INSTITUT ZA UPOREDNO PRAVO
INSTITUTE OF COMPARATIVE LAW

Stefan Andonović
Dragan Prlja

OSNOVI PRAVA ZAŠTITE PODATAKA O LIČNOSTI

Beograd, 2020

INSTITUT ZA UPOREDNO PRAVO

OSNOVI PRAVA ZAŠTITE PODATAKA O LIČNOSTI

Stefan Andonović
Dragan Prlja

Beograd
2020

INSTITUT ZA UPOREDNO PRAVO

OSNOVI PRAVA ZAŠTITE PODATAKA O LIČNOSTI

Izavač:
Institut za uporedno pravo
Beograd, Terazije 41

Za izdavača:
Vladimir Čolović

Recenzenti:
dr Zoran Jovanović
dr Dejan Milenković
dr Mario Reljanović

Tehnički urednik:
Dragan Prlja

Lektor i korektor:
Milena Šećerović

Štampa:
"Službeni glasnik", Beograd

ISBN 978-86-80186-57-3

*Tiraž:*200

INSTITUTE OF COMPARATIVE LAW

THE BASICS OF PERSONAL DATA PROTECTION RIGHTS

Published by:
Institute of Comparative Law
Belgrade, Terazije Street 41

For the Publisher:
Vladimir Čolović

Reviewed by:
Zoran Jovanović Ph. D.
Dejan Milenković Ph. D.
Mario Reljanović Ph. D.

Techical Director:
Dragan Prlja

Proofs:
Milena Šećerović

Printed by:
"Službeni glasnik", Belgrade

ISBN 978-86-80186-57-3

*Copies:*200

SADRŽAJ

"Religija podataka sada kaže da su svaka vaša reč
i postupak deo velikog protoka podataka, da vas algoritmi
neprekidno posmatraju i da im je stalo do svega što radite i osećate.
Većini ljudi se ovo veoma dopada.
Istinskim vernicima isključenje iz protoka podataka
znači opasnost od gubitka samog smisla života.
U čemu je svrha da išta radite ili doživljavate ako niko za
to ne zna i ako to ne doprinosi globalnoj razmeni podataka?"

Juval Noa Harari
"Homo deus: Kratka istorija sutrašnjice"

1. UVOD

Jedna od značajnih posledica razvoja informacionih tehnologija u proteklih dvadesetak godina je enormno povećanje količine podataka o pojedincima. Svakodnevno prikupljanje milijardi podataka o građanima, njihovo skladištenje u velikim bazama podataka i obrada tih podataka uz upotrebu veštačke inteligencije postala ja naša realnost. Logično je da je, paralelno sa rastom prikupljenih podataka o svakom pojedincu, drastično porasla i opasnost od zloupotrebe ovih podataka, kako od strane pojedinaca, tako i od strane kompanija i državnih institucija. Slobodan protok informacija je nužnost, ali i velika opasnost za privatnost, nezavisnost i individualnost svakog pojedinca. Stavljanje podataka u središte razvoja industrije i upravljanja društvima zahteva podizanje na visok nivo kako sistema informacione bezbednosti, tako i sistema zaštite fundamentalnih prava građana. Pored tehničkih i informatičkih aspekata bezbednosti prikupljenih podataka izuzetno je važno stvaranje kompleksnog i delotvornog pravnog sistema zaštite podataka o ličnosti.

Naša knjiga predstavlja doprinos sagledavanju različitih aspekata tog složenog pravnog sistema zaštite podataka o ličnosti. Počeli smo od samih podataka, njihovog definisanja i određivanje različitih vrsta podataka, potom smo objasnili šta pojam pravne zaštite podataka obuhvata, kakav je bio istorijat razvoja ovog prava, na kojim se načelima zasniva i kakva su prava za građane proistekla razvijanjem sistema zaštite podataka. Poseban deo knjige posvećen je predstavljanju i analizi propisa koji na međunarodnom i nacionalnom planu regulišu oblast zaštite podataka o ličnosti. Poslednje poglavlje knjige posvećeno

je praksi zaštite pojedinaca od zloupotrebe podataka o ličnosti prikazivanjem i analizom jednog broja slučajeva koji su procesuirani pred Evropskim sudom za ljudska prava, Sudom pravde Evropske unije i nacionalnim nezavisnim organima koji u svojoj nadležnosti imaju zaštitu podataka.

Šta nam donosi budućnost? To je zaista teško predvideti, ali sa velikom sigurnošću možemo konstatovati da će se broj prikupljenih i obrađenih podataka o ličnosti u već bliskoj budućnosti enormno povećati i da će pravni sistemi morati da prate te promene, odnosno da razviju još sofisticiraniji i delotvorniji sistem zaštite podataka o ličnosti. Stoga, verujemo da je od velikog značaja istraživati puteve kojima će razvoj sistema zaštite podataka ići, a naša knjiga, nadamo se, predstavlja važan korak u tom pravcu.

Autori

2. PODACI O LIČNOSTI

Da bismo mogli adekvatno da odredimo pojam podataka o ličnosti neophodno je razjasniti šta podrazumevamo pod pojmom podatak, šta podrazumevamo pod pojmom informacija, kakva su teorijska shvatanja o pojmu podataka o ličnosti i kakvo značenje se svim tim pojmovima pridaje u našim i inostranim propisima.

2.1. Određenje pojma podataka

Određenje pojma podatka, informacije i zaštite podataka o ličnosti nije nimalo lak zadatak, jer se za ove pojmove danas upotrebljavaju sasvim različita značenja.

Reč podatak je množina latinske reči "*datum*" koja označava "nešto dato". Pod pojmom *podatak* danas podrazumevamo simbole u obliku brojeva i slova ili u obliku analogne ili digitalne slike ili zvuka – koji su pogodni za prenos i interpretaciju od strane ljudi ili automatizovanog sistema, uz pomoć unapred zadatih algoritama. Podaci mogu biti činjenice o nekome ili nečemu, mogu biti statistički brojevi ili mogu biti deo informacije. Oni predstavljaju registrovane činjenice o nekom objektu posmatranja. Sami po sebi podaci nemaju nikakvo značenje. Oni su samo kodovi koji mogu biti dekodirani na osnovu određenih pravila. Kada se podaci dekodiraju i pridruže drugim podacima, kada se obrade i interpretiraju oni se pretvaraju u *informaciju*.[1] Pojam podatka se često koristi za označavanje određene karakteristike nekog bića, predmeta ili pojave. Kada podatak dobije kontekstualno značenje od strane čoveka ili automatizovanog sistema tek tada on postaje informacija i dobija svoju vrednost. Neophodna je mentalna aktivnost čoveka ili primena algoritma od strane automatizovanog sistema kako bi skup podataka bez značenja dobio kontekstualno značenje, povećao nivo znanja primaoca i postao osnova za donošenje odluka. Podaci se mogu posmatrati i kao simboli koji su tako organizovani da mogu biti obrađeni od strane čoveka ili automatizovanog sistema (računara).

Termin podatak svoju primenu pronalazi prevashodno u pravnom diskursu i pravničkoj terminologiji u vezi sa različitim pravnim institutima poput

[1] Peter Checkland, Sue Holwell, Information, *Systems and information Systems: Making Seance of the Fild*, Wiley, New York 1998, p. 18.

zaključenja ugovora, sudskih i upravnih postupaka, identifikovanja određenog lica od strane organa javne vlasti i tome slično.

Informacija predstavlja jedan od najaktuelnijih pojmova današnjice. Suštinski, ona predstavlja krajnji rezultat analize podataka o nekom predmetu ili pojavi. U tom smislu, više povezanih podataka kojima je dato neko značenje predstavljaju informaciju. Ovaj pojam upotrebljava se u svakodnevnom govoru i u različitim okolnostima, pa tako dobijamo pojmove poput informacionog doba, informacionog društva, informacione revolucije, informacione tehnologije, itd. Informacije čine toliko snažan uticaj na savremeno društvo da se moderne generacije nazivaju informacionim društvom, a doba u kome živimo označava se kao informaciono doba.[2] Upotreba pojma informacije zastupljena je i u naučnom diskursu, prilikom vršenja bezbednosnih provera, u medijskim izveštajima, itd.

Posmatrano iz pravne perspektive, između pojma podataka i informacija postoji značajna razlika koja povlači za sobom različito postupanje i različite pravne posledice. Pravnička terminologija poznaje i pojam podatka i pojam informacije. Da ova dva pojma nisu sinonimi u pravu Srbije svedoči Zakon o opštem upravnom postupku, koji u okviru svojih načela poznaje i „načelo pristupa informacijama i zaštite podataka".[3].

Što se tiče drugih pozitivno-pravnih propisa, određenje pojma podatka možemo pronaći u Zakonu o zaštiti podataka o ličnosti.[4] Podatak o ličnosti predstavlja podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta.[5] Iz izložene definicije zaključujemo – da bi jedan podatak postao informacija, on mora da nosi u sebi određeni sadržaj (značenje) o pojedinom predmetu ili pojavi (u slučaju podataka o ličnosti, podatak se odnosi na određenu karakteristiku fizičkog lica). Na osnovu ove razlike možemo zaključiti da informacija predstavlja kvalifikovan podatak koji je ispunjen određenim sadržajem, značenjem i kontekstom.

Sličan pristup određenju pojma podatka možemo pronaći u Zakonu o tajnosti podataka koji određuje „podatke od interesa za Republiku Srbiju". Podaci

---

[2] Više o pojmu informacionog društva vid. László Z. Karvalics, „Information Society – what is it exactly?" (The meaning, history and conceptual framework of an expression), Budapest 2007, p. 5-21.

[3] Čl. 15 Zakona o opštem upravnom postupku, „Sl. glasnik RS", br. 18/2016, 95/2018.

[4] Zakon o zaštiti podataka o ličnosti, „Sl. glasnik RS", br. 87/2018.

[5] Čl. 4, st. 1, tač. 1, Zakona o zaštiti podataka o ličnosti.

od interesa su svi oni podaci kojima raspolaže organ javne vlasti, a koji se odnose na teritorijalni integritet, suverenost, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbednost, odbranu, unutrašnje i spoljne poslove.[6]

U literaturi, Nible (*Niblett*) navodi da „informaciju nije lako definisati, s obzirom da se ovom izrazu pridaju različita značenja. Ona se koristi za označavanje određenih operacija u procesu upravljanja, za obaveštenja koja su sadržana u knjigama, dokumentima, člancima, novinama, različitim evidencijama i dosijeima koji se mogu obrađivati elektronskim putem".[7] Ovaj autor, takođe, zastupa stanovište da informaciju treba razlikovati od pojma podatka. U tom smislu navodi da se „podatak odnosi na činjenice ili pojmove koji mogu biti formalizovani i kao takvi biti podobni za komunikacionu manipulaciju, dok informacija nužno podrazumeva *smisao, odnosno značenje koje se tom podatku priznaje*".[8]

Osim podataka, i pojam informacije pronalazimo i u pozitivno-pravnim izvorima. Pojam informacije nalazimo u Zakonu o slobodnom pristupu informacijama od javnog značaja.[9] Ovaj zakon definiše informaciju od javnog značaja kao informaciju kojom raspolaže organ javne vlasti, koja je nastala u radu ili u vezi sa radom organa javne vlasti, a sadržana je u određenom dokumentu i odnosi se na sve ono o čemu javnost ima opravdan interes da zna.[10] Dakle, informacija predstavlja određeno *saznanje*, odnosno zapis o određenoj pojavi (podatku) koja je zabeležena, opisana ili bliže određena u nekom dokumentu. Sa tehničke strane posmatrano, informacija predstavlja *sistem znakova koje nose određeno značenje* i prenose poruku sa određenim značenjem.

2.2. Određenje pojma podataka o ličnosti

Podaci o ličnosti predstavljaju opredmećeni deo čovekove ličnosti. Čovekova ličnost[11] predstavlja kompleksnu pojavu, koja se izučava u okvirima različitih naučnih disciplina. Kao važna društvena kategorija, čovekova ličnost

---

6 Čl. 3, st. 1, tač. 2, Zakona o tajnosti podataka, „Sl. glasnik RS", br. 104/2009.

7 G. B. F. Niblett, *Digital Information and the Privacy Problem, Organization for Economic Co-operation and Development*, Paris 1971, p. 9.

8 *Ibidem.*

9 Zakon o slobodnom pristupu informacijama od javnog značaja, „Sl. glasnik RS", br. 120/2004, 54/2007, 104/2009, 36/2010.

10 Čl. 2, st. 1. Zakona o slobodnom pristupu informacijama od javnog značaja.

11 Engleski termin za ličnost (*personality*) potiče od latinskog termina persona koji označava maske glumaca u rimskim pozorištima koje su prikazivale karakter glumaca.

predstavlja predmet interesovanja pravne nauke i prakse. Svaki pravni sistem teži da pravnim normama sistematski uredi i usmeri ponašanja ljudi kako bi se obezbedila pravna sigurnost i predvidljivost u društvu. Kako su ponašanja ljudi suštinski vezana za čovekovu ličnost, ona se javljaju kao neposredni i posredni predmet normi različitih grana prava. Naravno, pravne norme ne uređuju prirodu čovekove ličnosti, budući da je to prirodna pojava na koju se ne može i ne sme uticati. Pravni sistemi prihvataju neponovljivu prirodu ličnosti i teže da joj pruže zaštitu u slobodnom razvoju od svih nedozvoljenih uticaja pojedinca i društva. Zbog kompleksne pravne prirode, čovekova ličnost kao predmet pravne zaštite nalazi se na granici između privatnog i javnog prava. Iz perspektive javnog prava, čovekova ličnost se posmatra u odnosu sa državom i njenim organima. Tačnije, čovekova ličnost se štiti u takvom odnosu, budući da država i njeni organi poseduju monopol fizičke sile koji se ne sme zloupotrebljavati prema „slabijoj" strani, odnosno građanima. Normama javnog prava (upravnog, ustavnog i krivičnog) štite se vrednosti koje su od značaja za čitavu društvenu zajednicu, ali i za pojedince. To znači da država na jednak način garantuje svim ljudima različite mehanizme pravne zaštite pred državnim organima, u slučaju nastale povrede ili štete i u vezi sa zaštitom od zloupotrebe podataka o ličnosti.

Sa druge strane, privatno pravna zaštita znači to da pojedinac može samostalno zahtevati zaštitu pred državnim organima u cilju zaštite svojih ličnih interesa. Na taj način, pojedinac preuzima aktivnu ulogu u cilju zaštite svoje društvene i pravne pozicije, koja može biti ugrožena činjenjem i nečinjenjem trećih lica. I kod privatno pravne zaštite dolazi do aktiviranja normi javnog prava, tako što u toj zaštiti učestvuju državni organi sa javnim ovlašćenjima, koji štite i privatne i javne interese. Međutim, centralno mesto u takvoj zaštiti pripada pojedincu. Privatno pravna zaštita uređena je normama građanskog prava (obligacionog, porodičnog, naslednog, itd.).[12]

Na značaj čovekove ličnosti ukazuje i činjenica da ona svoje mesto nalazi u ustavima, kao najvišim pravnim aktima država. Takav je slučaj i sa Srbijom, gde je Ustavom zajamčeno da svaki čovek ima pravo na slobodan razvoj ličnosti, ako time ne ugrožava prava drugih.[13] Dakle, čovekova ličnost predstavlja

[12] Upor. Ivana Simović, Miroslav Lazić, „Građansko pravna zaštita prava ličnosti", *Zbornik radova Pravnog fakulteta u Nišu*, br. 68, (ur. Irena Pejić), Niš 2014, str. 272-273.

[13] U istom članu u kome se garantuje slobodan razvoj ličnosti, Ustav obezbeđuje i ljudsko dostojanstvo, kao sastavni element čoveka i njegove ličnosti. Kao takvo, ono je neprikosnoveno i svi su dužni da ga poštuju i štite. Na ovaj način ljudsko dostojanstvo uživa isti stepen zaštite kao sâm ljudski život, koji je neprikosnoven. Međutim, upitna je obaveza „svih" da štite ljudsko dostojanstvo, koje je pri tom nepovredivo, što može voditi u različite logičke i pravne nedoslednosti. Vid. Čl. 23, Ustava RS, „Sl. glasnik RS", br. 98/2006.

(ustavno) pravnu kategoriju. Ona se dovodi u vezu sa slobodom, kao osnovnom vrednošću koja je neophodna za razvoj i napredak. Kako bi se očuvala posebnost čovekove ličnosti, država garantuje uslove za njen slobodan razvoj i unapređenje, ali do tačke u kojoj se ne ugrožava razvoj ličnosti drugih pojedinaca. Za razvoj ličnosti čoveka važno je to da je ljudski život neprikosnoven i da je zabranjeno kloniranje ljudskih bića.[14] Zabranom kloniranja ljudskih bića sprečava se veštačko stvaranje, odnosno reprodukcija neponovljivog sklopa čovekove ličnosti.

Garantovanje nepovredivosti psihičkog i fizičkog integriteta predstavlja još jedan stub koji doprinosi slobodnom razvoju ličnosti. Kao jedan od pravnih elemenata čovekove ličnosti, Ustav Srbije predviđa i pravo na pravnu ličnost. Pravna ličnost predstavlja pojavni oblik čovekove ličnosti u pravnim odnosima. Ona se može razumeti kao jedinstvo pravne i poslovne sposobnosti. Pravna sposobnost znači to da svako fizičko i pravno lice ima sposobnost da bude imalac prava i obaveza u pravnom životu, dok poslovna sposobnost predstavlja mogućnost da se samostalno odlučuje o svojima pravima i obavezama.[15]

Možemo zaključiti da se različiti delovi čovekove ličnosti štite drugačijim ljudskim pravima i institutima, pa se ni sama čovekova ličnost ne može posmatrati jednostrano, već jedino u korelaciji sa bliskim pravnim institutima.

Takav je slučaj i sa podacima o ličnosti, koji predstavljaju deo čovekove ličnosti koji je „angažovan" u pravnom prometu. Kao pojavni oblik čovekove ličnosti različiti podaci o ličnosti svakodnevno se upotrebljavaju i razmenjuju, označavajući i bliže određujući subjekte i druge elemente pravnog odnosa. Zbog jake veze sa samom ličnosti čoveka, povreda podataka o ličnosti ujedno predstavlja i povredu čovekove ličnosti. Kako je za opstanak pojedinca i društva neophodna zaštita privatnosti i integriteta ličnosti, značajno mesto u očuvanju čovekove ličnosti ima zaštita od zloupotrebe podataka o ličnosti. Zbog toga je neophodna kvalitetna zaštita podataka o ličnosti i temeljeno uređenje načina postupanja sa podacima o ličnosti.

---

[14] Čl. 24, Ustava RS.

[15] Fizička lica postaju imaoci pravne sposobnosti samim rođenjem, dok je pravna lica nju stiču posebnim postupkom priznanja pravne ličnosti odnosno pravnog subjektiviteta. Pravna sposobnost zajedno sa poslovnom i deliktnom sposobnošću čine pravni subjektivitet jednog lica. Radenka Cvetić, „Pravna sposobnost i biomedicina – biomedicinska diskriminacija", *Zbornik radova Pravnog fakulteta u Novom Sadu*, 3/2011, (ur. Dragiša Dakić), Novi Sad 2011, str. 349-350.

2.2.1. Podaci o ličnosti – teorijsko određenje

Podaci o ličnosti predstavljaju karakterističnu osobinu određenog lica. Oni se koriste u svakodnevnim životnim situacijama, služeći kao sredstvo konkretizacije i ostvarivanja pravnih odnosa. Međutim, podaci o ličnosti ne predstavljaju samo sredstvo identifikacije. Zapravo, oni predstavljaju pojavni oblik određene ličnosti u pravnom životu koji služi za ostvarivanje različitih prava i interesa.

Švarc (*Schwartz*) je slikovito odredio podatke o ličnosti kao „važnu valutu u novom milenijumu".[16] Ovo određenje ukazuje na ogromnu važnost koju imaju podaci o ličnosti u savremenom svetu, pa čak da je njihova uloga izjednačena sa ulogom novca. Korišćenje društvenih mreža i učestvovanje u elektronskoj komunikaciji manje zahteva novac, a više podatke o ličnosti koji predstavljaju osnovno sredstvo razmene.

Lilić navodi da se „za podatak može reći da predstavlja neku vrstu „osnovne sirovine" koja se nakon obrade, tj. procesiranja pretvara u „informaciju". Informacije se mogu koristiti u najrazličitije svrhe, odnosno registrovati i čuvati u kompjuterizovanim informacionim sistemima".[17]

Prema Purtovoj, „lični podaci jesu sistemski izvori koji ne sadrže samo pojedinačne podatke koji se odnose na pojedince koji se mogu identifikovati, već celokupan "ekosistem", koji sadrži međusobno povezane, ali odvojene elemente: 1. Sami ljudi čije postojanje stvara lične podatke, 2. Elektronske platforme dizajnirane da "uhvate" ljude, nudeći im jedinstvene elektronske usluge i istovremeno prikupljajući podatke o svojim korisnicima, 3. Lične podatke koji nisu prikupljeni direktno, već se stvaraju na osnovu ranije dostupnih ličnih podataka."[18]

Krivokapić i ostali autori *Vodiča za organe vlasti – Zaštita podataka o ličnosti*, određuju pojam podataka o ličnosti. Oni navode da podatak o ličnosti predstavlja „svaku informaciju koja se odnosi na fizičko lice, koje se u nekom trenutku može identifikovati. Dakle, da bi se konstatovao podatak o ličnosti

---

[16] Za ovu valutu se navodi da je monetarna, da je velika i da i dalje raste, pa američke korporacije brzo menjaju svoje poslovanje ka profitu od ovog trenda. Paul Schwartz, „Property, Privacy and Personal Data", *Harvard Law Review*, vol. 117, Harvard 2003, p. 2056.

[17] Stevan Lilić, „Pravni aspekti zaštite podataka u automatizovanim službenim evidencijama", *Naša zakonitost*, br. 5, Zagreb 1989, str. 616.

