Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/58/EZ

Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Digitalni kompas 2030.: europski pristup za digitalno desetljeće, Bruxelles, 2021, COM (2021) 118 final

Komunikacija Komisije Europskom parlamentu i Vijeću, Pravila o zaštiti podataka kao katalizator povjerenja u EU-u i izvan njega - analiza napretka, Bruxelles, 2019., COM(2019) 374 final

Konvencija za zaštitu ljudskih prava i temeljnih sloboda, MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10,

Međunarodni pakt o građanskim i političkim pravima, rezolucija br. 2200 A /XXI

Mišljenje Nezavisnog odvjetnika Manuela Camposa Sanchez-Bordone od 12. svibnja 2016. u predmetu C-582/14, Breyer, EU:C:2016:339, para.68., 2016.

Mišljenje 06/2014 radne skupine o pojmu legitimnih interesa voditelja obrade u skladu s člankom 7. Direktive 95/46/EZ (WP217), 844/14/EN RD 217

Opća deklaracija o ljudskim pravima, rezolucija br. 217 /III

Povelja Europske unije o temeljnim pravima (2016/C 202/02)

Revidirani nacrt Rezolucije o pravu na privatnost u digitalnom dobu, A/C.3/69/L.26/Rev. 1, 2014.

Revidirani nacrt Rezolucije o pravu na privatnost u digitalnom dobu A/C.3/71/L.39/ Rev. 1, 2016

Rezolucija o pravu na privatnost u digitalnom dobu, A/RES/68/167, 2013.

Smjernice 2/2019 o obradi osobnih podataka na temelju članka 6. stavka 1. točke b Opće uredbe o zaštiti podataka u kontekstu pružanja internetskih usluga ispitanicima, Europski odbor za zaštitu podataka, 2019.

Smjernice 5/2020 o privoli na temelju Uredbe 2016/679, Europski odbor za zaštitu podataka, 2020

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119/1

Ustav Republike Hrvatske, NN 85/2010,

Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola; NN MU 4/2005

Zakon o provedbi Opće uredbe o zaštiti osobnih podataka, NN 42/2018

Web poveznice:

All about cookies, <https://allaboutcookies.org>

‘Article 29 Working Party targets device fingerprinting’,
<https://www.osborneclarke.com/insights/artikel-29-datenschutzgruppe-nimmt-device-fingerprinting-ins-visier>

AZOP: Što su izrada profila, automatizirano donošenje odluka i ciljano oglašavanje?,
<https://azop.hr/najcesce-postavljena-pitanja/>,

Cooley, Thomas M. A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract. Chicago, 1879., <https://repository.law.umich.edu/books/11/>

ESLJP, Niemietz v. Germany, 72/1991/324/396, 1992,
<https://www.refworld.org/cases,ECHR,3f32560b4.html>

Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021.
<<http://www.enciklopedija.hr/Natuknica.aspx?ID=27406>>

International Working Group on Data Protection in Telecommunications: Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential,
[https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2013/2013-WP-Webtracking-en.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/publikationen/working-paper/2013/2013-WP-Webtracking-en.pdf),

Kuneva, Meglena, Roundtable on Online Data Collection, Targeting and Profiling, 2009.,
https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156,

Priručnik o europskom zakonodavstvu o zaštiti podataka,
https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_hr.pdf,

Prva godina primjene Uredbe o zaštiti podataka: 73 % Europljana zna za barem jedno od svojih prava, https://ec.europa.eu/commission/presscorner/detail/hr/IP_19_2956

Sud Europske unije, <http://www.vsrh.hr/EasyWeb.asp?pcpid=1050>

Vodič kroz članak 8. Konvencije – Pravo na poštovanje privatnog i obiteljskog života, 2020.
<https://uredzastupnika.gov.hr/UserDocsImages/dokumenti/Edukacija/Vodi%C4%8D%20kroz%20%C4%8Dlanak%208.%20Konvencije.pdf>

Vrhovni sud SAD-a, Olmstead v. US, 277 U.S. 438, 1928,
<https://www.law.cornell.edu/supremecourt/text/277/438>