[18] Nadezhda Purtova, „Illusion of Personal Data as No Ones' Property", *Law, Innovation and Techonology*, vol. 7, is. 1, Taylor and Francis 2015, p. 28.

neophodno je utvrditi četiri odvojena elementa: 1. informaciju, 2. koja se odnosi, 3. na identifikovano ili podložno identifikaciji, 4. fizičko lice".[19]

2.2.2. O pojmu podataka o ličnosti u propisima evropskog prava

Jedno od prvih određenja podataka o ličnosti u uporednom pravu nalazimo u Konvenciji o zaštiti lica u odnosu na automatsku obradu podataka,[20] koju je usvojio Savet Evrope 1981. godine. Ova konvencija predviđa da podaci o ličnosti predstavljaju sve informacije koje se odnose na identifikovano lice ili lice podložno identifikaciji. U odnosu na ostale domaće i strane propise ovo je najšira definicija. Budući da je usvojena pre više od 35 godina, ovo određenje predstavljalo je pionirsku definiciju podataka o ličnosti u svetu prava, koja se nije previše menjala u godinama koje su sledile. Možemo reći da je pomenuta definicija korišćena, u izmenjenom i dopunjenom izdanju, i u kasnijim evropskim propisima.

Direktiva EU o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom protoku takvih podataka iz 1995. godine, sadržala je određenje pojma podataka o ličnosti. U okvirima Direktive, podaci o ličnosti su se odnosili na svaku informaciju koja se odnosi na određeno ili odredivo lice, pri čemu se odredivo lice može identifikovati neposredno ili posredno, posebno pomoću identifikacionog broja ili jednog ili više specifičnih faktora koji se odnose na njegov telesni, fiziološki, psihički, ekonomski, kulturni ili socijalni identitet.[21]

Osnove ove definicije sledio je i najvažniji evropski dokument u vezi sa zaštitom podataka, Uredba o zaštiti fizičkih lica u odnosu na obradu podatka o ličnosti i o slobodnom kretanju takvih podataka (Opšta uredba o zaštiti podataka EU), poznatija kao GDPR (skraćeno od *General Data Protection Regulation*) (u daljem tekstu: Opšta uredba EU),[22] čijim stupanjem na snagu je ukinuta Direktiva

---

[19] Danilo Krivokapić, Đorđe Krivokapić, Ivan Todorović, Stefan Komazec, Andrej Petrovski, Katarina Ercegović, *Vodič za organe vlasti – Zaštita podataka o ličnosti*, Share fondacija, Beograd 2016, str. 13.

[20] Konvencija o zaštiti lica u odnosu na automatsku obradu podataka, Savet Evrope, br. 108, Strazbur, 1981. god.

[21] Čl. 2, st. 1, tač. a, Direktive EU o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti i slobodnom protoku takvih podataka iz 1995. godine.

[22] Opšta uredba o zaštiti podataka EU – Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95&46EC (General Data

iz 1995. godine.[23] Opšta uredba EU daje određenje pojma podataka o ličnosti. U njoj se navodi da su podaci o ličnosti „*svi podaci koji se odnose na fizičko lice čiji je identitet određen ili se može odrediti*; fizičko lice čiji se identitet može odrediti je lice koje se može identifikovati posredno ili neposredno, posebno pomoću identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili pomoću jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog fizičkog lica".[24] Da bi se jedan podatak mogao odrediti kao podatak o ličnosti on mora nositi karakteristiku koja se odnosi na određeno fizičko lice ili fizičko lice koje se može odrediti, pri čemu se dobijena informacija odnosi na određeno lično i jedinstveno svojstvo konkretnog fizičkog lica, što je rešenje prihvaćeno iz Direktive.

Neki od podataka o ličnosti koje obuhvata prethodna definicija jesu: ime, prezime, nadimak, elektronska adresa, adresa i poštanski broj, poslovna adresa ili lokacija, državljanstvo, podaci iz izvoda iz matične knjige rođenih, pasoša, lične karte ili putne vize, fizička obeležja (boja kose, očiju), fiziološka obeležja (podaci iz zdravstvenog kartona), kulturni identitet (članstvo u kulturnim organizacijama), socijalni identitet (profili na društvenim mrežama), broj socijalnog osiguranja, audio snimci, video snimci, fotografije, brojevi telefona, podaci o lokaciji, istorija pretraživanja sajtova, digitalni potpis i dr.[25] Definicija Opšte uredbe EU identična je određenju podataka o ličnosti iz Zakona o zaštiti podataka o ličnosti Srbije.

2.2.3. O pojmu podataka o ličnosti u pravu Srbije

U pravnom sistemu Srbije, pojam podataka o ličnosti ne možemo pronaći u Ustavu, iako ovaj akt uređuje pitanje zaštite podataka o ličnosti. Određenje pojma podataka o ličnosti ostavljeno je propisima niže pravne snage, odnosno posebnom zakonu. Tako je pojam podataka o ličnosti određen u Zakonu o zaštiti podataka o ličnosti.

Prema zakonskoj definiciji, podatak o ličnosti predstavlja „*svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv*, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni

Protection Regulation), of 27. April 2016, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.*

[23] Upor. Andrej Diligenski, Dragan Prlja, Dražen Cerović, *Pravo zaštite podataka – GDPR*, Institut za uporedno pravo, Beograd 2018, str. 23.

[24] Čl. 4, st. 1, tač. 1, Opšte uredbe EU.

[25] Vid. A. Diligenski, D. Prlja, D. Cerović (2018), str. 27-29.

broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta".[26]

Da bi jedan podatak predstavljao podatak o ličnosti on mora da se odnosi na fizičko lice, što isključuje pravna lica iz obima zaštite. Nije važan način i sredstvo putem koga se saznaju, kao ni koja vrsta podataka je u pitanju. Na kraju, podatak o ličnosti mora se odnositi na posebnu karakteristiku fizičkog lica koja ga čini jedinstvenim, pri čemu je neophodno da se radi o konkretnom licu ili o licu koje može biti određeno (odredivo) na osnovu činjenica konkretnog slučaja.

Ovo određenje razlikuje se od definicije koja je sadržana u prethodnom Zakonu o zaštiti podataka o ličnosti (2008).[27] Prethodni zakon određivao je podatak o ličnosti kao „svaku informaciju koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije (papir, traka, film, elektronski medij i slično), po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja, način saznavanja informacije (neposredno, putem slušanja, gledanja, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana) ili bez obzira na drugo svojstvo informacije".[28]

Prethodni zakon izjednačavao je podatak o ličnosti sa konkretizovanom informacijom. Takvo rešenje nije bilo adekvatno budući da se mora praviti razlika između informacije i podatka, pa je bolje podatak o ličnosti odrediti po svojoj pravnoj prirodi, nego ga određivati u odnosu sa informacijom. U ovom određenju pojma podatka o ličnosti više se išlo za tim da se relativizuje način saznavanja, nosač, oblik i vrsta konkretnog ličnog podatka.

Pojam podatak o ličnosti u propisima prava u Srbiji izjednačen je sa pojmom podataka o ličnosti u propisima evropskog prava.

2.3. Vrste podataka o ličnosti

Podaci o ličnosti u današnjem svetu imaju veliku upotrebnu vrednost. Oni se koriste kao sredstvo raspoznavanja lica, identifikacioni faktor, informacioni resurs, itd. Oni su potrebni u velikom broju pravnih odnosa kako bi ti odnosi proizveli pravne posledice. Takođe, oni su neophodni da bi se sprovela kazna, prebacila novčana sredstva na račun, prenela svojina, prepisala odgovarajuća

[26] Čl. 4, st. 1, tač. 1, Zakona o zaštiti podataka o ličnosti.
[27] Zakon o zaštiti podataka o ličnosti, „Sl. glasnik SRJ", br. 24/98 i 26/98.
[28] Čl. 3, st. 1, tač. 1, Zakona o zaštiti podataka o ličnosti (2008).

terapija, dodelilo lično ime, uručila sportska nagrada, itd. Kako se koriste u svakodnevnim odnosima i u različite svrhe, postoji i veliki broj podataka o ličnosti.

Značajnu ulogu u rasprostranjenosti podataka o ličnosti imaju informaciono-komunikacione tehnologije preko kojih se objavljuje i razmenjuje veliki broj podataka o ličnosti. Samim tim, neprestano raste i broj podataka o ličnosti koji se upotrebljavaju u svakodnevnom životu, pa se tako i pravna zaštita pruža različitim kategorijama podataka. Ipak, i pored velike rasprostranjenosti i široke upotrebe, pravni sistemi ne pružaju fizičkim licima mogućnost zaštite svim podacima o ličnosti.

Podaci o ličnosti mogu se klasifikovati na različite načine. Razlika se može praviti između podataka u ličnoj, istorijskoj, finansijskoj, javnoj i društvenoj sferi života pojedinca.[29] Pomenuta podela se može suziti tako da prati podatke u tri osnovne oblasti života pojedinca. To su privatna, javna i profesionalna oblast života pojedinca. Fizičko lice ima svoju ličnu sferu, koju obično ne deli sa javnošću, javnu sferu koja se deli i sa kojom je obično upoznat veći broj ljudi ili svi zainteresovani i profesionalnu sferu u koju se ubrajaju podaci u vezi sa poslovnim aktivnostima lica. Ove oblasti neretko se poklapaju, pa podaci o ličnosti koji se upotrebljavaju u jednoj oblasti društvenog života imaju veliki značaj i u ostale dve.

2.3.1. Podaci o ličnosti koji se odnose na lični život pojedinca

U podatke koji se odnose na lični život pojedinca spadaju: psiho-fizički elementi lica (godine života, fizičke i psihičke karakteristike kao što su boja kože, težina, visina, oblik tela, razvijenost, itd.), istorija o ličnom životu (podaci o događajima i dešavanjima u životu tog lica i sa njime povezanih lica), uverenja i mišljenja (lična mišljenja izražena u vezi sa određenom temom, religijska uverenja, filozofska uverenja, itd.), lični stavovi i naklonost lica prema stvarima, licima i pojavama (omiljena vrsta hrane, omiljena boja, pesma i drugo).

U ovu grupu možemo svrstati i druge identifikacione podatke lične prirode, kao što su podaci o etničkom i socijalnom poreklu lica (rasa, nacionalna i etnička pripadnost, jezici koje govore, akcenti kojima se služi upotrebom jezika, itd.), podaci o seksualnosti (rodna pripadnost, seksualna naklonost, istorija

[29] Enerprivacy Consulting Group, „Categories of Personal Information“, online 2017, *https://enterprivacy.com/2017/03/01/categories-of-personal-information*.

ljubavnih odnosa, itd.), medicinski podaci i podaci o zdravlju (fizička i psihička zrelosti i zdravlje, fizički i psihički nedostaci, istorija bolesti, krvna grupa, zdravstveni karton, itd.).

2.3.2. Podaci o ličnosti koji se odnose na javni život pojedinca

U lične podatke koji se tiču javnog života pojedinca ubrajaju se oni podaci o ličnosti koji se odnose na segmente života pojedinca u društvenoj zajednici. Ovde možemo svrstati podatke o porodičnom životu (da li lice ima porodicu, veličina porodice, odnosi u porodici, itd.) podatke o socijalnom okruženju (prijatelji, konekcije, pripadnost u formalnim i neformalnim organizacijama, itd.), podatke o kriminalnoj prošlosti lica (da li je osuđivano, da li se vode postupci protiv njega, itd.).

2.3.3. Podaci o ličnosti koji se odnose na profesionalnu oblast života pojedinca

Podaci koji se tiču profesionalne sfere života jednog lica govore o društvenim aktivnostima lica u vezi sa radom i obavljanjem profesionalnih delatnosti. To su podaci o obrazovanju (da li je i koje forme obrazovanja lice pohađalo i završilo, ocene, završeni kursevi, itd.), poslovni podaci (da li je lice zaposleno, na kom radnom mestu, ocene o rezultatima rada, podaci o odsustvu sa posla, itd.), finansijski podaci (brojevi računa, banke u kojima su uskladištena sredstva tog lica, podaci o ličnoj imovini lica, kreditni status lica, itd.), radna istorija (podaci o firmama u kojima je radilo lice, podaci o zaposlenima u firmi tog lica, podaci o novčanim primanjima i transakcijama, itd.).

Sve navedene vrste podataka po svojoj pravnoj prirodi predstavljaju podatke o ličnosti. Oni sadrže karakteristiku o određenom segmentu života fizičkog lica, za koga su vezani i na koga se odnose. Ovi podaci su nekada dostupni isključivo licu na koga se odnose, dok su u određenim slučajevima dostupni povezanim licima ili široj društvenoj zajednici.

2.3.4. Podela na „obične“ i „posebne“ kategorije podataka o ličnosti

Moguće je izvršiti podelu na „obične“ lične podatke i „osetljive“ lične podatke,[30] koji se još nazivaju i „posebna kategorija“ podataka o ličnosti. Ova podela pravi razliku podataka o ličnosti u zavisnosti od stepena poverljivosti i značaja koji lični podatak ima za fizičko lice. „Obični“ podaci o ličnosti nose uobičajenu informaciju o fizičkom licu, dok „osetljivi“ podaci o ličnosti nose posebno značajnu informaciju o ličnom identitetu fizičkog lica.

Povreda osetljivih podataka o ličnosti, po pravilu, proizvodi značajniju posledicu za fizičko lice od povrede običnih podataka o ličnosti. Shodno ovoj podeli, osetljivi podaci o ličnosti uživaju veći stepen pravne zaštite u odnosu na druge vrste podataka o ličnosti. U grupu osetljivih podataka o ličnosti ubrajaju se podaci o verskim i filozofskim uverenjima, rasno i etničko poreklo, genetski podaci, biometrijski podaci, podaci o seksualnom životu i seksualnoj orijentaciji fizičkog lica i podaci o zdravstvenom stanju.[31] Ostali podaci o ličnosti spadaju u grupu „običnih“ podataka o ličnosti.

2.3.5. Podela na lične podatke maloletnih lica i lične podatke punoletnih lica

Moguće je napraviti razliku između podataka o ličnosti maloletnih i punoletnih fizičkih lica. Ovo razlikovanje zasniva se na drugačijim mehanizmima zaštite i načinu ostvarivanja zaštite podataka o ličnosti u zavisnosti od subjekata kojima pripadaju. Zaštita podataka o ličnosti maloletnih lica zahteva prisustvo roditelja ili drugog zakonskog zastupnika u vezi sa pojedinim pitanjima zaštite, na način kako je to objašnjeno u posebnom delu o starosnoj granici za uživanje zaštite podataka o ličnosti. Takođe, u odnosu na lične podatke maloletnih lica u propisima se uspostavljaju i posebne uloge rukovaoca i obrađivača podataka, poput dužnosti proveravanja saglasnosti roditelja ili staratelja.

---

[30] U prethodnom Zakonu o zaštiti podataka o ličnosti (2008), za ove podatke koristio se termin „naročito osetljivi podaci o ličnosti“. Ipak, smatramo da to nije opravdan naziv, budući da zakon nije pominjao „osetljive lične podatke“, niti razliku između „osetljivih“ i „naročito osetljivih“ podataka o ličnosti.

[31] Naravno, lista naročito osetljivih podataka o ličnosti zavisi od pravnog sistema i procene zakonodavca koji to podaci o ličnosti treba da uživaju veći stepen zaštite u odnosu na druge.

2.3.6. Podaci o ličnosti koji (ne) uživaju pravnu zaštitu

2.3.6.1. Podaci o ličnosti koji (ne) uživaju pravnu zaštitu u pravnom sistemu Srbije

Sistem zaštite teži da obuhvati što više podataka o ličnosti kako bi se zaštitio što veći deo čovekove ličnosti i privatnosti. Ipak, određene vrste podataka ostaju izvan „kišobrana" zaštite. Takav je slučaj sa onim ličnim podacima koji su manje važni, koji su dostupni javnosti ili koji se ne mogu zloupotrebiti. U pozitivno-pravnom zakonodavstvu Srbije obično se navode kategorije podataka o ličnosti koji uživaju zaštitu i one kategorije kod kojih pravna zaštita izostaje.

U pravu Srbije izvan sfere pravne zaštite podataka o ličnosti ostaju oni podaci koji se obrađuju od strane fizičkih lica za lične potrebe ili potrebe njihovog domaćinstva. U ovoj situaciji stepen opasnosti od propusta i zloupotreba nije previše izražen, pa samim tim izostaje i zaštita države. Kada se obrada podataka o ličnosti vrši u lične i porodične svrhe, fizičko lice na koje se odnose ti podaci i koje vrši obradu, mora samo voditi računa o bezbednosti takve obrade. Ovo je jedina grupa podataka o ličnosti kojima Zakon o zaštiti podataka o ličnosti uskraćuje pravnu zaštitu.

Raniji Zakon o zaštiti podataka o ličnosti (2008) predviđao je znatno širi krug podataka o ličnosti koji su izostajali iz domašaja pravne zaštite. Grupe podataka o ličnosti kod kojih je izostajala pravna zaštita su:

1. Podaci koji su dostupni svakome i objavljeni u javnim glasilima i publikacijama ili pristupačni u arhivama, muzejima i drugim sličnim organizacijama,
2. Podaci koji se obrađuju za porodične i druge lične potrebe i nisu dostupni trećim licima,
3. Podaci o članovima političkih stranaka, udruženja, sindikata, kao i drugih oblika udruživanja koji se obrađuju od strane tih organizacija, pod uslovom pismene izjave da se ne primenjuju odredbe ovog zakona, najduže do vremena trajanja članstva lica koje je dalo izjavu,
4. Podaci koje je lice sposobno da se samo stara o svojim interesima objavilo o sebi.[32]

U prvom slučaju, aktom objavljivanja podaci o ličnosti postaju dostupni javnosti, pa im svako zainteresovano lice može pristupiti i dalje ih koristiti. Javnim objavljivanjem oni gube garantovanu „privatnost". Na taj način, izostaje i zaštita koja država uobičajeno pruža. U ovu kategoriju spadaju podaci u pisanim

[32] Čl. 5 Zakona o zaštiti podataka o ličnosti (2008).

dokumentima, fotografije, audio zapisi i drugi javno objavljeni podaci o ličnosti. Osim njih, tu su i podaci o ličnosti koji su od značaja za širu društvenu zajednicu (istorijska istraživanja, muzejske postavke, itd.), pa pravna zaštita koja se pruža ličnim podacima ne bi bila adekvatna zbog interesa javnosti da bude upoznata sa određenim činjenicama i podacima.

Kada se radi o podacima o ličnosti koji se obrađuju u porodične svrhe, polazi se od pretpostavke da je porodica posebna grupa blisko povezanih članova koje znaju podatke jedni o drugima. Takav je slučaj sa telefonskim imenicima, porodičnim knjigama i zapisima, albumima sa fotografijama, itd. Ukoliko nisu dostupni trećim licima oni ostaju u okvirima porodice, pa zaštita države u ovom slučaju izostaje.

Slična je situacija i sa podacima o ličnosti fizičkih lica koja se udružuju u posebne grupe i udruženja povezana zajedničkim interesima njihovih članova. Zbog toga se pretpostavlja da će se privatnost ovih podataka štiti u okvirima takvih grupa i organizacija. Ovde pripadaju podaci o ličnosti članova grupe, zaduženja i način obavljanja delatnosti u okviru grupe, podaci o finansijskim i drugim davanjima organizaciji, i tome slično.

Kada fizičko lice samo objavi podatke o svom ličnom životu pravni sistem prihvata njegovu slobodu volju da podeli lične podatke sa trećim licima. Međutim, tako objavljeni podaci više nemaju strogo lični karakter, pa samim tim izostaju iz državne zaštite. To je slučaj sa pisanim objavama, audio i video zapisima i fotografijama objavljenim na društvenim mrežama. Da bi jedan podatak predstavljao deo ove grupe, lice koje ga objavljuje mora biti poslovno sposobno. U suprotnom je učinjena objava ništavna i takvi podaci ne smeju se obrađivati ni koristiti.

Ipak, predviđen je i izuzetak u odnosu na podatke koji ne uživaju pravnu zaštitu. Naime, pravnu zaštitu je uživalo lice kome su povređeni takvi podaci kada u konkretnom slučaju „očigledno pretežu interesi tog lica“. Očiglednu pretežnost morao je da utvrdi nadležni organ, na osnovu dokaza i iskaza lica o čijim podacima je reč.

Iako ima opravdanja za uskraćivanje pravne zaštite pomenutim grupama podataka o ličnosti predviđenih Zakonom o zaštiti podataka o ličnosti (2008), smatramo da je bolje rešenje novog zakona koji poznaje samo jednu grupu podataka koja ne uživa pravnu zaštitu. Na ovaj način povećava se stepen pravne sigurnosti i predvidljivosti, budući da veći broj podataka ostaje pod „kišobranom“ pravne zaštite.

2.3.6.2. Podaci o ličnosti koji (ne) uživaju pravnu zaštitu u pravu EU

U pravnom sistemu zaštite podataka EU određene kategorije podataka o ličnosti takođe ostaju izvan pravne zaštite. Ovi podaci zadržavaju lični karakter, ali ne uživaju pravnu zaštitu. U skladu sa Opštom uredbom EU, podaci o ličnosti koji ne uživaju zaštitu kao podaci o ličnosti su:

1. Podaci koji se obrađuju u okviru delatnosti koja nije obuhvaćena područjem primene prava Unije,
2. Podaci koje države članice EU obrađuju prilikom objavljivanja aktivnosti koje su obuhvaćene područjem primene poglavlja 5. dela Ugovora o Evropskoj Uniji,
3. Podatke koje obrađuje fizičko lice za isključivo lične ili porodične aktivnosti,
4. Podaci koje obrađuju nadležni organi u svrhu sprečavanja istrage, otkrivanja ili gonjenja učinioca krivičnih dela ili izvršenja krivičnog dela,[33]
5. Podaci koji se odnose na lica koja nisu živa.

U prvu grupu spadaju oni podaci koji se obrađuju izvan teritorijalne i funkcionalne nadležnosti Opšte uredbe EU, odnosno organa EU i njenih država članica. Radi se o obradama podataka o ličnosti koji se odvijaju u državama koje nisu članice EU, kao i u međunarodnim organizacijama koje nisu povezane sa EU, pod uslovom da se ti podaci ne odnose na državljane država članica EU.

Važan deo suverenosti koji nije prenet na evropske institucije od strane država članica odnosi se na njihovu nacionalnu bezbednost. Kada države članice obrađuju lične podatke u vezi sa pitanjima nacionalne ili javne bezbednosti, tada se ne primenjuje pravo EU, odnosno ne mogu se koristiti mehanizmi zaštite Opšte uredbe EU, već posebni propisi država članica.

Mehanizmi pravne zaštite Opšte uredbe EU ne mogu se koristiti ni prilikom obrade podataka o ličnosti koju vrše države članice u vezi sa zajedničkom spoljnom i bezbednosnom politikom EU. To je materija koju uređuje 5. deo Ugovora o funkcionisanju EU (odnosno Lisabonski sporazum) - Delovanje Unije na spoljnom planu. Ovaj deo reguliše pitanja poput zajedničke trgovinske politike država članica, saradnje sa trećim državama i humanitarnu pomoć, međunarodne sporazume, odnose Unije sa trećim državama itd.[34] Na neki način i

[33] Čl. 2, st. 2, Opšte uredbe EU.

[34] Vid. deo 5. Ugovora o funkcionisanju Evropske unije, odnosno Ugovor iz Lisabona kojim se menja Ugovor o Evropskoj Uniji i Ugovor o uspostavljanju Evropskih zajednica, br. 207/S

ova pitanja su povezana sa bezbednošću i integritetom unije i njenih članica. Pomenute formulacije su apstraktne i ostavljaju prostor za potencijalne zloupotrebe podataka o ličnosti, pod parolom nacionalne bezbednosti ili bezbednosti Unije.

Treću grupu podataka o ličnosti koji ne uživaju pravnu zaštitu jesu podaci koje fizička lica obrađuju u lične i porodične svrhe. U ovim situacijama izostaje reakcija države, jer ne postoji potreba za uplivom države u strogo ličnu sferu pojedinca. Samim tim, pretpostavlja se da je obrada podataka o ličnosti u lične ili porodične svrhe privatna stvar o kojoj prevashodno mora da vodi računa lice čiji su podaci.

Podaci o ličnosti koji obrađuju nadležni organi (policija, tužilaštvo) u cilju primene odredaba krivičnih i prekršajnih propisa, a radi gonjenja učinioca krivičnih i prekršajnih dela ostaju izvan zaštite koju pruža Opšta uredba EU. Postupanje sa takvim ličnim podacima uređuje se posebnim propisima koji uređuju pravila postupanja organa koji rade na rasvetljavanju i gonjenju učinioca krivičnih dela.

Već je pomenuto da se pravila o zaštiti podataka o ličnosti odnose isključivo na fizička lica koja su živa, pa se ličnim podacima preminulih lica ne pruža pravna zaštita.

2.3.8. Posebne kategorije podataka o ličnosti

2.3.8.1. Posebne kategorije podataka o ličnosti u pravu Srbije

Pojedine vrste podataka o ličnosti ne uživaju pravnu zaštitu. Međutim, postoje i druge vrste podataka o ličnosti koje uživaju veći stepen zaštite u odnosu na onu koja se uobičajeno pruža. Javljaju se posebne kategorije podataka o ličnosti koje se ne smeju obrađivati. Ove kategorije uživaju posebnu zaštitu, budući da se odnose na karakteristike osetljive prirode i njihovom povredom ili zloupotrebom može doći da značajnih negativnih posledica po fizičko lice na koje se odnose. Povreda ovih kategorija podataka o ličnosti može imati uticaja na društvenu poziciju, ugled i status određenog lica.

Posebne kategorije podataka o ličnosti postoje i u pravnom sistemu Srbije. Ova grupa podataka nekada je nosila naziv (naročito) osetljivi podaci o ličnosti, kako ih je imenovao prethodni Zakon o zaštiti podataka o ličnosti (2008). Aktuelni Zakon o zaštiti podataka o ličnosti određuje ovu vrstu podataka, kao

306/01, deo pod nazivom „Spoljne akcije Unije“. Ugovor iz Lisabona, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2007:306:FULL&from=HR*.

„posebnu kategoriju“ podataka o ličnosti, čija obrada nije dozvoljena, osim pod određenim uslovima.[35] U ovu grupu spadaju podaci koji se odnose na:

1. Rasno i etničko poreklo,
2. Političko mišljenje,
3. Versko i filozofsko uverenje,
4. Članstvo u sindikatu,
5. Genetske podatke,
6. Biometrijske podatke,
7. Podatke o zdravstvenom stanju,
8. Podatke o seksualnom životu i seksualnoj orijentaciji lica.[36]

Ipak postoje određene situacije u kojima je dozvoljena njihova obrada.[37] Takve situacije odnose se na postojanje određenog oblika javnog interesa ili pretežnijeg privatnog interesa u odnosu na interes lica čiji se podaci obrađuju.

Ukoliko ne bi postojala mogućnost obrade posebnih podataka, pravni sistem ne bi mogao normalno da funkcioniše i redovni društveni tokovi bi bili sputani i usporeni. Zbog toga, sistem zaštite podataka o ličnosti Srbije predviđa nekoliko situacija u kojima je moguće obrađivati posebne podatke. Prilikom obrade ovih podataka neophodno je da organ uprave preduzme razumne i odgovarajuće mere u cilju zaštite prava i interesa lica čiji se podaci obrađuju, kao poseban uslov obrade.

Obrada posebnih kategorija podataka može se vršiti uz pristanak lica o čijim podacima je reč. Kada postoji izričita i jasna saglasnost, nema prepreka obradi posebnih podataka o ličnosti. Smatra se da pristanak za obradu postoji i kada je lice na koje se podaci odnose učinilo javnim takve podatke, pa se i u takvim situacijama može vršiti obrada.

Pojedine posebne podatke mogu obrađivati i različite organizacije, poput udruženja, fondacija i zadužbina, ali isključivo u svrhu funkcionisanja organizacije. Mogu se obrađivati jedino podaci članova organizacija ili sa organizacijom povezanih lica, uz dodatan uslov da se takvi podaci ne objavljuju izvan organizacije. Takođe, u vezi sa organima uprave, rukovaoci u oblasti rada, socijalnog osiguranja i socijalne zaštite imaju pravo da obrađuju posebne podatke kada je takva obrada neophodan uslov izvršenja obaveze organizacije. Takva obrada mora biti predviđena posebnim zakonom ili kolektivnim ugovorom o radu, što znači da nije dovoljna pojedinačna odluka rukovaoca.

---

[35] Više o uslovima dopuštenosti obrade posebnih kategorija podataka o ličnosti u srpskom pravu vid. čl. 17, st. 2, Zakona o zaštiti podataka o ličnosti.

[36] Čl. 17, st. 1, Zakona o zaštiti podataka o ličnosti.

[37] Posebni slučajevi mogućnosti obrade posebnih vrsta podataka o ličnosti predviđeni su u čl. 17, st. 2, Zakona o zaštiti podataka o ličnosti.

Obradu posebnih kategorija podataka mogu vršiti i sudski organi kada postupaju u poslovima iz svoje nadležnosti. Potreba pravičnog vođenja sudskog postupka i saznavanja istine u postupku zahteva temeljnu analizu svih činjenica konkretnog slučaja, koje se mogu odnositi i na posebne kategorije podataka. U vezi sa sudskim i drugim pravnim postupcima, treba pomenuti da je dozvoljena obrada posebnih kategorija podataka koja se odvija u cilju podnošenja, ostvarivanja ili odbrane od pravnog zahteva.

Postoje situacije u kojima se mogu obrađivati posebne podaci radi zaštite javnog zdravlja. Tako, obrada može se preduzeti radi ostvarivanja preventivnih dužnosti u medicini ili medicini rada, a u cilju ocenjivanja radne sposobnosti zaposlenih i budućih zaposlenih, što mora biti utemeljeno na zakonu ili kolektivnom ugovoru. Dozvoljene su obrade posebnih kategorija podataka radi ostvarivanja zdravlja stanovništva, kada posebnim zakonom moraju biti predviđene dodatne mere zaštite.

Upravni organi mogu vršiti obradu posebnih kategorija podataka kada postoji potreba za ostvarivanjem „značajnog javnog interesa". Postojanje takvog interesa procenjuje postupajući organ u vršenju svojih dužnosti, ali on mora biti propisan zakonom. Čak i kada postoji značajan javni interes, upravni organ kod obrade posebnih kategorija podataka mora voditi računa o *principu srazmernosti* i poštovanju suštine prava fizičkih lica čiji se podaci obrađuju.

Situacija koja ostavlja najviše prostora za polemiku jeste mogućnost obrade osetljivih podataka *u svrhe arhiviranja u javnom interesu*, u svrhe naučnog ili istorijskog istraživanja i u statističke svrhe.[38]

Ova odredba postavljena je suviše široko i dozvoljava relativno lak pristup posebnim kategorijama podataka. Kao dodatni uslov za vršenje ovakvih obrada predviđeno je poštovanje suštine prava na zaštitu podataka i primena odgovarajućih i posebnih mera zaštite podataka koji se obrađuju. Statističke i istorijske svrhe dozvoljavaju široko tumačenje u okviru koga se mogu obrađivati značajni podaci građana. Ovu odredbu trebalo bi postaviti znatno uže, tako da predstavlja predmet posebnog zakona koji bi predvideo dodatne uslove, poput dužnosti obrazloženja svake obrade u pomenute svrhe.

Za razliku od zakona koji je trenutno na snazi, prethodni Zakon o zaštiti podataka o ličnosti (2008) predviđao je kategoriju „naročito osetljivih podataka". On je sadržao dužu listu „posebnih", odnosno naročito osetljivih podataka. U odnosu na trenutno stanje stvari, kao naročito osetljivi podaci bili su predviđeni i pol, jezik, pripadnost političkoj stranci, podaci o primanju socijalne pomoći, podaci o žrtvama nasilja i podaci o osudi za učinjeno krivično delo.

[38] Čl. 17, st. 2, tač. 10, Zakona o zaštiti podataka o ličnosti.

Značajna odredba u odnosu na obradu naročito osetljivih podataka odnosila se na to da je i mere zaštite i način arhiviranja podataka iz ove kategorije uređivala Vlada, uz prethodno pribavljeno mišljenje Poverenika. Ova odredba je izostala u novom zakonu. Takvo pravilo je predstavljalo dodatni stepen zaštite osetljivih podataka, budući da su upravni organi morali da postupaju prema odluci Vlade i mišljenju Poverenika, što govori o većem stepenu važnosti ovih podataka. Takav princip treba široko prihvatati u oblasti zaštite podataka, jer što je više stepena zaštite, manja je opasnost od povrede (osetljivih) podataka o ličnosti.

2.3.8.2. Posebne kategorije podataka o ličnosti u pravu EU

Opšta uredba EU takođe poznaje određene kategorije podataka o ličnosti koji uživaju posebnu zaštitu.[39] Ovi podaci nose naziv „posebne kategorije podataka o ličnosti".[40] Oni se odnose na rasno i etničko poreklo, političko opredeljenje, verska i filozofska ubeđenja, pripadnost sindikatu, obradu genetskih i biometrijskih podataka, zdravstveno stanje, seksualni život i seksualnu orijentaciju fizičkog lica.[41] U odnosu na domaće propise, primećujemo da je lista „posebnih kategorija podataka o ličnosti" nešto duža u odnosu na „naročito osetljive podatke" iz srpskog prava.

Za posebne kategorije podataka smatra se da su „po svojoj prirodi posebno osetljivi u pogledu osnovnih prava i sloboda (koje štite) i zaslužuju posebnu zaštitu, jer bi u okviru njihove obrade moglo da dođe do značajnih rizika za osnovna prava i slobode".[42] Međutim, i u posebnim kategorijama podataka o ličnosti postoje podaci koji uživaju poseban tretman. Naime, državama članicama je ostavljena mogućnost da unutrašnjim propisima dodatno urede uslove koji se odnose na obradu genetskih podataka, biometrijskih podataka i podataka o zdravstvenom stanju. Ove kategorije podataka mogu direktno uticati na život i psiho-fizički integritet fizičkih lica, pa njihova obrada zaslužuje regulativu koja obuhvata i posebnosti određenog društva i njegovih članova.

Obrada posebnih kategorija podataka o ličnosti u pravu EU je zabranjena. Ipak, javljaju se određene situacije koje opravdavaju i čine obradu ovih kategorija podataka legalnom.

---

[39] Za više vid. Paul Lambert, *Understanding the New European Data Protection Rules*, CRC Press, 2018, p. 112-115.

[40] U teoriji se navodi da je za ovu vrstu podataka uobičajen naziv „osetljivi podaci". A. Diligenski, D. Prlja, D. Cerović (2018), str. 43.

[41] Čl. 9, Opšte uredbe EU.

[42] Tač. 52 Preambule, Opšte uredbe EU.

Prva grupa situacija koja opravdava obradu posebnih kategorija podataka o ličnosti tiče se pojedinca čiji se podaci obrađuju. Obrada posebnih kategorija je dozvoljena ukoliko postoji izričit pristanak njihovog imaoca na obradu, kada je neophodno da se izvrši obrada radi zaštite osnovnih životnih interesa lica na koje se podaci odnose i kada je takve podatke očigledno objavilo lice na koje se podaci odnose.

Druga grupa situacija odnosi se na posebne obrade podataka o ličnosti. Vrste obrade koje opravdavaju upotrebu posebnih kategorija podataka o ličnosti odnose se na ciljeve rukovaoca i obrađivača u oblasti rada, prilikom zapošljavanja, ostvarivanja prava iz socijalnog osiguranja i socijalne zaštite i prilikom obrada koje preduzimaju fondacije, udruženja i drugi neprofitni oblici udruživanja, kada su usmerene na podatke njihovih članova.

Treća grupa situacija koja opravdava obradu posebnih kategorija podataka o ličnosti tiče se ostvarivanja značajnih javnih interesa. To su situacije kada sud obrađuje posebne kategorije podataka radi ispitivanja pravnih zahteva, kada je obradu neophodno sprovesti u medicinske svrhe i svrhe javnog zdravlja, kao i kada obradom treba da se ostvari svrha naučnog, istorijskog ili statističkog istraživanja.

U svakoj od ovih situacija, rukovalac i obrađivač moraju imati adekvatan zakonski osnov koji je utemeljen na konkretnim činjenicama koje opravdavaju obradu posebnih kategorija podataka o ličnosti. Uz to, rukovalac i obrađivač moraju posvetiti posebnu pažnju zaštiti ljudskih prava u vezi sa ovakvim obradama, pri čemu moraju imati u vidu pravo EU i pravo države članice.

2.3.9. Baze podataka o ličnosti

2.3.9.1. Teorijski pristup bazama podataka

U današnjem svetu podaci o ličnosti prikupljaju se u različite svrhe. Njih prikupljaju privatni rukovaoci i obrađivači u poslovne namene, ali i organi države, radi obavljanja javnih poslova i omogućavanja normalnog odvijanja društvenih tokova. Podaci o ličnosti koji prikupe organi uprave čuvaju se i koriste, u najvećem obimu, u digitalnoj formi. U takvim situacijama, prikupljanjem velikog broja podataka o ličnosti stvaraju se baze podataka, odnosno organizovani skupovi podataka o ličnosti. „Baze podataka i tehnologija baza podataka ima ogroman značaj u razvoju računara. Pošteno je reći da baze podataka imaju odlučujuću ulogu u skoro svim oblastima u kojima se koriste računari, poput poslovanja, elektronske trgovine, inženjerstva, medicine, genetike, prava,

obrazovanja i bibliotekarstva…".[43] Ove reči bliže opisuju značaj koje imaju baze podataka u današnjim informacionim sistemima. Bez baza podataka informacioni sistemi se ne mogu ni zamisliti. Njihova važnost ogleda se u strukturi informacija koje su pohranjene i koje se mogu brzo i lako koristiti u različite svrhe u raznim oblastima društvenog života.

Teorijski, baze podataka se određuju kao organizovani skup podataka o ličnosti.[44] Dakle, nije dovoljno prikupiti lične podatke, već je neophodno sistematizovati ih i čuvati ih po određenom obrascu. Kada govorimo o organima uprave, njihove ranije baze podataka sastojale su se od velikog broja papirnih dokumenata sa ličnim podacima. Razvoj informaciono-komunikacionih tehnologija omogućio je uštedu vremena i prostora, pa su se baze podataka digitalizovale.

Danas se baze podataka obično čuvaju u elektronskom obliku, pohranjene u memoriji računara ili u virtuelnom obliku u „oblacima" (eng. *clouds*). Oni predstavljaju jedinstveno mesto gde se može pristupiti sačuvanim podacima određene kategorije ili vrste, radi njihovog preuzimanja i daljeg korišćenja u određene svrhe. Zbog toga su baze podataka našle svoje mesto u pravnim sistemima širom sveta, pa i u Srbiji, posebno u vezi sa delatnostima elektronske javne uprave.

2.3.9.2. Baze podataka u pravnom sistemu Srbije

Upravljanje bazama podataka treba da bude uređeno zakonom ili drugim podzakonskim aktima. U Srbiji, Zakon o zaštiti podataka o ličnosti, ne uređuje na poseban način upravljanje i vođenje bazama podataka, ali na podatke koji čine određenu bazu mogu se primeniti odredbe o čuvanju i pristupu podacima o ličnosti.

Sa druge strane, rukovođenje bazama podataka predstavlja jedan od predmeta uređenja Zakona o informacionom sistemu Republike Srbije.[45] Ovaj zakon uređuje način postupanja organa uprave prilikom vođenja evidencija i upravljanja podacima u vezi sa informacionim sistemom Republike Srbije. Sadržaj baze podataka čine podaci čije je vođenje predviđeno zakonom, a tako formirane baze podataka predstavljaju informacioni podsistem društvene oblasti u vezi sa kojim se i čuvaju podaci o ličnosti. Određenje pojma baze podataka sadrži

---

[43] Ramez Elmasri, Shamkant Navathe, *Fundamentals of Database Systems*, Addison-Wesely Publishing Company, Boston – Columbus - ets. 2010, p. 4.

[44] Ramez i Navte daju jednostavnije određenje baza podataka kao kolekcije povezanih podataka. Upor. *Ibidem*.

[45] Zakon o informacionom sistemu Republike Srbije, „Sl. glasnik RS", br. 12/1996.

i Zakon o elektronskoj upravi, koji određuje bazu podataka kao organizovan i uređen skup međusobno povezanih struktuiranih podataka koji može imati jednu ili više evidencija.[46]

Zakon o informacionom sistemu Republike Srbije poznaje i kategoriju zajedničke baze podataka koja predstavlja centralni registar iz kojeg organi i organizacije uprave povlače podatke kada su im neophodni za vođenje posebnih evidencija ili posebnih baza podataka. Dakle, zajedničke baze podataka predstavljaju elektronsku magistralu kojoj se može pristupiti pod određenim uslovima radi preuzimanja pojedinog podatka.

Od izuzetnog je značaja voditi računa o mogućnosti pristupa ovom registru, jer postoji veliki broj organa uprave, pa je važno tačno odrediti subjekte i razlog pristupa bazi, kako bi se izbegle zloupotrebe. Svaki korisnik mora da prođe kroz proces odobrenja koji se prolazi upotrebom elektronskih identifikacionih podataka korisnika. Na taj način, obrazovanjem baze podataka, ostvaruje se i zaštita podataka o ličnosti, budući da se vodi evidencija subjekata koji pristupaju bazi.

Organi uprave moraju da vode i sekundarne (alternativne) baze podataka koje omogućavaju konstantnost u radu, ukoliko se jave problemi na primarnoj bazi podataka. Sekundarne baze ne smeju da se čuvaju na istom mestu gde i primarne baze podataka. Pravilo je i da se sve baze podataka čuvaju u Srbiji, a samo uz posebne mere bezbednosti mogu da se iznose van teritorije Republike Srbije.

2.3.9.3. Značaj baza podataka za funkcionisanje države i društva

Važnost baza podataka za obavljanje delatnosti države i za normalno odvijanje društvenih tokova od velikog je značaja.[47] Pravilno donošenje odluka i preduzimanje mera mora se zasnivati na potpuno utvrđenom činjeničnom stanju konkretnog slučaja. Međutim, činjenično stanje je moguće potpuno utvrditi jedino uzimanjem u obzir svih elemenata slučaja koji se neretko mogu naći pohranjeni u odgovarajućoj bazi podataka. Imajući u vidu da organi uprave svoje delatnosti

[46] Čl. 4, st. 1, tač. 1 Zakona o elektronskoj upravi, „Sl. glasnik RS“, br. 27/2018.

[47] Potreba za bazama podataka posledica je činjenice rasta uloge i značaja informacija u savremenom svetu i informaciono orijentisanom društvu. Zbog toga, baze podataka imaju veliki značaj kao centralno mesto gde se može pohraniti veliki broj informacija u vidu tekstova, podataka, slika, audio i video sadržaja, itd. Mark Davison, *The Legal Protection of Databases*, Cambridge University Press, Cambridge – New York – Melbourne 2003, p. 2.

vrše u raznim oblastima života (zdravstvo, kultura, poljoprivreda, vodoprivreda, itd.), otuda postoje i različite baze podataka koja se čuvaju.

Različite baze podataka mogu pružiti značajne informacije za rešavanje nespornih i spornih situacija društva i građana, što može da bude od značaja za ubrzanje upravnog postupka. Takođe, one se koriste kao sredstvo koje pomaže organima da brže i efikasnije obavljaju svoje delatnosti, bilo da se radi o javnom interesu ili o interesu stranke, odnosno fizičkog lica čijim podacima se u bazi pristupa.

Zbog velike praktične primene u različitim oblastima života baze podataka predstavljaju sredstvo koji pomaže razvoju države i društva. Stoga, napredak informacionih tehnologija otvara nove mogućnosti upotrebe baza podataka. Podaci o ličnosti i baze podataka o ličnosti posebno dobijaju na značaju i praktičnoj primeni u sadejstvu sa informaciono-komunikacionim tehnologijama. To se posebno odnosi na perspektivnu informacionu oblast velikih baza podataka, odnosno *big data*, u koju se sve više ulaže i koja se brzo razvija.

2.3.10. Big data i podaci o ličnosti

2.3.10.1. Određenje pojma big data

Velike baze podataka o ličnosti mogu se koristiti kao sredstvo za efikasnije donošenje poslovnih i državnih odluka, unapređenja tehničkih i stručnih postupaka i za predviđanje ponašanja subjekata na koje se podaci iz baze odnose. To je od velikog značaja za rad organa uprave koji mogu koristiti grupe podataka za donošenje odluka, preduzimanje mera i radnji zasnovanim na rezultatima analize velikog broja podataka koji se odnose na pojedinu oblast društvenog života, u kojoj oni imaju nadležnost.[48]

Baze podataka koji su na sistemski način povezane i umrežene korišćenjem informaciono-komunikacionih tehnologija nose naziv *big data*. Teorijski posmatrano, pojam *big data* se „odnosi na projektovanje i realizaciju pouzdane, distribuirane i skalabilne infrastrukture za upravljanje, analizu, deljenje, skladištenje i prenos velikih količina podataka. Potreba za ovakvom infrastrukturom nastaje zbog skupova podataka koji su toliko veliki da ih nije

[48] Upor. Christian Döpke, „The Importance of Big Data for Jurisprudence and Legal Practice“, *Big Data in Context- legal, Social and Technological Insights*, (eds. Thomas Hoeren, Barbara Kolany-Raiser), Springer, online 2018, p. 14.

moguće obraditi pomoću standardnih pristupa i alata".[49] Drugi određuju pojam *big data* preko osnovnih karakteristika, odnosno osnovnih sastavnih elemenata. Sikular (*Sicular*) navodi da *big data* predstavlja „obiman, brz i raznovrsan sistem informacija koji omogućava štedljive i inovativne oblike obrade podataka koji omogućavaju kvalitetnije odlučivanje i donošenje odluka".[50]

Velike skupove podataka karakteriše različitost sadržaja koji se nalaze u njima. Podaci mogu biti u različitim oblicima, poput teksta, zvuka i slike. Takođe, sistemska povezanost podataka omogućava veliku brzinu u njihovoj razmeni i pristupu, što je još jedna od odlika *big data* sistema.

[49] Božidar Radenković, Marijana Despotović-Zrakić, Zorica Bogdanović, Dušan Barać, Aleksandra Labus, *Elektronsko poslovanje*, Fakultet organizacionih nauka, Beograd 2015, str. 278.

[50] Svetlana Sicular, „Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three 'V's", Forbes, online 2013, *http://www.forbes.com/ sites/ gartnergroup 2013/03/27/gartners-big-data-definition-consists-of-threeparts-not-to-be-confused-with-three-vs/*. Upor. Hugh Watson, "Tutorial: Big Data Analytics: Concepts", *Technologies and Application, Communications of the Associations for Information Systems*, vol. 34, art. 65, The Berkeley Electronic Press, Berkeley 2014, p. 1249, *https://pdfs.semanticscholar.org/ d392/ 0f02dbb15da19b04d782fc0546ef113e0bf7. pdf*.

3. ZAŠTITA PODATAKA O LIČNOSTI

3.1. Pojam zaštite podataka o ličnosti

U današnjem modernom društvu, podaci o ličnosti se koriste u velikoj meri na svakodnevnom nivou. Podatke o ličnosti koriste građani, privredni subjekti, organi javne vlasti i međunarodne organizacije, dakle svi subjekti koji učestvuju u pravnom i poslovnom prometu. Kupovina stvari preko interneta, deljenje slika i fotografija na društvenim mrežama, zakazivanje termina u policiji radi dobijanja nove lične karte, učestvovanje u igrama na sreću preko interneta, predstavljaju samo neke od brojnih situacija u kojima se koriste podaci o ličnosti. Zbog toga su oni jedan od najvažnijih resursa savremene privrede i neophodan element komunikacije. Tako se i javlja stanovište da podaci predstavljaju naftu 21. veka.

Veliki broj situacija u kojima se koriste podaci o ličnosti otvara mnoge mogućnosti za napredak privrede i društva. Međutim, napredak otvara vrata i različitim opasnostima. Opasnosti, odnosno rizici javljaju se po same podatke o ličnosti, ali i po prava i slobode građana na koji se podaci odnose. U ugroženu grupu prava spadaju: pravo na privatnost, pravo na slobodu, pravo na porodični život, pravo na nepovredivost prepiske i mnoga druga prava. Zbog toga, međunarodne organizacije, države, građani i drugi društveni faktori ukazuju na potrebu zaštite podataka o ličnosti u savremenom svetu.

Imajući u vidu specifičnu prirodu podataka o ličnosti, njihova zaštita može biti višedimenzionalna. „Priroda i stepen pravne zaštite podataka, u kranjoj liniji, zavise od stepena političkog značaja koji se pridaje ličnim pravima, odnosno zaštiti privatnosti i ličnih podataka u odgovarajućim uslovima“.[51] Podatke o ličnosti moguće je zaštititi pomoću sistema fizičke, informacione i pravne zaštite. Svaki od ovih sistema neraskidivo je povezan sa ostalima. Nazivi sistema zaštite potiču od metoda i načina zaštite, pa je u okviru svakog od ovih sistema moguće razlikovati konkretne mere kojima se pruža zaštita podacima o ličnosti. Naravno, moguće je napraviti i podelu mera zaštite. Ukratko, možemo

[51] Stevan Lilić, „Zaštita ličnih podataka u pravu Srbije i evropski standardi“, u *Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske unije* (ur. Duško Dimitrijević, Brano Miljuš), Institut za međunarodnu politiku i privredu, Beograd 2010, str. 442.

napraviti razliku između tehničkih, organizacionih i pravnih mera zaštite podataka o ličnosti. Kao i kod sistema, zaštitne mere najbolje dejstvo postižu uzajamnim delovanjem i primenom na različite aspekte podataka o ličnosti i elemente obrade.

Imajući u vidu da zaštita podataka u celini predstavlja gotovo nepreglednu oblast**,** *naš fokus u ovoj knjizi biće usmeren na pravni sistem zaštite i mere koje se predviđaju u okvirima tog sistema***.** U tom smislu, možemo govoriti o pravnom sistemu zaštite podataka o ličnosti, kao širem pojmu i o pravnim merama u okviru tog sistema, kao užem pojmu.

U ovoj glavi analiziraćemo pojam pravne zaštite podataka o ličnosti, istorijat pravne zaštite, kao i osnovne principe i prava građana na kojima se zasniva pravna zaštita podataka o ličnosti. Na taj način napravićemo teorijsku osnovu za razumevanje kompleksnih pravnih instituta. Tako ćemo čitaocima olakšati razumevanje često složenih pravnih instituta u vezi sa podacima o ličnosti.

3.1.1. Pravna norma kao osnovni element pravnog sistema zaštite podataka o ličnosti

Svesni smo da se teorijska razmatranja neretko zaobilaze pri proučavanju bilo koje pojave. Ipak, kako u ovom radu težimo da prikažemo osnove pravne zaštite podataka o ličnosti, ukratko ćemo se osvrnuti na same temelje prava i sistema koje obrađujemo.

Osnovni element svakog pravnog sistema predstavlja pravna norma**.** Pravna norma predstavlja pravilo ponašanja koje uređuje različite odnose između lica, pojava i stanja. Funkcije pravnih normi u sistemu zaštite podataka o ličnosti odnose se na uređivanje, usmeravanje, usklađivanje i oblikovanje ponašanja različitih lica u vezi sa podacima o ličnosti. U tom smislu, one imaju za cilj da uspostave koherentan i funkcionalan sistem u okviru koga se smanjuju mogućnosti zloupotrebe i rizici nepravilnog i nezakonitog korišćenja podataka. Na taj način štite se građani, njihova prava, interesi i slobode. Takođe, time se pruža mogućnost za slobodno i sigurno poslovanje, u okviru koga se mogu predvideti prava i obaveze svih učesnika u poslovnim poduhvatima. Na kraju, pravne norme omogućavaju i sigurnost građana u odnosu prema državi i njenim organima.

Pomenuli smo da pored pravnih, postoje organizacione, tehničke, moralne i druge vrste normi. Jedna od osnovnih razlika pravnih normi, u odnosu druge vrste normi nalazi u njihovom dejstvu. Naime, samo one imaju pravno dejstvo koje se ostvaruje kroz pravno relevantne posledice u vidu prava ili obaveze. Pored

toga, njihova snaga ogleda se i kroz mogućnost sprovođenja u život putem monopola državne prinude (izvršitelji, policija, vojska), što nije odlika ostalih vrsti normi. Druge norme mogu imati samo posredni efekat, kada su uobličene u pravnu normu.

3.1.2. O sistemima zaštite podataka o ličnosti

Kada govorimo o sistemu pravne zaštite podataka o ličnosti, govorimo o složenoj mreži načela, prava i obaveza, pravnih instituta i mehanizama njihovog ostvarivanja. Svi ti elementi predstavljaju delić šire slike. Zbog toga, svi elementi pravne zaštite ne mogu se posmatrati odvojeno od fizičkih ili informacionih sredstava i mera. *Jedan od osnovnih ciljeva sistema pravne zaštite podataka o ličnosti jeste uspostavljanje pravila koja imaju za cilj zaštitu građana i privrede, kao i uspostavljanje predvidljive i moralno ispravne oblasti društvenog života, koja se tiče podataka o ličnosti*.

Sistem zaštite ličnih podataka može biti uspostavljen na različitim nivoima. Posmatrajući od opšteg ka posebnom, najopštiji sistem zaštite podataka o ličnosti jeste onaj koji se ustanovljava na *međunarodnom planu*, kroz internacionalne forume i međunarodne konvencije i ugovore. Budući da je zaštita podataka o ličnosti relativno nova, neistražena i osetljiva oblast (zbog različitih interesa i brojnih mogućnosti korišćenja podataka), međunarodni sistem podataka o ličnosti gotovo i da ne postoji u pravom smislu reči. Ovaj sistem trenutno se sastoji od nekoliko međunarodnih ugovora kojima se samo posredno štite podaci o ličnosti i to pretežno zaštitom prava na privatnost, neretko, samo određenih grupa lica. Takav je slučaj sa Konvencijom Ujedinjenih nacija o pravima deteta. Međutim, čak i ovi ugovori moraju da prođu kroz postupak ratifikacije, odnosno prihvatanja u nacionalnom zakonodavstvu (primer: Zakon o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta[52]), kako bi stupili na snagu u jednoj državi i na taj način dobili punu pravnu snagu i mogućnost izvršavanja.

Osim međunarodnog, možemo govoriti o *regionalnom sistemu pravne zaštite podataka o ličnosti*. U vezi sa Srbijom u ovom smislu relevantne su organizacije Evropske Unije i Saveta Evrope, budući da je Srbija strateški i pravno opredeljena pripadnosti evropskim principima i vrednostima. Evropska unija je usvojila niz propisa na regionalnom planu, od kojih je najpoznatiji i najznačajniji *Opšta uredba o zaštiti podataka EU*, što ne umanjuje značaj ostalih

[52] Zakon o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta, „Sl. list SFRJ“ br. 15/1990 i „Sl. list SRJ“, br. 4/1996 i 2/1997.

direktiva i odluka sudova EU. Sistem zaštite podataka o ličnosti polako se uspostavlja i razvija na teritoriji EU, kroz praksu sudova, organa javne vlasti i nezavisnih nadzornih organa država članica. Trenutno, Srbija nije država članica EU, što znači da se na njenoj teritoriji ne primenjuju propisi EU. Ipak, kao kandidat za članstvo Srbija teži da uskladi svoje zakonodavstvo sa EU, što je evidentno u odnosu Opšte uredbe EU i domaćeg Zakona o zaštiti ličnih podataka, koji skoro predstavljaju preslikane propise.

Savet Evrope predstavlja regionalnu međunarodnu organizaciju evropskih zemalja čije članstvo uživa i Srbiji. Pojedini dokumenti koji su usvojeni pod okriljem Saveta Evrope odnose se na pravo privatnosti i zaštitu podataka o ličnosti. Ipak, i u ovom slučaju teško možemo govoriti o postojanju pravog regionalnog sistema pravne zaštite podataka o ličnosti. Od važnijih dokumenata u vezi sa pravom privatnosti i ličnim podacima ističemo Evropsku konvenciju o zaštiti ljudskih prava i osnovnih sloboda (1950) i Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka (1991). Neophodno je pomenuti i Evropski sud za ljudska prava koji štiti prava i slobode ustanovljene konvencijom i svojom praksom utiče na razvoj ljudskih prava u državama članicama.

Praktično, pravi sistem zaštite podataka o ličnosti uspostavlja se tek na *državnom nivou*. Država donosi propise - Ustav, zakone, podzakonske akate, kao i pojedinačne pravne akte preko kojih se opšti propisi sprovode u život. Na taj način ustanovljavaju se pravila koja pokrivaju različite elemente zaštite podataka o ličnosti koje su dužni da poštuju i primenjuju svi subjekti koji potpadaju pod primenu domaćeg prava. Tako, u Srbiji, odredbe u vezi sa podacima o ličnosti mogu se pronaći u Ustavu, Zakonu o zaštiti podataka o ličnosti, Zakonu o opštem upravnom postupku, Krivičnom zakoniku, Zakonu o obligacionim odnosima, Zakonu o javnim nabavkama i mnogim drugim. Treba voditi računa da potvrđeni međunarodni ugovori, kao i opšteprihvaćena pravila međunarodnog prava predstavljaju izvor prava u Srbiji, pa tako Konvencija o zaštiti lica u odnosu na automatsku obradu podataka predstavlja deo domaćeg pravnog sistema. Pored državnog nivoa i zahvaljujući njemu, uspostavljaju se *interni sistemi zaštite podataka u okvirima organa javne vlasti i privrednih subjekata*. Ovi subjekti uspostavljaju unutrašnje sisteme zaštite, tako što donose pravila koja se zasnivaju na opštim pravnim aktima, putem kojih se konkretizuju opšte pravne norme. Ovi subjekti donose i pojedinačne akte kada donose odluke u vezi sa konkretnim slučajevima u oblasti zaštite podataka o ličnosti.

3.1.3. Određenje pojma pravne zaštite podataka o ličnosti

Pojam pravne zaštite podataka o ličnosti može se zasnivati na različitim kriterijumima. Na prvom mestu, pravnu zaštitu možemo odrediti prema tehničkim elementima – pravnim normama. To bi značilo da pravna zaštita podataka o ličnosti znači ustanovljavanje i primenu pravnih normi u vezi sa zaštitom podataka o ličnosti.

Pomenuti pojam moguće je odrediti i prema objektu koji se štiti pravnim normama, odnosno prema materiji koja se reguliše. Objekti zaštite su podaci o ličnosti, ali i prava i slobode fizičkih lica u vezi sa njima. Na ovaj način, dolazimo do *materijalnog pojma pravne zaštite podataka o ličnosti*, kao načina ustanovljavanja i primene pravila kojima se štite prava fizičkih lica u vezi sa podacima o ličnosti, ali i sami podaci o ličnosti, kao nematerijalno dobro čoveka.

U teoriji se javlja i *funkcionalni pojam pravne zaštite podataka o ličnosti*. On se odnosi na načine ostvarivanja utvrđenih ciljeva zaštite, odnosno na sva sredstva i mere koje su neophodne za postizanje bezbednosti podataka građana i njihovih prava i sloboda. Prema ovom teorijskom stanovištu, funkcionalni (formalni) pojam zaštite podataka određen je obavljanjem aktivnosti:

1. ograničenja raspolaganja određenim vrstama podataka,
2. obaveze (ne) davanja informacija nedržavnim subjektima, državnim organima i organizacijama,
3. obaveštavanja građana o podacima koji se o njima prikupljaju i u koju svrhu.[53]

Pored pomenutih aktivnosti, smatramo da se mogu uvrstiti i dodatni elementi i mere zaštite kako bi ovaj pojam bio sveobuhvatan. Ti elementi tiču se uređivanja pravila postupka pred nadležnim organima u vezi sa zaštitom podataka o ličnosti, kao i primene sankcija u slučaju njihove povrede.

Na osnovu svega navedenog, možemo izvesti sveobuhvatan pojam pravne zaštite podataka o ličnosti. Pod pojmom pravne zaštite podataka o ličnosti podrazumeva se *proces donošenja i primene opštih i posebnih pravnih normi, na međunarodnom, državnom i internom planu, što podrazumeva implementaciju tehničkih i organizacionih pravila i uspostavljanje pravnih mehanizama i*

[53] Dragan Prlja, Mario Reljanović, *Pravna informatika*, Službeni glasnik, Beograd 2010, str. 87.

sredstava u cilju zaštite prava na privatnost, kao i drugih prava i sloboda građana u vezi sa podacima o ličnosti.[54]

Pomenuto određenje obuhvata elemente tehničkog, materijalnog i funkcionalnog pojma zaštite, čime se dobija kompletan pojam pravne zaštite podataka o ličnosti koji uvažava teorijska razmišljanja, ali i praktična u ovoj oblasti. Pomenuto određenje omogućava nezavisnost pojma pravne zaštite podataka o ličnosti od promenljivih elemenata pravnog sistema i društvenog razvoja.

3.2. Istorijat pravne zaštite podataka o ličnosti

Zaštita podataka o ličnosti predstavlja jednu od najaktuelnijih teorijskih i praktičnih tema u svetu prava. Aktuelnost ove oblasti prouzrokovana je povećanom ulogom podataka i njihovim masovnim korišćenjem u svakodnevnim aktivnostima, ali i ogromnom ulogom interneta, društvenih mreža (*Facebook, Instagram, Youtube*, itd.). Pored dozvoljenih i opravdanih aktivnosti, podaci se koriste za razumevanje ponašanja korisnika, za praćenje ljudi i posmatranje njihovog ponašanja, za ucene, prisluškivanje i mnoge druge delatnosti.

U periodu koji je prethodio pojavi informaciono-komunikacionih tehnologija i interneta, podaci o ličnosti nisu imali preveliki značaj. Oni su korišćeni kao sredstvo prepoznavanja u svakodnevnom životu („Zdravo, ja sam Marko“ i učestvovanja u društvenim i pravnim odnosima („Kupac, Marko Marković, iz sela Marković). Države su posedovale skromne baze podataka koje su se prevashodno odnosile na nepokretnosti i druge stvari koje su im omogućavale prikupljanje poreza i drugih dažbina. Uz to, sve do Francuske buržoaske revolucije ljudska prava nisu bila previše zanimljiva državama, koje su funkcionisale na nešto drugačijem političkom uređenju nego većina današnjih. Osim toga, svet nije bio globalizovan u današnjem smislu, pa su i privredni i poslovni odnosi bili mnogo manjeg obima i zahtevali manje podataka. Zbog toga, možemo zaključiti da je povećanje interesovanja države, privrede i građana javlja tek sa pojavama globalizacije, interneta, informaciono-komunikacionih sistema i mogućnostima koje one nude.[55] *To znači da se razvoj pravne zaštite podataka o ličnosti vezuje tek za poslednje decenije 20. veka*.

---

[54] Vid. Stefan Andonović, *Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti*, doktorska disertacija, Pravni fakultet Univerziteta u Beogradu, Beograd 2019, str. 134.

[55] Stevan Lilić, Dragan Prlja, *Pravna informatika veština*, Pravni fakultet Univerziteta u Beogradu, Beograd 2010, str. 112.

Ipak, kao prelomni momenat, koji se može uzeti kao sam začetak prava zaštite podataka o ličnosti, navodi se 1890. godina i teorijsko ustanovljavanje prava na privatnost, kao preteče prava na zaštitu podataka o ličnosti.

3.2.1. Ustanovljavanje prava na privatnost

Kao teorijski koncept, pravo na privatnost potiče od „prava da se bude ostavljen na miru" (*right to be left alone*), koji su kreirali američke sudije *Samuel Warren*-a i *Louis Brandais*-a, krajem 19. veka.[56] Dvojica sudija su u prestižnom časopisu *Harvard Law Review* objavili rad pod naslovom „*Pravo na privatnost*".[57] Kao osnovni cilj rada autori su naveli potrebu da razmotre da li postojeće (tadašnje) pravo poznaje princip na koji se sudovi mogu pozivati u cilju zaštite lične sfere pojedinca, i u slučaju potvrdnog odgovora, kakva je priroda i obim takve zaštite. Autori su konstatovali da je pravo pojedinca da uživa punu zaštitu ličnosti i imovine staro koliko i običajno pravo (*common law*), ali da je došao period kada je neophodno definisati pravu prirodu tog prava, budući da se tokom vremena menjala priroda i obim drugih prava, kao što je slučaj sa pravom na život i pravom na imovinu, itd.

Povećana moć javne vlasti, novi tehnološki pronalasci i modeli poslovanja stvorili su potrebu za zaštitom ličnosti „što sudija *Cooley* naziva „pravom da se bude ostavljen na miru". Dakle, vidimo da je pravo na privatnost prevashodno formulisano u praksi kao svojevrstan odgovor na neprimerene fotografije štampe (novinara) koje su tražile senzaciju i zadirale u privatni život pojedinaca. U ovom radu ukazano je na potrebu da se zbog takvih pojava i zadiranja u lični život pojedinaca omoguće pravna sredstva koja bi ukazala na jasnu liniju između javnog i privatnog života. Značajna misao u radu odnosi se na ograničenje prava na privatnost i sredstva za njegovu zaštitu. Autori konstatuju da pravo na privatnost ne može da spreči objavljivanje informacije koje su u javnom interesu. Taj princip poznat je i u savremenim pravnim sistemima.

Vremenom, došlo je do kritike u ovakvom pristupu i definisanju prava na privatnost. Kako se navodi, „i pored neizlečive nepreciznosti ove formulacije, ima nečeg zavodljivog u pokušaju da se privatnost izjednači s uznemiravanjem, tj. s

56 Predrag Dimitrijević, „Pravna regulacija elektronske komunikacije i pravo na privatnost, *Zbornik radova Pravnog fakulteta Univerziteta u Istočnom Sarajevu* (ur. Goran Marković), Pravni fakultet u Istočnom Sarajevu, Istočno Sarajevo 2011, str. 202.

57 Warren, Brandeis, „The Right to Privacy", Harvard Law Review, vol. IV, no. 5, 1890, https://groups.csail.mit.edu/mac/classes/6.805/ articles/privacy/ Privacy_brand _warr2.html.

idejom da se bude ostavljen na miru ono što filozofi nazivaju negativnom slobodom. Izjednačavanje ovih pojmova je pogrešno i može izazvati zablude."[58]

Nezavisno od kritike formulacije, rad pomenutih sudija imao je ogroman uticaj na dalji razvoj pravne nauke i prakse. Autoritet sudija i časopisa u kome je objavljen, izvršio je uticaj na kreiranje novih propisa, iz kojih će gotovo vek kasnije nastati pravo na zaštitu podataka o ličnosti. No, konstituisanju ovog prava prethodio je dug period utvrđivanja i potvrđivanja prava na privatnost.

3.2.2. Razvoj prava na privatnost na međunarodnom planu

I pored stvaranja svesti o neophodnosti poštovanja ljudskih prava, svet je morao da prođe katastrofe dva svetska rata kako bi se odlučnije zahtevala zaštita osnovnih prava i sloboda građana, među kojima je i pravo na privatnost. Nakon svetskih ratova, usvojen je jedan od najznačajnijih međunarodnih dokumenata. Reč je *Univerzalnoj deklaraciji o ljudskim pravima*, koja je usvojena u Parizu 1948. godine od strane Generalne skupštine Ujedinjenih nacija.[59] Iako u većini država na svetu ne predstavlja formalni izvor prava, Deklaracija je osnažila građane sa brojnim ljudskim pravima koja će svoje mesto naći i u kasnijim međunarodnim i državnim propisima. Takav je slučaj i sa *pravom na privatnost*.

U samoj preambuli Deklaracije pominje se pravo na privatnost, čime se ukazuje na njegov veliki značaj. „Pošto je priznavanje urođenog dostojanstva i jednakih i neotuđivih prava svih članova porodice temelj slobode, pravde i mira u svetu,… pošto je stvaranje sveta u kojem će ljudska bića uživati slobodu govora i ubeđenja i biti slobodna od straha i nestašice proglašeno kao najviša težnja svakog čoveka... pošto su odlučili (narodi Ujedinjenih nacija) da podstiču društvenih napredak i poboljšaju uslove života u većoj slobodi...".[60]

Konkretne odredbe u vezi sa pravom na privatnost nalazimo u članu 12. Deklaracije. Ovaj član predviđa da *niko ne sme biti izložen proizvoljnom mešanju u privatni život, porodicu, stan ili prepisku, niti napadima na čast i ugled, pri čemu svako ima pravo na zakonsku zaštitu od takvog mešanja ili napada*.[61] Dakle, nije dovoljno samo predvideti ovo pravo, već je neophodno da potpisnice

---

[58] Artur Schafer, „Privacy – A Philosophical Overview", Aspects of Privacy Law (ed. Dale Gibson), Butterworth, Toronto 1980, str. 5-8.

[59] Organizacija Ujedinjenih Nacija, Univerzalna deklaracija Ujedinjenih nacija o ljudskim pravima, 217 (III), od 10. decembra 1948. godine, Pariz.

[60] Vid. Uvod (preambulu) Univerzalne deklaracije o ljudskim pravima.

[61] Vid. čl. 12, Univerzalne deklaracije o ljudskim pravima.

Deklaracije obezbede i njegovu primenu u svakodnevnom životu. Primećujemo da pravo na privatnost nije apsolutnog karaktera, već da se zaštita pruža samo od „proizvoljnog mešanja" drugih lica. To znači da fizička i pravna lica, a posebno organi javne vlasti, mogu da u određenom delu „zađu" u privatnu sferu pojedinca, ali samo ako je takvo mešanje utemeljeno na propisima, kao i na odgovarajućem i pretežnijem privatnom ili javnom interesu.

Nedugo nakon usvajanja Univerzalne deklaracije, 1950. godine, pod okriljem Saveta Evrope usvojena je Evropska konvencija o ljudskim pravima (Konvencija Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda),[62] koja je stupila na snagu 1953. godine. Kao jedno od najvećih dostignuća Konvencije svakako se ističe stvaranje Evropskog suda za ljudska prava, kao nadnacionalnog suda koji štiti prava utvrđena konvencijom i svojom praksom utiče na adekvatnu primenu tih prava u državama članicama Saveta Evrope. Danas, zahvaljujući odlukama ovog suda, države isplaćuju godišnje milionske odštete zbog povrede prava i sloboda građana.

Pravo na privatnost predviđeno je u okviru šireg *prava na poštovanje privatnog i porodičnog života* koji je regulisan, sada već čuvenim, *članom 8*. *„Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. Javna vlast ne sme da se meša u vršenje ovog prava, osim ako je takvo mešanje predviđeno zakonom i ako je to neophodna mera u demokratskom društvu, radi zaštite interesa nacionalne bezbednosti, javne sigurnosti, ekonomske dobrobiti, sprečavanja nereda ili sprečavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih"*.[63] Vidimo da je zakonodavna vlast jedina merodavna da uvodi ograničenja privatnost i to samo u posebnim slučajevima koji se tiču zaštite javnih interesa i potreba šireg broja građana jedne države. Privatnost obuhvata tri segmenta čovekovih ličnih dobara. Prvi se odnosi na zaštitu fizičkog i moralnog integriteta pojedinca, drugi se tiče privatne sfere pojedinca u najširem smislu reči, dok se treći segment odnosi na slobodu čovekove ličnosti.[64]

Uočavamo da se pod pravom na privatnost koje je predviđeno ovim članom nije predviđeno i pravno na zaštitu podataka o ličnosti. Ipak, praksa Evropskog suda za ljudska prava podvela je to pravo u okvire prava na poštovanje privatnog i porodičnog života. Evropski sud za ljudska prava stao je na stanovište da država ima dužnost da se uzdrži od prikupljanja, čuvanja i objavljivanja

---

62 Savet Evrope, Konvencija Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda, Rim, 1950.

63 Čl. 8. Evropske konvencija o zaštiti ljudskih prava i osnovnih sloboda.

64 Aleksandar Jakšić, Evropska konvencija o ljudskim pravima, Pravni fakultet univerziteta u Beogradu, Beograd 2006, str. 251.

podataka koji se tiču ličnog života pojedinca.[65] Osim toga, sudska praksa je zauzela stav da pod ličnim životom pojedinca treba podrazumevati poslovne i političke aspekte života privatnog života, što se može dovesti u vezu sa ličnim podacima građana u ovim oblastima.[66]

Nakon prihvatanja pomenutih dokumenata, pravo na privatnost predviđeno je i u kasnijim međunarodnim ugovorima. Generalna skupština Ujedinjenih nacija je 1966. godine usvojila Međunarodni pakt o građanskim i političkim pravima,[67] koji je stupio na snagu deset godina kasnija. U članu 17. Pakta predviđa se da *niko ne može biti izložen proizvoljnom ili nezakonitom mešanju u privatni život, porodicu, stan ili prepisku, niti protivzakonitim napadima na čast i ugled*. Uz to, svako lice ima pravo da uživa zakonsku zaštitu od mešanja ili napada na privatan život.[68] Na ovaj način, osnažena je odredba iz Univerzalne deklaracije o ljudskim pravima i još jednom je ukazano na značaj privatnog života, pa i prava privatnosti u međunarodnom sistemu ljudskih prava.

Nedugo nakon usvajanja Međunarodnog pakta o građanskim i političkim pravima dolazi do ubrzanog razvoja informacionih tehnologija. Na području Sjedinjenih Američkih država javljaju se preteče interneta, u vidu povezanih mreža i komunikacionih sistema. Godine 1969. u sklopu Ministarstva odbrane Sjedinjenih Američkih država, ustanovljena je Agencija za napredne istraživačke projekte (*Advanced Research Project Agency – ARPA*) koja je stvorila i prvu računarsku mrežu. Mreža je povezivala različite organizacije i ustanove u okviru administracije SAD. Ubrzo se razvijaju i nove računarske mreže poput „AlohaNet-a" (AlohaNet), koja je umrežavala kampuse fakulteta i univerziteta na Havajima, zatim „Mark 1" (Mark 1) kao mreža Državne laboratorije za fiziku Velike Britanije iz 1970, „Merit iz Mičigena, „Cyclades" iz Francuske i mnoge druge.[69] Iako prvobitno korišćenja za vojno bezbednosne svrhe SAD-a, sveopšta težnja ka povezivanju dovela je do korišćenja interneta i u civilnom sektoru.[70]

---

65 ECHR, Rotary, presuda od 04.05.2000. god., br. 46., ECHR, Amman, presuda od 16.02.2000. god., br. 69. Nav. prema: A. Jakšić (2006), str. 254.

66 ECHR, Halford, presuda od 25.06.1997. god., RJD, 1997 – III, br. 44. Nav. prema: *Ibidem.*

67 Međunarodni pakt o građanskim i političkim pravima, „Sl. list SFRJ", (Međunarodni ugovori), br. 7/1971.

68 Vid. čl. 17, Međunarodnog pakta o građanskim i političkim pravima.

69 Aleksandar Vranješ, *Internet i razvoj ili ograničavanje slobode subjekata globalnog komuniciranja*, doktorska disertacija, Fakultet političnih nauka, Beograd, 2017, str. 94.

70 „Do oktobra 1990. godine preko 3,000.000 računara je bilo umreženo, da bi do kraja 1992. godine ovaj broj prešao jedan milion. Kako ARPANET nije mogao više da prati razvoj Interneta, ugašen je 28. februara 1990. godine što označava kraj vojne i početak civilne ere Interneta". A. Vranješ (2017), str. 94.

U tom trenutku već postoje računari koji mogu da pamte i obrađuju različite vrste podataka. Ujedno, naslućuju se velike mogućnosti obrade, ali i računarskog umrežavanja. Privredni subjekti se sve snažnije povezuju, razmenjujući dobra i usluge, ne samo u okvirima svojih država, već i na regionalnom i međunarodnom planu. Uz to, države počinju da vode sve brojnije evidencije o različitim informacijama koji su im od koristi, bilo na bezbednosnom, bilo na privrednom planu. Među takvim evidencijama sve značajnije mesto zauzimaju i podaci o ličnosti. Na taj način, polako sazreva svest o potrebi zaštite podataka o ličnosti.

3.2.3. Razvoj prava na zaštitu podataka o ličnosti na međunarodnom planu

Istorija zakonodavstva zaštite podataka započela je 7. oktobra 1970. godine u Nemačkoj saveznoj državi Hese. Tada je prvi put usvojen zakon koji se odnosi na zaštitu podataka u elektronskim sistemima.[71] Zakon o zaštiti podataka države Hese (*Hessisches Datenschutzgesetz*), nije sadržao previše odredbi, ali je izvršio veliki uticaj na kasniju evropsku, pa i svetsku, regulativu u vezi sa zaštitom podataka o ličnosti.

Jedna od najvećih vrednosti ovog propisa jeste uvođenje *nezavisnog nadzornog tela* koje je bilo zaduženo za kontrolu zakonitosti obrade i druga pitanja u vezi sa podacima o ličnosti. To je institucija Ombudsmana za zaštitu podataka (*Datenschutzbeauftragter*). Građani države Hese mogli su da se obrate ombudsmanu, koji ipak nije imao mogućnost donošenja obavezujućih odluka, ali je imao savetodavnu ulogu i usmeravao je građane kojem organu javne vlasti mogu da se obrate u slučaju zloupotrebe i nepravilnog korišćenja podataka o ličnosti.[72] Zakonska materija obuhvatala je isključivo organe uprave ove savezne države, budući da zbog specifičnog administrativnog položaja država nije mogla da uređuje pitanja u vezi sa zaštitom podataka na opšti način.

Nedugo zatim, u Evropi se javlja prvi zakon na nivou država. Švedska postala prva evropska državu koja je zakonom na sistematski način pružila zaštitu podataka o ličnosti građana. *Zakon o zaštiti podataka Švedske usvojen je 1973. godine*. Osnovni razlog za donošenje tog propisa krio se u jednoj zanimljivoj

---

[71] Mina Zirojević, Zvonimir Ivanović, *Zaštita prava intelektualne svojine u sektoru informaciono-komunikacionih tehnologija*, Institut za uporedno pravo, Beograd 2016, str. 76.

[72] Herbert Burkert, „Privacy – Data Protection a German/European Perspective“, in *Governance of Global Networks in the Light of Differing Local Values*, (eds. E. Christoph, K. Keeneth), Nomos: Baden-Baden 2000, p. 46.

činjenici. Naime, Švedska je u to doba bila država sa najviše računara po glavi stanovnika, a ujedno je ulazila u red bezbednosno neutralnih država.[73] Imajući u vidu pojačano korišćenje računarskih i informacionih tehnologija, ali i bezbednosno-političku opredeljenost države, javio se rizik po očuvanje neutralnosti, zbog moguće zloupotrebe informacija koje su se čuvale i razmenjivale. Zato je i usvojen ovaj zakon, koji ustanovljava pravila korišćenja podataka o ličnosti, tako da se očuva stabilnost države i nastavi tehnološki razvoj. Ističemo da je ovaj zakon kreirao *načela* na kojima će počivati mnogi državni, ali i evropski propisi. Posebno mesto zauzimao je *princip transparentnosti* kao jedan od stožera zaštite podataka o ličnosti, koji govori u prilog tezi da građani moraju imati informaciju o obradi svojih podataka.

Sledeći primer Švedske, i ostale skandinavske države su ubrzo donele svoja zakonodavstva u ovoj oblasti. Tako su 1978. godine Danska i Norveška usvojile svoje zakona. Iste godine je i Austrija stala u red država čije zakonodavstvo uređuje oblast zaštite podataka o ličnosti,[74] kao i Francuska, koja je usvojila Zakon o informatici, evidencijama i slobodama.[75] Francuski zakon predvideo je ustanovljavanje posebnog tela – Nacionalne komisije za informatiku i slobode (*Commission Nationale de L'informatique et des Libertes*),[76] kojem su poverena regulatorna i kontrolna ovlašćenja. Nacionalna komisija, u nešto izmenjenom obliku i danas ima značajnu ulogu u francuskom sistemu zaštite ličnih podataka.

Nakon toga su i ostale evropske države pristupile usvajanju ili izmeni nacionalnih propisa u oblasti zaštite podataka o ličnosti. „SR Nemačka 1977 (god.), Francuska, Danska i Austrija 1978, Velika Britanija 1984. God, Belgija 1992, Italija 1996, Poljska 1997, Portugal, Švedska i Ujedinjeno Kraljevstvo 1998, Albanija, Slovenija, Finska i Španija 1999, Austrija, Češka, Danska, Island, Letonija, Holandija i Norveška 2000, Rumunija 2001, Bugarska, Lihtenštajn i Slovačka 2002, Estonija, Litvanija, Hrvatska 2003."[77]

---

[73] *Ibid.,* str. 48.

[74] Izvan evropskog kontinenta Sjedinjene Američke Države usvojile su propis u vezi sa zaštitom ličnih podataka 1974. god. Vid. Dejan Milenković, *Pristup informacijama, zaštita podataka o ličnosti i tajnost informacija – Aktuelna pitanja zakonodavstva u Srbiji*, Komitet pravnika za ljudska prava, Beograd 2009, str. 64.

[75] Zakon o informatici, evidencijama i slobodama – *Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés*.

[76] Stevan Lilić, „Pravo, informatička tehnologija i zaštita podataka", *Anali Pravnog fakulteta u Beogradu*, br. 2-3/1989, Beograd 1989, str. 220.

[77] Navedeno prema Saša Gajin, „Zaštita podataka o ličnosti, perspektive harmonizacije domaćeg prava sa pravom Evropske Unije", u: *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005, str. 12.

Prateći zakonodavnu i poslovnu praksu, Organizacija za ekonomsku saradnju i razvoj (*OECD*),[78] je 1980. godine usvojila *Smernice za zaštitu privatnosti i prekogranični protok podataka o ličnosti*.[79] Smernice nisu imale snagu formalnog izvora prava, ali su imale za cilj da države članice više rade na razvoju principa i prava u vezi sa zaštitom privatnosti i prenosa podataka o ličnosti koji se koriste u poslovnim tokovima. Smernice su sadržale definiciju rukovaoca, podataka o ličnosti i prekograničnog protoka podataka. Takođe, ustanovljeni su i principi na kojima treba zasnivati zaštitu privatnosti i podataka o ličnosti. To su: zakonitost, transparentnost, potpunost i tačnost podataka (princip kvaliteta podataka), određene svrhe obrade, ograničenje obrade, odgovornosti za obradu, kao i učešća i prava građana u vezi sa obradom. Pomoću ovih Smernica, dat je podsticaj državama članica da u domaćim zakonodavstvima usvoje predviđene principe i prava građana, kako bi se obezbedio slobodan protok podataka, ali i poštovanje privatnosti, odnosno legitimni interes. U tom smislu, kako se u Smernicama navodi, države članice bi trebalo da:

1. Usvoje odgovarajuće propise u oblasti zaštite podataka,
2. Ohrabre i podstaknu samoregulaciju u obliku kodeksa postupanja,
3. Omoguće razumne mehanizme građanima za ostvarivanje njihovih prava,
4. Obezbede adekvatne sankcije i pravna sredstva u slučaju nepoštovanja prava u vezi sa principima obrade i pravima građana,
5. Zabrane diskriminaciju lica čiji se podaci obrađuju.[80]

Pomenuti principi svedoče o značaju privatnosti za svetsku trgovinu i razmenu dobara i usluga. Iako su usvojene pre 40 godina, sadržaj ovih Smernica je aktuelan i u današnjim zakonodavstvima i međunarodnim odnosima. Smernice su zbog toga imale značajnu podsticajnu ulogu u načinu uređivanja zaštite podataka i privatnosti.

Godinu dana nakon Smernica usvojen je, možda i najvažniji međunarodni dokument u oblasti zaštite podataka o ličnosti. Reč je *Konvenciji Saveta Evrope o*

---

[78] OECD (Organisation for Economic Cooperation and Development) predstavlja međuvladinu ekonomsku organizaciju koja je osnovana radi podsticanja ekonomskog razvoja i svetske trgovine.

[79] *Smernice za zaštitu privatnosti i prekogranični protok ličnih podataka, Aneks preporuke Saveta* od 23.09.190. god., Organizacija za ekonomsku saradnju i razvoj, https:// habeasdatacolombia. uniandes.edu.co/ wp-content/ uploads/ OECD_Privacy_ Guidelines _1980.pdf.

[80] Vid. deo 4, Smernica za zaštitu privatnosti i prekogranični protok ličnih podataka.

zaštiti lica u odnosu na automatsku obradu podataka (Konvencija 108),[81] koja je usvojena u Strazburu 28. januara 1981. godine. Ovaj datum nešto kasnije postaće i *Međunarodni dan zaštite podataka o ličnosti* (2006. godine odlukom Komiteta Ministara Saveta Evrope), što svedoči o značaju Konvencije za zaštitu podataka o ličnosti u Evropi, ali i u svetu. Ipak, Konvencija je morala da sačeka 1985. godinu i broj od 5 ratifikacija da bi stupila na snagu. Vremenom, sve države članice Saveta Evrope su ratifikovale Konvenciju, a to su učinile i pojedine države van Evrope, kao što je slučaj sa Argentinom, Mauricijusom, Meksikom, Marokom, Senegalom, Tunisom, Urugvajem, itd.[82]

Konvencija je usvojena u vremenu početka ekspanzije interneta i novih tehnologija koje su omogućile automatizaciju prilikom donošenja odluka u vezi sa pravima građana, ali i lakši protok podataka o ličnosti koji je počeo da prevazilazi državne granice. Imajući u vidu rizike koje nose ove pojave, države članice Saveta Evrope želele su da prošire zaštitu osnovnih prava na pravo privatnosti i prava na zaštitu ličnih podataka. Otuda i *osnovni cilj Konvencije*, da na teritoriji država potpisnica, garantuje svakom fizičkom licu *pravo na privatnost u slučaju automatske obrade njegovih ličnih podataka*, bez obzira na njegovu nacionalnost, prebivalište i boravište.[83] Obim primene obuhvata kako obradu podataka od strane lica privatnog prava, tako i obradu podataka u javnom sektoru.

Konvencija se bazira na osnovnim principima zaštite podataka (zakonitost i pravednost obrade, legitimni interes i svrha obrade, tačnost i potpunost podataka koji se obrađuju, transparentnost) iz kojih prolaze obaveze svake države potpisnice da pravilno primenjuju njene odredbe. Posebna pažnja posvećena je *posebnim kategorijama podataka o ličnosti*, odgovarajućim merama kojima se štiti njihova bezbednost, sankcijama i pravnim sredstvima koje treba ustanoviti zbog kršenja osnovnih načela i prava, kao i mogućnostima izuzetaka i ograničenja od osnovnih principa (javni interes, zaštita značajnog privatnog interesa, i standard neophodne mere u demokratskom društvu).

Značajno mesto u Konvenciji posvećeno je i *prekograničnoj razmeni ličnih podataka* i međusobnoj pomoći koje strane ugovornice pružaju u vezi sa ličnim podacima i odredbama ove Konvencije. U tom smislu je predviđeno da svaka država odredi jedan ili više nadležnih organa za saradnju. U slučaju Srbije, to je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti. U

---

[81] Konvencija Saveta Evrope o zaštiti lica u odnosu na automatsku obradu podataka (Konvencija 108), Savet Evrope, Strazbur, 1981., https://rm.coe.int/CoERMPublicCommon Search Services/ DisplayDCTMC ontent? documentId=0900001680078b37.

[82] Za sve potpisnice Konvencije 108 vidi: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

[83] Čl. 1, Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu podataka.

cilju olakšane saradnje i primene konvencije ustanovljen je i Savetodavni komitet koga saziva Generalni sekretar Saveta Evrope. Pored toga, Konvencija uređuje pravila u vezi sa izmenama, rezervama i drugim proceduralnim stvarima jednog međunarodnog ugovora.

Zbog svega navedenog i činjenice da i dalje ima veliki značaj Konvencija je obogaćena i novinama (Protokol br. 223 iz 2018. godine). Na taj način, Konvencija je opstala, čak 40 godina posle njenog usvajanja, u pozitivnim nacionalnim zakonodavstvima kao jedan od najvažnijih međunarodnih propisa u oblasti zaštite podataka.

Približavajući se današnjem trenutku, značajni istorijski koraci u razvoju sistema i prava na zaštitu podataka o ličnosti, učinjeni su pretežno u okvirima EU. U tom pogledu važna je Direktiva o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka od 24.10.1995. godine.[84] Direktiva je predstavljala prvi pokušaj da se sveobuhvatno reguliše zaštita podataka o ličnosti na nivou EU. Ona se odnosila na obradu svih podataka o ličnosti, nezavisno od toga da li se obrađuju automatski ili ručno. Sistem zaštite zasnovan je na tri osnovna načela: transparentnosti, legitimne svrhe obrade i proporcionalnosti. Predviđeno je i uvođenje nezavisnog nadzornog tela na nivou država članica koje obavlja različite nadzorne i stručne poslove u cilju zaštite podataka građana.

Ipak, zbog pravne prirode samih direktiva, države nisu imale obavezu da je direktno primene, već su prihvatale njena rešenja kroz nacionalne zakone. Takođe, mnogi principi, prava i mehanizmi nisu uređeni, pa je ostalo otvoreno pitanje primene brojnih instituta u vezi sa prikupljanjem i zaštitom podataka.

Nedugo zatim, 2002. godine usvojena je još jedna direktiva na teritoriji EU. Reč je o *Direktivi o obradi ličnih podataka i zaštiti prava privatnosti u sektoru elektronskih komunikacija (poznatija kao Direktiva o privatnosti i elektronskim komunikacijama*).[85] Suštinski ova Direktiva predstavlja svojevrsni dodatak Direktivi iz 1995 godine, koji se odnosi na privatnost i podatke o ličnosti u digitalnom svetu, tačnije na njihov odnos sa informaciono-komunikacionim tehnologijama. Njenim odredbama uređuju se bezbednost mobilnih (komunikacionih) mreža i usluga informacionog društva, kao i zaštita tajnosti

[84] Direktiva o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23/11/1995 P. 0031 – 0050.

[85] Direktiva 2002/58 Evropskog parlamenta i Saveta od 12. 07. 2002 godine, koja se odnosi na obradu ličnih podataka i zaštitu privatnosti u sektoru elektronskih komunikacija. Dostupna na: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri= CELEX% 3A32002L0058.

komunikacija. Uvedena je obaveza lica koja pružaju informacione usluge i servise da *brišu ili anonimiziraju podatke o ličnosti* nakon što nestane svrha zbog koje su prikupljeni ili obrađivani, pri čemu je od značaja i institut pristanka za obradu podataka u marketinške ili neke druge svrhe.

Od posebnog značaja je uvođenje zabrane upotrebe elektronskih adresa (*e-mail*) u marketinške svrhe u slučaju nepostojanja pristanka ili druge svrhe obrade, odnosno zabrana spam mejlova (*spam e-mail*), što će imati uticaj i na zakonodavstva van EU. Njenim odredbama uređena su i pitanja „kolačića" (eng. *Cookies*), malih datoteka koje omogućavaju internet stranicama da prepoznaju i prate korisnike, kao i korišćenju podataka o lokaciji građana.

Pomenute direktive utemeljile su put za najvažniji evropski propis u oblasti zaštite podataka ličnosti. Sve brži razvoj nauke i tehnologije, poduhvati Edvarda Snoudena i Juliana Asanža, kao i društvena dešavanja (curenje podataka) uticala su na to da se 2012. godine pokrene postupak za usvajanje opšteg propisa u oblasti zaštite podataka koji će jednako važiti u svim državama članicama EU.

Usledile su opsežne pripreme na njenom donošenju, brojne javne rasprave i komentari, ali i preko 4.000 amandmana na tekst novog propisa.[86] Kao rezultat tih dešavanja, doneta je Opšta uredba EU koja se direktno primenjuje na teritoriji svih članica EU. Stupanjem na snagu Opšte Uredbe EU ukinuta je Direktiva iz 1995. godine.[87] Kao *osnovni cilj Opšte uredbe* ističe se poštovanje osnovnih prava i sloboda, a posebno poštovanje privatnog i porodičnog života, komunikacije, zaštite ličnih podataka, slobode mišljenja, veroispovesti, slobode izražavanja i informisanja, slobode preduzetništva, prava na efikasan pravni lek i pošteno suđenje, kao i prava na kulturnu, versku i jezičku različitost.

Opšta uredba EU se sastoji od preambule koja ima 173 tačke i 99 članova, koji pokrivaju skoro sva značajnija pitanja u vezi sa zaštitom podataka o ličnosti. Ovaj tekst reguliše osnovne principe obrade, prava građana u vezi sa zaštitom podataka o ličnosti, prava i obaveze rukovaoca i obrađivača, zabranu i uslovi obrade posebnih kategorija podataka o ličnosti, mere koje je neophodno ustanoviti u cilju ostvarivanja bezbednosti podataka, imenovanje lica ovlašćenog za zaštitu podataka, ovlašćenja i rad nezavisnih nadzornih tela, sudsku zaštitu zbog povrede podataka o ličnosti, kao i ogromne zaprećene kazne za nepoštovanje njenih odredaba.[88]

---

[86] Dušan Pavlović, „Uredba Evropske unije o zaštiti podataka o ličnosti", http://pravoikt.org/uredba-evropske-unije-o-zastiti-podataka-o-licnosti.

[87] Upor. A. Diligenski, D. Prlja, D. Cerović (2018), str. 23.

[88] Više o novinama koje je unela Opšta uredba vid. Sanja Prlja, Pravo na zaštitu ličnih podataka u EU", *Strani pravni život* 1/2018, Beograd 2018, str. 91-96.

Značaj Opšte uredbe prevazilazi granice evropskog kontinenta i EU. Ovaj dokument je postao simbol višegodišnje borbe za privatnost i zaštitu podataka o ličnosti u savremenom digitalnom svetu. U moru informacija koje se svakodnevno koristi, podaci o ličnosti dobijaju zaštićen status. Domašaj Opšte uredbe može se posmatrati i na planu „pobede" građana nad različitim vrstama digitalnog nadzora i praćenja njihovog ponašanja, budući da građani, privredni subjekti i državni organi moraju da promene dosadašnje obrasce ponašanja i relativno bezazlen pristup podacima. Kako se navodi „Svakodnevne zloupotrebe ličnih podataka uslovile su pojavu nove pravne regulative u ovoj oblasti. Uredba predstavlja odgovor na potrebu da podaci o ličnosti budu pažljivo prikupljani, obrađivani i čuvani. Institucije koje prikupljaju i obrađuju lične podatke moraće da promene način dosadašnjeg funkcionisanja. Oni će morati da uvedu interna pravila i procedure u svoje poslovanje koje će biti u skladu sa mnogobrojnim zahtevima Uredbe".[89]

Naravno, ostaje da se vidi na koji način će se zaista primenjivati odredbe ove uredbe u upravnoj, sudskoj, pa i međunarodnoj praksi. Sudeći prema prvim uzorcima, Opšta uredba u velikoj meri ispunjava svoj cilj uređivanja aktivnosti u vezi sa podacima o ličnosti, o čemu svedoče značajne kazne koje su izrečene za veliki broj firmi.

Iako ne predstavlja deo domaćeg zakonodavstva, Opšta uredba predstavlja uzor prema kome se gradi pravo zaštite podataka i u državama kandidatima za EU, kao što je slučaj sa Srbijom. Opšta uredba predstavljala je osnovni model za Zakon o zaštiti podataka o ličnosti Srbije koji je trenutno na snazi. Srbija je kandidat za članstvo pa svoje celokupno zakonodavstvo, i praksu, treba da uskladi sa evropskim standardima i propisima. Značajni socijalni, ekonomski, kulturni i drugi odnosi domaćih lica sa evropskim stvara potrebu za približavanjem dva sistema.

Na ovaj način zaključujemo razmatranje o istorijski značajnim momentima u vezi sa zaštitom podataka o ličnosti na međunarodnom planu. Pomenuti faktori i momenti imali su uticaja i na domaće prilike i propise u ovoj oblasti. Zahvaljujući njima mi danas možemo da štitimo svoju privatnost i podatke o ličnosti. Oni su predstavljali dugogodišnju bitku da nam niko ne može svojevoljno, bez posledica ulaziti u privatni život, tražiti podatke o osetljivim delovima života prilikom zapošljavanja, da ne trpimo javnu osudu zbog pojedinosti iz ličnog života koje nas opisuju kao pojedince.

[89] *Ibid*, str. 97.

3.2.4. Istorijat pravne zaštite podataka o ličnosti u Srbiji

Za početke pravnog regulisanja oblasti zaštite podataka o ličnosti u Srbiji, moramo se osvrnuti na doba *Socijalističke Federativne Republike Jugoslavije* (u daljem tekstu: SFRJ).[90] SFRJ, u čijem je sastavu bila i Srbija, nije na sistemski način uredila oblast zaštite podataka o ličnosti, a nije postojao ni poseban propis u ovoj materiji. Ipak, osnove sistema podataka bile su prisutne u ustavnim i zakonskim tekstovima.

Ustav SFRJ iz 1974. godine,[91] uređivao je pojedina pravila u vezi sa društvenim sistemom informisanja. Ustavom je predviđeno da se „društvenim sistemom informisanja obezbeđuje usklađeno evidentiranje, prikupljanje, obrada i iskazivanje podataka i činjenica značajnih za praćenje, planiranje i usmeravanje društvenog razvoja, kao i dostupnost informacija o tim podacima i činjenicama".[92]

Takođe, važnost podataka za društvo i tadašnji društveno-politički sistem prepoznat je u *Zakonu o osnovama društvenog sistema informisanja i informacionom sistemu Federacije*.[93] Zakon je u čl. 1. predviđao da „Radnici i drugi radni ljudi i građani osiguravaju u društvenom sistemu informisanja podatke i informacije neophodne za život, rad i samoupravljanje, za praćenje, usmeravanje i planiranje društvenog razvoja, usklađivanje odnosa u društvenoj reprodukciji, vršenje funkcija oblasti i upravljanje drugim društvenim poslovima". Ipak, ovaj Zakon nije bliže uređivao pitanja zaštite podataka o ličnosti, na način kako se to čini u savremenim zakonodavstvima.

Nadalje, treba pomenuti i *Ustav Republike Srbije iz 1990 godine*, koji je (osim izbacivanja prefiksa „socijalistička" iz naziva države), jemčio zaštitu tajnosti podataka o ličnosti, što je interesantna formulacija koja se nije zadržala u kasnijim propisima, budući da je izbačena odlika „tajnosti".[94]

Nova država na ovim prostorima, Savezna Republika Jugoslavija (u daljem tekstu: SRJ) unela je normativne promene u oblasti zaštite podataka o

---

[90] U literaturi se navodi da najraniji trag prava na privatnost u Republici Srbiji seže do Ustava Kraljevine Srbije iz 1888. godine, gde se u članu 15 garantovala nepovredivost stana, a u članu 23 nepovredivost tajnosti pisama i telegrafskih depeša. Danilo Krivokapić, Đorđe Krivokapić, Milica Jovanović, Bojan Perkov, Andrej Petrovski, *Moji podaci, moja prava*, SHARE fondacija, Beograd 2018, str. 14. Ipak, na ovaj način nije pružena zaštita podacima o ličnosti, već samo privatnosti, odnosno određenim segmentima života građana.

[91] Ustav SFRJ, „Sl. list SFRJ", br. 9/1974.

[92] Čl. 75, Ustava SFRJ.

[93] Zakon o osnovama društvenog sistema informisanja i o informacionom sistemu Federacije, „Sl. list SFRJ", br. 68/1981.

[94] Ustav Republike Srbije, „Sl. glasnik RS", br. 1/1990.

ličnosti. Prvo, SRJ je pristupila Konvenciji Saveta Evrope o zaštiti lica u odnosu na automatsku obradu ličnih podataka iz 1981. godine, ali je ona potvrđena tek 1992. godine, kada je usvojen Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka.[95] Na taj način, potvrđeni međunarodni ugovor postao je deo domaćeg pravnog sistema. Iste godine, usvojen je i *Ustav Savezne Republike Jugoslavije* (1992),[96] koji je jemčio zaštitu privatnosti, ali i zaštitu podataka o ličnosti. Privatnost i lična prava čoveka bila su zajamčena zajedno sa nepovredivošću fizičkog i psihičkog integriteta.[97] Pored privatnosti, zaštita je zajamčena i podacima o ličnosti. Uvedena je *zabrana upotrebe podataka o ličnosti izvan namene za koju su prikupljeni*. Zanimljivo da je Ustav koristio termin „namena" u vezi sa obradom, umesto današnjeg termina „svrha". Svako je imao *pravo da bude upoznat* sa prikupljenim podacima o ličnosti koji se na njega odnose, kao i *pravo na sudsku zaštitu* u slučaju njihove zloupotrebe. Pored toga, bilo je predviđeno da će se pitanja prikupljanja, obrade, korišćenja i zaštite podataka o ličnosti urediti saveznim zakonom.[98]

Sa usvajanjem posebnog zakona u ovoj oblasti čekalo se do *1998. godine, kada je usvojen Zakon o zaštiti podataka o ličnosti*. Osnovna težnja prilikom donošenja ovog zakona bila je da se domaće pravo uskladi sa pomenutom Konvencijom Saveta Evrope. Zakon je uređivao isključivo zaštitu podataka, ali je propustio da uredi pitanja prikupljanja, obrade i korišćenja ličnih podataka, sa tendencijom da se ova materija uredi posebnim zakonima, što se u praksi nikada nije desilo.[99] Osim toga, zakonske odredbe nisu bile usklađene ni sa Direktivom EU iz 1995. godine, što je predstavljalo smetnju za slobodno obavljanje trgovina i usluga sa partnerima iz EU.

Nakon demokratskih promena, u Državnoj zajednici Srbije i Crne Gore, *Poveljom o ljudskim i manjinskim pravima i građanskim slobodama iz 2003. godine*,[100] *zajamčeno je pravo na zaštitu podataka o ličnosti*. U tadašnjem pravnom sistemu nije postojalo posebno pravo, već se zaštita pružala *u okvirima prava na poštovanje privatnog i porodičnog života*. Sankcionisana je upotreba podataka o ličnosti u svrhe različite od one zbog koje su prikupljeni. Predviđeno

---

[95] Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka, „Sl. list SRJ – Međunarodni ugovori", br. 1/1992.

[96] Ustav Savezne Republike Jugoslavije, „Sl. list SRJ", br. 1/1992.

[97] Čl. 22 Ustava SRJ.

[98] Čl. 33 Ustava SRJ.

[99] Aleksandar Resanović, „Zaštita podataka o ličnosti u Srbiji i Crnoj Gori, odnosno u SR Jugoslaviji", u *Zaštita podataka o ličnosti i poverljivi podaci – pravni aspekti*, Fond za otvoreno društvo, Beograd 2005, str. 52.

[100] Povelja o ljudskim i manjinskim pravima i građanskim slobodama, *Službeni list* SCG, br. 6/2003.

je i pravo svakog lica da bude obavešten o prikupljenim podacima o svojoj ličnosti. Kao i u prethodnim ustavnim tekstovima, prikupljanje, držanje i korišćenje podataka o ličnosti ostavljeno je za uređivanje posebnim zakonom.[101]

U Republici Srbiji, kao samostalnoj i nezavisnoj državi, osnovni propis za uređenje oblasti zaštite podataka o ličnosti predstavlja *Ustav Republike Srbije iz 2006. godine*,[102] koji je i dalje na snazi. *Ustav jemči zaštitu podataka o ličnosti*. Zabranjuje i kažnjava upotrebu podataka o ličnosti izvan svrhe za koju su prikupljeni, osim za potrebe krivičnog postupka ili zaštite bezbednosti Republike Srbije, što mora biti definisano posebnim zakonom. Uz to, predviđena su i dva posebna prava. *Pravo svakog lica da bude obavešten* o prikupljenim podacima koji se odnose na njega i *pravo na sudsku zaštitu* u slučaju zloupotrebe podataka.

Prvi zakon u ovoj oblasti, Zakon o zaštiti podataka o ličnosti usvojen je 23. 10. 2008. godine. Njime su uređeni uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Srbije i nadzor nad izvršenjem njegovih odredbi.[103] Donošenjem ovog zakona, Srbija je dobila *sistemski uređenu oblast zaštite podataka* koja je uređena po ugledu na pravne sisteme država EU.

Iako značajan zakon, čini se da je već prilikom njegovog usvajanja postojalo prostora za kvalitativno poboljšanje. Ustanovljavanje novog pravnog (pod)sistema, posebno u složenoj oblasti kakva je zaštita podataka, predstavlja komplikovan posao. O tome svedoče i činjenice do kojih je Poverenik u svom radu tokom prve godine primene ovog zakona (2009): „Oko 350.000 subjekata javnog i privatnog sektora bave se obradom podataka o ličnosti. Većina tih subjekata, ima po nekoliko zbirki ili baza podataka o ličnosti i ukupan broj evidencija se procenjuje na preko milion. Ove evidencije obuhvataju evidencije državnih organa, ustanova penzijskog i zdravstvenog osiguranja, obrazovanja, socijalne zaštite, bankarskog sistema, komunalnih službi, udruženja građana, kao i obradu podataka putem video nadzora na javnim mestima, poslovnim i stambenim objektima i dr. Za mnoge od tih obrada podataka ne postoji izričit zakonski osnov, odnosno saglasnost lica ili zakonom nije uređena svrha i obim podataka koji se obrađuju, trajanje i dr, a u mnogim od ovih slučajeva se radi o

[101] Čl. 24, st. 4 i 5 Povelje o ljudskim i manjinskim pravima i građanskim slobodama državne zajednice Srbije i Crne Gore.
[102] Ustav Republike Srbije, „Sl. glasnik RS“, br. 98/2006.
[103] Čl. 1, st. 1 Zakona o zaštiti podataka o ličnosti (2008).

obradi naročito osetljivih podataka, kao što su podaci o lečenju, socijalnom statusu i dr.“[104]

Zbog ovih činjenica, potrebe za uspostavljanjem stabilnog sistema i lakšim funkcionisanjem Poverenika, boljeg ostvarivanja prava građana, praćenja brzih i velikih promena u svetu informacionih tehnologija, kao i potrebe za usklađivanjem domaćeg zakonodavstva sa propisima EU, Vlada Republike Srbije je usvojila *Strategiju zaštite podataka o ličnosti 2010. godine*. Kao jedna od osnovnih stavki Strategije predviđena je neophodnost izmene i dopune osnovnog zakona u oblasti zaštite podataka o ličnosti.

Imajući u vidu ove činjenice, „ministarstvo pravde je 2013. godine oformilo Radnu grupu za izradu Nacrta Zakona koju čine predstavnici više relevantnih ustanova (Ministarstvo unutrašnjih poslova, Ministarstvo odbrane, Ministarstvo pravde i drugi). Intenzivan rad na izradi Nacrta Zakona nastavljen je u maju 2015. godine“.[105] Kao osnovu za nov zakon, uzet je Model Zakona o zaštiti podataka o ličnosti koji je tokom svog rada izradio Poverenik.

Pet godina od formiranja javne grupe, velike polemike i rasprave između zakonodavnog organa, Poverenika i predstavnika civilnog sektora, niza amandmana i različitih modela zakona, Narodna skupština Srbije je 09. 11. 2018. godine, usvojila nov *Zakona o zaštiti podataka o ličnosti,*[106] čija je primena započela devet meseci od stupanja zakona na snagu, avgusta 2019. godine. Ovaj zakon izrađen je po ugledu na Opštu uredbu EU, sa svim novim institutima koja je i ona predvidela, pa možemo reći da je u velikoj meri usklađen sa evropskim standardima u ovoj oblasti. Uvedeni su novi instituti, poput *lica za zaštitu podataka, kodeksa postupanja, posebnih prava građana u vezi sa podacima o ličnosti, obaveza rukovaoca i obrađivača i drugi*. Međutim, tokom i nakon usvajanja javilo se niz nejasnoća u vezi sa dometima primene ovog propisa, što predstavlja osnovni izazov zakonite i pravilne primene.

Budući da je reč o mladom zakonskom tekstu, neophodno je da se formira upravna i sudska praksa koje u trenutku izrade ove knjige ima vrlo malo. Takođe, potreban je i teorijski doprinos radi razumevanja i ukazivanja na moguće pravce primene ovog zakonskog teksta, koji i pored svojih manjkavosti (nije uređen video nadzor, propisane su relativno niske sankcije, dosta je nejasnoća u vezi sa brojnim institutima u posebnim oblastima), po prvi put u istoriji Srbije, stvara

[104] Strategija zaštite podataka o ličnosti, „Sl. glasnik RS“, br. 58/2010.

[105] Milorad Debeljački, „Zakon o zaštiti podataka o ličnosti: radna grupa za izradu nacrta“, PravoIkt, online 2016, https://pravoikt.org/zakon-o-zastiti-podataka-o-licnosti-radna-grupa-za-izradu-nacrta/.

[106] Zakon o zaštiti podataka o ličnosti, „Sl. glasnik RS“, br. 87/2018.

pravu podlogu za razvoj celokupnog pravnog sistema u oblasti zaštite podataka o ličnosti.

3.3. Načela zaštite podataka o ličnosti

Svaka grana prava zasniva se na principima, odnosno vrednostima koje predstavljaju „izvor" iz koga proizlaze konkretna pravila ponašanja. Ti principi u zakonodavstvu predstavljaju apstraktna pravila ponašanja i obično se određuju kao načela, odnosno apstrakta pravna pravila iz kojih proizlaze konkretna pravila. „Načela predstavljaju najmanji zajednički imenitelj smisla svih normi nekog zakona ili grane prava, pa samim tim mogu da se upotrebe za iznalaženje smisla bilo koje norme".[107]

Zaštita podataka o ličnosti, kao posebna grana prava, sadrži određena načela na kojima se zasniva celokupan sistem. U literaturi pronalazimo stavove autora koji smatraju da načela nisu *conditio sine qua non* pravnih propisa. U tom smislu se navodi da ne postoji prava potreba za osnovnim načelima u zakonskim tekstovima, već da njihova sadržina treba da bude implementirana u svaku normu tog propisa. Takođe, povreda načela ne vodi nikakvoj sankciji, tako da ona više predstavljaju „želje" i težnje zakonodavca koje nepotrebno opterećuju propise.[108]

Iako je izneti stav suštinski tačan, načela u oblasti zaštite podataka o ličnosti ipak imaju značajnu ulogu. Kako se navodi u Mišljenju radne grupe člana 29, „Principi i obaveze u vezi sa zaštitom podataka u okviru EU često nisu dovoljno ostvareni kroz unutrašnje mere i aktivnosti. Ukoliko zaštita podataka postane deo zajedničkih vrednosti i prakse organizacija, kao i odgovornosti koja ih prati, efektivno poštovanje propisa biće pod velikim rizikom i nedostaci u zaštiti podataka će se verovatno nastaviti".[109] Ove reči govore o velikom značaju koji imaju načela zaštite podataka, kao osnova za nove univerzalne vrednosti kroz koje se ostvaruju prava i interesi građana, nezavisno ko su i odakle dolaze.

Načela zaštite podataka označavaju se i kao „principi kvalitetnih podataka".[110] Naime, ova oblast pravnog regulisanja je relativno mlada i konstantno se menja pod uticajem razvoja informaciono-komunikacionih tehnologija. Zbog toga, važno je postaviti osnovne principe koji su

[107] Mihajlo Vuković, *Interpretacija pravnih propisa*, Školska knjiga, Zagreb 1953, str. 128.
[108] Više o tome vid. Dragan Milkov, Upravno pravo II – upravna delatnost, Pravni fakultet u Novom Sadu, Novi Sad 2017, str. 84-85.
[109] Radna grupa člana 29, Mišljenje 3/2010 o principu odgovornosti, br. 00062/10/EN, WP 173, od 13. 07.2010. godine, str. 2, https://www.dataprotection.ro/ servlet/ ViewDocument?id=654.
[110] P. Lambert (2017), p. 136.

„vanvremenski“, neprolazni i nezavisni od razvoja tehnike i tehnologije, budući da oni postavljaju osnove na kojima se zasniva zaštita prava građana. Njihovim predviđanjem olakšava se posao tumača pravnih normi, nezavisno da li se u toj ulozi nalaze fizička lica, pravna lica ili organi vlasti. U tom smislu, načela predstavljaju vodiče za tumačenje nejasnih i nepotpunih normi, za popunjavanje pravnih praznina i rešavanje složenih praktičnih situacija.

Poput drugih pravnih sistema i pravni sistem Srbije poznaje načela u oblasti zaštite podataka o ličnosti. Kako su pojedine vrednosti u vezi sa podacima o ličnosti ustanovljene kao univerzalne, a i uporedno-pravni sistemi teže usklađivanju i približavanju, načela zaštite su u najvećoj meri istovetna u različitim državama i pravnim sistemima. Takav je slučaj i sa načelima zaštite podataka Srbije i EU koja su u najvećoj meri istovetna.

Osnovna načela zaštite podataka o ličnosti u domaćem pravnom sistemu su:

1. Načelo zakonitosti, poštenja i transparentnosti,
2. Načelo ograničenja u odnosu na svrhu obrade,
3. Načelo minimizacije podataka o ličnosti,
4. Načelo potpunosti i tačnosti,
5. Načelo ograničenog čuvanja podataka o ličnosti,
6. Načelo integriteta i poverljivosti,
7. Načelo odgovornosti rukovaoca za postupanje u vezi sa podacima o ličnosti.

3.3.1. Načelo zakonitosti, poštenja i transparentnosti

Načelo zakonitosti, poštenja i transparentnosti obično se označava kao osnovno u sistemima zaštite podataka o ličnosti**.** Uloga ovog načela je od presudnog značaja za funkcionisanje čitavog pravnog sistema, budući da potiče iz principa vladavine prava i pravne države. U odnosu na oblast zaštite podataka o ličnosti, ovo načelo se može razložiti na *tri pojedina načela*, koja ćemo ukratko analizirati, radi lakšeg razumevanja**.**

Načelo zakonitosti predstavlja osnovni element svakog pravnog sistema. Njegova uloga jeste da osigura zakonitu primenu normi u vezi sa zaštitom podataka, tako da spreči samovolju onih koje te norme primenjuju. U zavisnosti od toga da li se posmatra šire ili uže u odnosu na svoju funkciju, načelo zakonitosti se može posmatrati na nekoliko načina. „U najširem smislu (*načelo*

zakonitosti) označava saglasnost svih odnosnih akata sa zakonom kao višim aktom. U nešto užem smislu zakonitost označava da svi pravni akti i sve materijalne radnje koje preduzimaju državni organi i građani jesu, odnosno moraju biti u skladu sa zakonom, moraju se doneti, odnosno vršiti u skladu i na osnovu zakona kao najvišeg pravnog akta. U najužem smislu, zakonitost znači da svi pravni akti sa manjom pravnom snagom jesu, odnosno moraju biti, u skladu i doneti na osnovu pravnih akata s većom pravnom snagom".[111]

Zakonitost usmerava svaku obradu podataka o ličnosti tako da bude zasnovana na odgovarajućoj zakonskoj ili drugoj opštoj pravnoj normi. Na taj način se ispunjava osnovni cilj ovog načela da pravne norme budu postavljene iznad lične (samo)volje rukovaoca i obrađivača. Drugim rečima, intencija zakonodavca je da svaka obrada podataka o ličnosti bude zasnovana na odgovarajućem pravnom aktu, da bude doneta od nadležnog lica i da se zasniva na poštovanju svih prava i interesa lica čiji se podaci obrađuju. Osim toga, svaka odluka koja se donese u vezi sa podacima o ličnosti mora biti utemeljena, odnosno obrazložena kako bi se razumeo razlog primene opšte norme na konkretan slučaj. Nezaobilazni element ovog načela jeste i mogućnost korišćenja pravnih sredstava u slučaju pogrešne ili nepravilne primene prethodno navedenih elemenata. Na taj način, zakonitost prožima sve nivoe odlučivanja i različite subjekte koji učestvuju u tom postupku.

Načelo poštenja teži da usmeri sve one koji primenjuju pravne norme da vode računa o svakoj obradi, što znači da se činjenice i norme tumače i primenjuju u skladu sa okolnostima svakog konkretnog slučaja. Rukovaoci i obrađivači treba pošteno da pristupaju obradama podataka o ličnosti, tako da ih koriste kao tuđe lično dobro sa punom pažnjom i poštovanjem. Suštinski posmatrano, uvođenje načela poštenja ima za cilj da poveća svest o značaju uloge rukovanja sa podacima o ličnosti. „Načelo savesnosti i poštenja suprotstavlja se načelu autonomiji volje u smislu neophodnosti borbe suprotnosti, a time i ravnoteže, između egoističkog u pravu, s jedne, i etičkog i socijalnog, odnosno zajedničkog, društvenog, kolektivnog, s druge strane".[112]

Načelo transparentnosti, predstavlja možda i najznačajniju kariku sistema pravne zaštite podataka o ličnosti. Ono je usmereno ka ostvarivanju uvida u radnje prikupljanja i obrade podataka o ličnosti, kao i donošenja odluka u vezi sa

[111] Dragan Mitrović, *Uvod u pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2010, str. 360-361.

[112] Oliver Antić, „Moral (etika) u građanskom pravu, Zbornik radova *Harmonizacija građanskog prava u regionu* (ur. Dijana Marković-Bajalović), Pravni fakultet Univerziteta u Istočnom Sarajevu, Istočno Sarajevo 2013, str. 4.

njima. Zato možemo reći da ono prožima sva posebna prava građana u vezi sa podacima o ličnosti. Obaveštenost građana i potreba da budu upoznati sa najvažnijim radnjama obrade u vezi sa njihovim podacima o ličnosti, predstavljaju ključne preduslove za ostvarivanje zakonitosti obrade i bezbednosti podataka o ličnosti. Takođe, načelo poštenja podrazumeva transparentnu i otvorenu obradu, jer onaj ko zakonito radi, nema šta da krije. Kako se navodi: „…u društvenom, odnosno političkom kontekstu, (načelo transparentnosti) označava javno delovanje pojedinca, društvenih grupa, organizacija, institucija i državne vlasti koje karakteriše otvorenost ili spremnost da se podaci o njemu što je moguće više učine dostupnim javnosti i na taj način odgovornim prema široj zajednici".[113]

Zahvaljujući načelu transparentnosti građani dobijaju mogućnost da budu upoznati sa svim aktivnostima koje se odnose na njihove lične podatke, što podrazumeva odgovore na pitanja *ko kada, na koji način i kako upotrebljava njihove podatke o ličnosti*.[114]

Kroz zajedničko delovanje i uzajamno sadejstvo pomenutih načela, ostvaruju se i drugi demokratski i pravni principi, kao što je pravna država i vladavina prava. Uz to, osnažuje se i pozicija pojedinca prema svim drugima koji koriste njegove podatke o ličnosti i ujedno se ustanovljava odgovornost rukovaoca i obrađivača za nepravilne i nezakonite obrade. Na taj način razvija se i stepen ljudskih prava u društvu.

Naravno, načelo zakonitosti kao takvo prožima skoro sve pravne norme u sistemu zaštite podataka o ličnosti, što znači da ono ima i svoje praktične aspekte i pored apstraktne prirode. To je posebno vidljivo kod razloga zbog kojih se može vršiti obrada podataka o ličnosti. U tom smislu, da bi obrada podataka o ličnosti bila zakonita, ona se mora zasnivati na jednom od nekoliko zakonom predviđenih osnova. Obrada će biti zakonita ukoliko se zasniva na:

1. Pristanku,
2. Izvršenju ili zaključenju ugovora,
3. Poštovanju pravnih obaveza rukovaoca,
4. Na zaštiti životno važnih interesa,

[113] Distrikt, Transparentan – reč koju koriste oni koji ne znaju šta znači, online, http://distrikt.rs/transparentan-rec-koju-koriste-oni-koji-ne-znaju-sta-znaci.

[114] Nove tehnologije omogućavaju brzo širenje informacija, pa se tako građani danas mogu upoznati sa stvarnim stanjem stvari u praksi i putem mobilnih aplikacija, u okviru kojih građani prijavljuju određene greške i kvarove koji spadaju u nadležnost organa uprave. Tako se transparentnost, između ostalog, ostvaruje i kroz aplikacije za mobilne telefone. Vid. S. Goldsmith, S. Cawford (2014), pp. 27-29.

5. Obavljanju poslova u javnom interesu ili izvršenju zakonom propisanih ovlašćenja,
6. Ostvarivanju legitimnih interesa rukovaoca,

3.3.1.1. Pristanak ka osnov zakonite obrade

Obrada podataka o ličnosti ima zakonit karakter i osnov ako se zasniva na pristanku lica čiji se podaci o ličnosti obrađuju. Pristanak se određuje kao svako dobrovoljno, određeno, informisano i nedvosmisleno izražavanje volje kojim to lice, izjavom ili jasnom potvrdnom radnjom, daje pristanak za obradu podataka o ličnosti koji se na njega odnose.[115] Dakle, da bi pristanak bio punovažan mora da ispunjava *nekoliko uslova***.**

Prvo, *pristanak mora da bude dobrovoljan*. Svaki pristanak koji je dat pod prinudom ili zbog upotrebljene sile, ne proizvodi pravno dejstvo i može se pobijati pred sudom zbog nedostatka volje na strani davaoca. Ukoliko dođe do ispitivanja da li je pristanak slobodno dat, posebno u poslovnim odnosima, mora se obratiti pažnja da li je izvršenje ugovora ili pružanje usluge bilo uslovljeno davanjem pristanka koji nije neophodan za njegovo izvršenje.[116]

Dalje, *pristanak mora da bude određen*. To znači da se mora odnositi na konkretnu obradu (iako se u okviru radnje obrade može preduzeti više povezanih delatnosti u cilju izvršenja obrade), određene podatke ili vrste podataka i konkretnu svrhu obrade. Informisano davanje pristanka znači da lice koje daje pristanak mora da bude u potpunosti upoznato da potpisom određenog dokumenta (pismena) daje saglasnost za obradu svojih podataka o ličnosti.

Eventualno „sakrivanje" saglasnosti u okviru pravila poslovanja ili drugog dokumenta u vezi sa kojim se obrađuju podaci, ne može se smatrati za informisano davanje saglasnosti. Dakle, saglasnost mora da bude data u posebnom dokumentu za pristanak ili u okviru dokumenta koja se odnosi na druga pitanja, ali samo ako je zahtev za davanje pristanka lako uočljiv, jasno se izdvaja od ostalih odredbi, odnosno pitanja. U svakom slučaju, u dokumentu u kome je potrebno dati pristanak, neophodno je koristiti razumljiv stil, uz upotrebu jasnih i jednostavnih reči koji upućuju na davanje saglasnosti.[117] To znači da prosečan čovek može da razume da potpisom na dokumentu daje drugom licu mogućnost da preuzme i koristi njegove podatke o ličnosti.

U vezi sa prethodnim uslovom je i *nedvosmisleno izražavanje volje,* koje znači da saglasnost mora da bude jasno postavljena i predstavljena davaocu

[115] Čl. 4, st. 1, tač. 12 Zakona o zaštiti podataka o ličnosti.
[116] Vid. čl. 15, st. 4 Zakona o zaštiti podataka o ličnosti.
[117] Vid. čl. 15, st. 2 Zakona o zaštiti podataka o ličnosti.

saglasnosti, bez mogućnosti da se saglasnost krije pod drugim nazivima ili dokumentima. Saglasnost se daje jasnom i preciznom izjavom volje davaoca saglasnosti da pristaje na obradu tačno određenih podataka o ličnosti *u tačno određenu svrhu*. Dakle, ovde ne treba da postoje nepoznati elementi koji se odnose na neodređenost podataka ili razloga zbog kojih se obrađuju. Jasno izražene potvrdne radnje u slučaju nemogućnosti pisanog davanja saglasnosti ostvaruju pravne posledice davanja saglasnosti. Primera radu, ovde može biti reč o davanju otisaka prsta ukoliko je davalac saglasnosti nepismen.

Po svojoj pravnoj prirodi, pristanak na obradu podataka o ličnosti predstavlja *strogo ličnu izjavu volje*, budući da je može dati samo fizičko lice na koje se podaci odnose ili za to posebno ovlašćeno lice. Pristanak na obradu podataka o ličnosti mora se dati bez traženja protiv usluge. Kako se izjava volje o obradi podataka može izjaviti na različite načine (pismenim ili elektronskim putem), reč je o *neformalnom pravnom poslu*.

Zakon o zaštiti podataka o ličnosti ne sadrži eksplicitnu odredbu o *formama u kojima se pristanak može dati*. Ipak, kako rukovalac ili obrađivač moraju, kada se za to ukaže potreba, da budu u mogućnosti da predoče pristanak lica čiji se podaci obrađuju. To znači da pristanak mora biti dokumentovan, odnosno da mora biti u pisanom ili elektronskom obliku, radi kasnije mogućnosti korišćenja kao dokaza.

U pojedinim situacijama moguće je dati pristanak i *konkludentnim radnjama*. Ukratko, konkludentne radnje predstavljaju posredno izjavljivanje volje, kojima, imajući u vidu sve druge okolnosti slučaja, određeno lice izjavljuje volju na posredan način. *Primera radi*, u cilju stvaranja internet prezentacije, kompanija poziva zaposlene da pored svoje biografije dostave i fotografije koje će služiti u cilju predstavljanja zaposlenih, ali i same firme. Slanjem fotografije ili omogućavanjem direktnog postavljanja fotografije na internet prezentaciju, smatra se da postoji pristanak zaposlenog.[118]

Jedno od značajnijih pitanja u vezi sa pristankom, jeste njegovo trajanje. Osnovno je pravilo da pristanak može da traje do opoziva. *Opoziv pristanka* na obradu podataka o ličnosti može se dati u svakom trenutku, a upućuje se rukovaocu. Opoziv se mora dati u jasnom i jednostavnom obliku, na istovetan način na koje se pristanak može dati. Podrazumeva se da opoziv ne povlači za sobom ništavost radnji obrade koje su učinjene pre davanja opoziva, jer bi se na taj način narušila koncepcija obrade podataka o ličnosti koja se zasniva na pristanku.

[118] Upor. A. Diligenski, D. Prlja, D. Cerović (2018), str. 88.

Zakon o zaštiti podataka o ličnosti ne određuje vremensko trajanje datog pristanka. Ovaj zakon jedino predviđa pravo lica koje je dalo pristanak na obradu da ima mogućnost opoziva u svakom trenutku. *Smatramo da bi adekvatno rešenje bilo da se pristanak vremenski ograniči na određeni vremenski period (1 ili 2 godine) nakon čega bi rukovalac, odnosno obrađivač bio dužan da ponovo dobije pristanak, odnosno da dobije produženje pristanka*. Nakon prestanka ovog perioda, pristanak bi automatski trebalo da prestane da važi, ukoliko se ne produži. Na taj način izbegle bi se negativne posledice neograničenog trajanja pristanka, a rukovaoci i obrađivači imali bi dužnost pažljivog postupanja sa podacima građana.

Maloletna lica uživaju posebnu zaštitu u vezi sa njihovim podacima o ličnosti zbog njihovog stepena zrelosti i mogućnosti da sagledaju opasnosti i rizike koji se javljaju kod upotrebe interneta, društvenih mreža i njihovih podataka. „S jedne strane, deca i mladi se posmatraju kao digitalna generacija, pioniri u razvijanju digitalne kompetencije, dok, s druge strane, posmatraju se kao ranjiva grupa korisnika interneta koja je u potencijalnom riziku“.[119] Ova činjenica se odražava i na mogućnost davanja pristanka na obradu takvih podataka.

Maloletno lice koje je navršilo 15 godina života ima pravo da samostalno odlučuje o davanju pristanka za obradu podataka o svojoj ličnosti u korišćenju usluga informacionog društva.[120] Imajući u vidu napredak tehnologije i njen uticaj na svakodnevni život, posebno život mladih ljudi, zakonodavac prihvata mogućnost da i lica koja nisu potpuno poslovno sposobna mogu dati pristanak na obradu pojedinih podataka kako bi mogla da učestvuju u „digitalnom svetu“.

Međutim, maloletna lica mogu da daju pristanak isključivo u vezi sa uslugama koje se uobičajeno pružaju uz naknadu, na daljinu, elektronskim sredstvima na zahtev primaoca usluga. *Primera radi*, maloletnik od 16 godina života može dati svoj pristanak na obradu podataka o ličnosti koji su potrebni za kupovinu video igre i njeno igranje preko interneta. Ista je situacija i sa drugim platformama koje se zasnivaju na elektronskoj trgovini.

Kao što možemo zaključiti, maloletnici sa navršenih 15 godina života ne mogu da daju pristanak za druge vrste obrada, osim onih koje se odnose na usluge informacionog društva. *Smatramo* da to *nije adekvatno rešenje* imajući u vidu da maloletnici u tim godinama imaju pravom priznatu mogućnost da raspolažu

[119] Slađana Zuković, Senka Slijepčević, „Roditeljska kontrola ponašanja dece na internetu i socijalnim mrežama“, u *Nastava i vaspitanje*, br. 64/2, Pedagoško društvo Srbije i Institut za pedagogiju i andragogiju Filozofskog fakulteta Univerziteta u Beograd, Beograd 2015, str. 241-242.

[120] Čl. 16, st. 1 Zakona o zaštiti podataka o ličnosti.

zaradom i pravo da daju pristanak na pojedine medicinske zahvate. To implicira da oni imaju dovoljnu zrelost da daju pristanak na obradu podataka o ličnosti. „Mnogi rizici iz fizičke stvarnosti preseljeni su u virtuelno okruženje, pa se deca u okruženju socijalnih mreža mogu susresti sa različitim negativnim aspektima interpersonalne komunikacije sa vršnjacima i odraslima“.[121] Dakle, rizici koji postoje u fizičkom svetu, postoje i u virtuelnom, pa bi maloletnicima sa navršenih 15 godina trebalo proširiti mogućnost davanja saglasnosti na obradu podataka o ličnosti.

Budući da maloletna lica koja nisu navršila 15 godina života ne mogu dati pristanak na obradu podataka o ličnosti, umesto njih to može učiniti roditelj koji vrši roditeljsko pravo, odnosno drugi zakonski zastupnik maloletnog lica. *U situaciji kada oba roditelja vrše roditeljsko pravo, smatramo da bi trebalo omogućiti da samo jedan roditelj da pristanak na obradu*. Oni vrše roditeljsko pravo u najboljem interesu deteta, pa sa tom pretpostavkom treba krenuti i kod davanja saglasnosti za obradu dečijih podataka. Na taj način se ubrzava i olakšava pravni promet, bez povećanja rizika po prava roditelja ili deteta, posebno imajući u vidu da rukovalac, odnosno obrađivač imaju posebnu odgovornost za uspostavljanje zaštitnih mera u vezi sa podacima o ličnosti maloletnih lica.

3.3.1.2. Izvršenje ugovora kao zakonit osnov obrade

Prilikom pregovora oko zaključenja ili kod izvršenja ugovora može se javiti potreba jedne od ugovornih strana da obradi podatke o ličnosti druge ugovorne strane. Radi bezbednosti i ubrzanja poslovnog prometa predviđeno je da je zakonita ona obrada podataka o ličnosti koja je neophodna u cilju izvršenja ugovora ili preduzimanja radnji koje vode ka zaključenju ugovora.

Nije dovoljno da postoji bilo kakva potreba za obradom podataka u cilju izvršenja ugovora. Uslov za zakonitu obradu jeste da je takva obrada podataka o ličnosti neophodna. To znači da je kod nekih ugovora moguće izvršiti ugovor, a da se ne obrađuju podaci o ličnosti, pa u tim situacijama ne postoji ni osnov za zakonitu obradu. *Primer za takav ugovor jeste kupovina hleba u prodavnici*.

Sa druge strane, kao primer zakonite obrade podataka o ličnosti u cilju izvršenja ugovora pominjemo ugovor o kupoprodaji pokretnih stvari putem interneta. Kod ovog ugovora, budući da se prodavac i kupac ne nalaze na istom mestu, kupac mora da ostavi pojedine podatke o ličnosti poput imena, prezimena, kontakt telefona, adrese i slično, kako bi prodavac mogao da mu dostavi

[121] Marina Kovačević-Lepojević, Vesna Žunić-Pavlović, „Rizici socijalnog umrežavanja dece na internetu“, *Zbornik Instituta za kriminološka i sociološka istraživanja*, br. 1-2, Institut za sociološka i kriminološka istraživanja, Beograd 2011, str. 186.

zahtevani proizvod. *U ovom slučaju, javlja se potreba za obradom podataka u cilju izvršenja ugovora*.

Kada je reč o radnjama obrade koje se preduzimaju pre zaključenja ugovora (kao priprema za zaključenje), potrebno je da postoji i *zahtev lica čiji se podaci obrađuju* za takvu obradu.[122] Ove radnje u stvari predstavljaju predugovorne radnje koje imaju za cilj da dovedu do zaključenja ugovora. *Dostavljanje podataka o ličnosti i profesionalnim kompetencijama u cilju ispitivanja da li to lice ispunjava uslove za zaključivanje ugovora o autorskom delu*, predstavlja radnju koja prethodi zaključenju ugovora, pa dostavljanje podataka o ličnosti od strane kandidata, kao potencijalne buduće ugovorne strane, predstavlja zakonit osnov obrade.

3.3.1.3. Poštovanje pravnih obaveza rukovaoca

U određenim situacijama, rukovalac ima dužnost da dostavi podatke o ličnosti organu javne vlasti ili drugom licu. Takva dužnost se javlja kao posledica potrebe za normalnim i efikasnim odvijanjem društvenih, pravnih i privrednih tokova. Zbog toga, zakonita je ona obrada podataka o ličnosti koja je neophodna u cilju poštovanja pravnih obaveza rukovaoca. Suštinski, to znači da rukovalac mora da preduzme neku radnju obrade podataka, kako bi sa druge strane ispunio pravnu obavezu prema drugom licu.

Primera radi, *Zakon o sprečavanju pranja novca i finansiranja terorizma*,[123] kao jednu vrstu mere za sprečavanje i otkrivanje pranja novca i finansiranja terorizma, predviđa dostavljanje informacija, podataka i dokumentacije Upravi za sprečavanje pranja novca. Obveznici prema ovom zakonu jesu banke, ovlašćeni menjači, brokersko-dilerska društva, platne institucije, posrednici u prometu nepokretnosti, preduzetnici i pravna lica koja se bave pružanjem računovodstvenih usluga, poreski savetnici i mnogi drugi.[124] Kako je u ovom slučaju zakonom konstituisana obaveza dostavljanja podataka, među kojima se mogu naći i podaci o ličnosti, postoji i zakonit pravni osnov za obradu takvih podataka.

Na ovom mestu, postavljamo pitanje, da li pored opštih pravnih akata, pravnu obavezu mogu konstituisati i pojedinačni pravni akti (odluke upravnih organa)? *Primera radi*, inspektori su ovlašćeni da radi utvrđivanja činjenica od

[122] Vid. čl. 12, st. 1, tač. 2 Zakona o zaštiti podataka o ličnosti.

[123] Zakon o sprečavanju pranja novca i finansiranja terorizma, „Sl. glasnik RS“, br. 113/2017, 91/2019.

[124] Za listu svih obveznika po zakonu vid. čl. 4, st. 1 Zakona o sprečavanju pranja novca i finansiranja terorizma.

značaja za vršenje inspekcijskog nadzora nalože određenom licu da u određenom roku stave na uvid poslovne knjige, ugovore i drugu dokumentaciju koju nadzirani subjekt poseduje i čuva, a u okviru koje se mogu naći i podaci o ličnosti klijenata (građana). Inspektor izdaje pojedinačni pravni akt koji se odnosi na konkretnog subjekta i na izvršavanje konkretne obaveze, pa tako nastaje i osnov za pristup i obradu podataka o ličnosti. Takođe, sudska presuda može glasiti tako da stvara obavezu (pravni osnov) za određeno lice da omogući pristup određenim podacima o ličnosti.

Budući da se Zakon o zaštiti podataka o ličnosti ne izjašnjava o ovom pitanju, trebalo bi uzeti da se i pojedinačnim pravni aktom može ustanoviti obaveza za rukovaoca da pristupi određenim podacima o ličnosti i preduzme određenu radnju obrade. Podrazumeva se da takav pojedinačan pravni akt mora biti zasnovan na opštem pravnom aktu koji omogućava pristup, odnosno određuje svrhu obrade podataka o ličnosti, obrazložen i usko ograničen na rešavanje konkretnog slučaja.

U uslovima sveopšte povezanosti u modernom svetu, moguće je da organ strane države konstituiše pravnu obavezu za rukovaoca da pristupi obradi. U tom slučaju, kada se obaveza ne zasniva na pravu Republike Srbije, već na odredbama stranog prava, potreban je odgovarajući međudržavni sporazum ili odluka domaćeg organa o priznanju i izvršenju strane odluke, kako bi takav osnov bio zakonit i u Republici Srbiji.

3.3.1.4. Obrada u cilju zaštite životno važnih interesa

Obrada podataka o ličnosti ima zakonit karakter kada je neophodna da bi se zaštitio važan interes lica na koje se podaci odnose ili drugog fizičkog lica. Neophodan uslov jeste ugroženost životno važnog interesa fizičkih lica. Podaci o ličnosti mogu nositi informaciju o određenoj okolnosti ili činjenici koja može spasiti život određenog lica. „Generalno govoreći, u pitanju su zapravo situacije života i smrti – obrada je neophodna za nagledanje epidemije i njihovo širenje ili u slučajevima humanitarnih kriznih situacija, u situacijama prirodnih katastrofa i katastrofa uzrokovanih ljudskim delovanjem.“[125]

To znači da je na rukovaocu, odnosno obrađivaču da proceni da li u konkretnoj situaciji postoji važan životni interes koji treba zaštiti. Naravno, takva procena se može preispitivati pred nadležnim organom ili sudom, pa je važno voditi računa o svim činjenicama konkretnog slučaja. Kao neke od važnih

[125] Danilo Krivokapić, Jelena Adamović, Dunja Tasić, Andrej Petrovski, Petar Kalezić, Đorđe Krivokapić, *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – tumačenje novog pravnog okvira*, SHARE fondacija Beograd 2019, str. 43.

životnih interesa koje možemo pomenuti jesu zaštita psihičkog i telesnog integriteta ljudi, imovina veće vrednosti, privatnost i tome slično. Primera radi, kada je neko lice životno ugroženo i ne može da da saglasnost na obradu podataka o ličnosti, postoji potreba doktora da pristupi njegovom medicinskom kartonu kako bi pružio odgovarajuću medicinsku pomoć i negu.

Takođe, *na primeru pružanja medicinske* pomoći možemo pretpostaviti i potrebu za obradom podataka u slučaju zaštite važnog životnog interesa drugog lica, a ne lica na koga se podaci odnose. Radi zaštite života deteta, neophodno je pristupiti zdravstvenim podacima roditelja kako bi se postavila odgovarajuća dijagnoza i sprečile negativne posledice eventualnog pogrešnog postupka lečenja.

3.3.1.5. Obrada u javnom interesu i u cilju izvršenja ovlašćenja

Ovaj uslov zakonitosti obrade odnosi se prevashodno na organe javne vlasti. Organi javne vlasti obavljaju veliki broj poslova koji se odnose neposredno ili posredno na lična stanja građana. U tom smislu, oni imaju potrebu da pristupe određenim podacima o ličnosti kako bi se rešila određena životna situacija, u smislu utvrđivanja prava, obaveze ili interesa. Pod organima javne vlasti treba podrazumevati sve imaoce javnih ovlašćenja koji odlučuju o stanjima i situacijama građana. *Primera radi*, katastar nepokretnosti ima pravo da obrađuje pojedine podatke o ličnosti onih fizičkih lica koji su zaključili ugovor o prometu nepokretnosti, a u cilju upisa promene vlasnika nepokretnosti, čime se izvršava zakonom predviđena dužnost katastra.

Ipak, ova odredba ne odnosi se isključivo na organe javne vlasti, već i na sva ostala lica koja prikupe i na neki način koriste lične podatke građana u cilju izvršenja obaveze u javnom interesu. Tako, obrada podataka o ličnosti u cilju prijavljivanja učinjenog krivičnog dela od strane bankarskog službenika ne predstavlja zakonsko ovlašćenje, ali predstavlja vršenje posla u javnom interesu, pa i obavezu predviđenu krivičnim zakonodavstvom (neprijavljivanje krivičnog dela i učinioca) za čije nepoštovanje je predviđena kazna zatvora.[126] Na ovom primeru vidimo da obrada podataka o ličnosti nije jednoličan fenomen, već se mora posmatrati sa različitih aspekata i grana prava.

Osnov za obradu podataka o ličnosti u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja *mora se odrediti zakonom*. Zakonom treba ustanoviti i cilj obavljanja poslova kojima se ostvaruje javni

[126] Neprijavljivanje krivičnog dela i učinioca, čl. 332 Krivičnog zakonika, „Sl. glasnik RS“, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009. 111/2009, 121/2012, 104/2013, 108/2014 i 94/2016.

interes ili zakonsko ovlašćenje. To znači da se aktima niže pravne snage od zakona (uredbama, opštim podzakonskim aktima – pravilnicima, kao i pojedinačnim pravim aktima - upravni aktima ili presudom) ne može odrediti ovaj osnov za obradu.

3.3.1.6. Obrada u cilju legitimnih interesa rukovaoca

Zakonita je i ona obrada podataka o ličnosti koja je neophodna u cilju ostvarivanja legitimnih interesa rukovaoca ili treće strane, osim ako su nad tim interesima pretežniji interesi ili osnovna prava i slobode lica na koje se podaci odnose, a posebno ako je lice na koje se podaci odnose maloletno lice.[127] Vidimo da je za ostvarivanje ovog uslova obrade potrebno utvrditi interes rukovaoca ili treće strane. *Interes treba razlikovati od svrhe* zbog koje se obrađuju podaci. Interes se odnosi na pozitivne strane obrade podataka o ličnosti, odnosno korist koju imaju rukovalac ili treća strana, što treba razlikovati od svrhe obrade. Značajno je da interesi moraju biti legitimni, odnosno prihvatljivi sa pozicije pravnog poretka, pa je u tom smislu nelegitiman onaj pravni interes koji se ne zasniva na načelima zaštite podataka, onaj interes koji teži da ostvari neke protivpravne posledice ili onaj interes koji je usmeren na maliciozno korišćenje pravnih normi (npr. ostvarivanje protivpravne novčane koristi za sebe ili drugo lice, nezakonito ostvarivanje monopolske pozicije na tržištu, itd.).

Ipak, nije dovoljno samo utvrditi legitimni interes rukovaoca ili trećeg lica. *Potreban uslov je i da takav interes ne preteže nad interesima lica na koje se podaci odnose ili nad njihovim pravima i slobodama*.

Mišljenja smo da je ostvarivanje prava i slobode fizičkog lica u najvećem broju slučajeva značajnije od ličnog interesa rukovaoca ili trećeg lica, osim u slučaju odbrane od kakvog pravnog zahteva, ostvarivanja životno važnih interesa ili ostvarivanja javnog interesa koji se odnosi na veći broj lica.

U okvirima EU, *Radna grupa člana 29* je izrazila stav da korišćenje biometrijskih podataka u cilju zaštite imovine ili lica predstavlja opravdan interes kome se suprotstavlja interes lica čiji se podaci uzimaju. Zbog toga, neophodno je napraviti procenu i dokazati da postoji povećani stepen rizika za bezbednost imovine ili ljudi, što stvara potrebu uzimanja biometrijskih podataka. Sa značajem podataka, povećava se i rizik od njihove povrede, što treba imati u vidu prilikom uvođenja bezbednosnih mera.[128]

[127] Čl. 12, st. 1, tač. 6 Zakona o zaštiti podataka o ličnosti.
[128] A. Diligenski, D. Prlja, D. Cerović (2018), str. 100.

Zakonitost obrade se ne može zasnivati na pretežnijem legitimnom interesu kada se u poziciji rukovaoca nalazi *organ javne vlasti*, kako se ne bi previše proširilo polje diskrecione ocene. Takođe, treba imati u vidu i da obavljanje poslova u javnom interesu ili u cilju izvršenja zakonom propisanih ovlašćenja predstavlja osnov zakonitosti za organe javne vlasti.

U *pravnom poretku Republike Srbije mogu se uočiti neusklađenosti pojedinih prava i sloboda sa jedne strane i ovlašćenja, odnosno javnog interesa sa druge strane*. Tako, primera radi Agencija za privredne registre ima zakonsku obavezu vođenja i javnog prikazivanja registara koji između ostalog sadrže i određene lične podatke fizičkih lica. U Registru privrednih subjekata, u okviru dela koji se odnosi na preduzetnike, mogu se naći lična imena, prezimena, adrese stanovanja i matični brojevi fizičkih lica. Smatramo da je neophodno izvršiti reviziju posebnih propisa i uskladiti njihovo stanje sa ustanovljenim sistemom zaštite podataka o ličnosti.

3.3.2. Načelo ograničenja u odnosu na svrhu obrade

Svaka obrada podataka o ličnosti mora se zasnivati na zakonitom osnovu i legitimnoj svrsi zbog koje se oni obrađuju. Svrha obrade suštinski predstavlja razlog zbog koga se podaci fizičkih lica obrađuju. Načelo ograničenja u odnosu na svrhu obrade ide za tim da spreči samovoljno i nepotrebno korišćenje tuđih podataka, već da se obrada vrši radi sa nekim ciljem koji pravni sistem prepoznaje kao adekvatan za korišćenje tuđih podataka. Zbog toga, moderni pravni sistemi, među kojima je i pravni sistem Srbije, predviđaju princip pomoću koga se ograničavaju mogućnosti obrade.[129]

Praktično, *načelo ograničenja u odnosu na svrhu obrade znači to da se prikupljanje* podataka o ličnosti *može vršiti samo na osnovu zakonom predviđenih razloga*. Rukovalac i obrađivač mogu preduzeti radnje obrade samo u odnosu na *određene, izričite i opravdane svrhe*.

Prikupljanje podataka bez određene svrhe je protivpravno. Kada se ukaže potreba za obradom, rukovalac mora tačno odrediti iz kog razloga se podaci prikupljaju i obrađuju. *Određenost* svrhe znači da rukovaoci i obrađivači vrše

[129] Čl. 5, st. 1, tač. 2 Zakona o zaštiti podataka o ličnosti. Za više o nastanku principa ograničene svrhe obrade vid. Nikolaus Forgó, Stefanie Hänold, Benjamin Schütze, „The Principle of Purpose Limitation and Big Data“, *New techonolgy, Big Data and the Law* (ed. Marcelo Corrales, Mark Fenwick, Nikolaus Forgó), Springer, Singapore 2017, p. 22-25.

delatnosti u vezi sa kojima su im potrebni podaci o ličnosti. Podaci o ličnosti ne mogu se prikupljati pre nego što se javi potreba za njihovom obradom. *Izričitost* ukazuje na to da lica čiji se podaci obrađuju moraju na jasan i razumljiv način biti upoznata sa svrhom obrade. Pored toga, izričitost podrazumeva i zabranu sakrivanja razloga zbog kojih se podaci o ličnosti obrađuju, što implicira da rukovaoci i obrađivači ne mogu davati apstraktne i neodređene razloge za prikupljanje i obradu podataka o ličnosti. *Opravdanost* znači da stvarno (objektivno) postoji potreba rukovaoca i obrađivača za prikupljanjem i obradom podataka o ličnosti građana, koja se zasniva na zakonskim propisima.

Još jedna posledica načela ograničenja u odnosu na svrhu obrade govori o tome da se podaci o ličnosti ne mogu koristiti i obrađivati u svrhe drugačije od onih zbog koje su prvobitno prikupljeni. *Primera radi*, ukoliko su podaci o ličnosti prikupljeni isključivo u cilju izvršenja ugovora, oni se ne mogu koristiti za slanje čestitki ili promotivnog materijala, ukoliko to prilikom prikupljanja podataka nije navedeno.

Ipak, javljaju se i izuzeci. To znači da se podaci o ličnosti u pojedinim i izuzetnim situacijama mogu koristiti u svrhe različite od one zbog koje su prvobitno prikupljeni. Naime, obrada podataka može se naknadno preduzeti radi zadovoljenja određenog oblika javnog interesa. To je slučaj sa obradom podataka koja se vrši u cilju *istorijskih, naučnih ili statističkih istraživanja*. U tim slučajevima postoji pretpostavka da se podaci ne obrađuju suprotno svrsi zbog koje su prvobitno prikupljeni. Reč je o delatnostima koje su od značaja za širu društvenu zajednicu, pri čemu imaju mali rizik po prava i slobode građana, zbog posebnih mera zaštite koje se moraju predvideti.

Kada je reč o *novoj obradi podataka o ličnost*, dakle u svrhu različitu od one zbog koje oni su prvobitno prikupljeni (pri čemu se takva obrada ne zasniva na ograničenjima prava građana ili na pristanku), *rukovalac ima dužnost da izvrši procenu da li je prvobitna svrha prikupljanja, odnosno obrade u skladu sa novom obradom*.

U cilju njenog uspešnog sprovođenja, rukovalac mora da proceni:

1. Odnos i vezu između svrhe zbog koje su podaci prvobitno prikupljeni i nameravane (nove) svrhe obrade,

2. Okolnosti u kojima su podaci prikupljeni, pod čime se podrazumeva i odnos rukovaoca i lica na koje se podaci odnose (primera radi- da li su oni u odnosu subordinacije – radnom odnosu ili drugoj vrsti odnosa poverenja),

3. Vrstu podataka koji se obrađuju,

4. Potencijalne rizike i negativne posledice koje se mogu javiti u slučaju obrade u nove svrhe,

5. Odgovarajuće tehničke mere zaštite podataka (primera radi: kriptozaštita i pseudonimizacija).[130]

Podrazumeva se da, radi ostvarivanja zakonitosti i pravne sigurnosti, građani moraju biti obavešteni o izmenjenoj svrsi obrade, što rukovalac i obrađivač moraju posebno i jasno obrazložiti. Na taj način, ostvaruje se i princip transparentnosti, ali i građani dobijaju mogućnost da iskoriste pravna sredstva koja im stoje na raspolaganju u cilju zaštite svojih prava i interesa.

3.3.3. Načelo minimizacije podataka o ličnosti

Načelo minimizacije se odnosi na upotrebu najmanjeg mogućeg obima podataka o ličnosti. Rukovalac ili obrađivač nemaju pravo da postavljaju neprimerene zahteve građanima u vezi sa prikupljanjem i obradom podataka o ličnosti, tako da oni prevazilaze razloge zbog kojih su prikupljeni i svrhu zbog koje se obrađuju. Kada postoji potreba za obradom podataka o ličnosti, oni mogu tražiti i koristiti samo one podatke o ličnosti koji su od suštinske važnosti za ostvarivanje (zakonitog) cilja obrade. Takođe, neophodnost se odnosi i na obim podataka koji se obrađuju, tako da se u nekim situacijama mogu obrađivati samo pojedini segmenti podataka o ličnosti.

Podaci o ličnosti koji se obrađuju moraju biti primereni, značajni i ograničeni na ono što je neophodno utvrditi u odnosu na svrhu obrade.[131] Možemo reći da se ovo načelo sastoji od tri ključna elementa. To su primerenost, značaj i ograničenost obima obrade.[132] Ove elemente rukovalac, odnosno obrađivač mora obrazložiti na zahtev lica čiji se podaci obrađuju, inače obrada neće biti u skladu sa principom zakonitosti.

Pojam primerenosti odnosi se na granicu dovoljne količine podataka o ličnosti koja omogućava ostvarivanje prethodno utvrđene svrhe obrade. *Značaj*, odnosno relevantnost podataka podrazumeva neophodnu vezu između podataka o ličnosti koji se obrađuju i svrhe obrade. *Ograničenost* se odnosi na obradu i znači da se podaci mogu koristiti samo u prikupljene svrhe obrade, dok bi obrada u druge svrhe bila nezakonita. Izostavljanje nekog od navedenih elemenata značilo bi povredu načela korišćenja najmanjeg mogućeg obima podataka.

---

[130] Vid. čl. 6, st. 2 Zakona o zaštiti podataka o ličnosti.

[131] Čl. 5, st. 1, tač. 3 Zakona o zaštiti podataka o ličnosti i čl. 5, st. 1, tač. 3 Opšte uredbe EU.

[132] Pojedini autori drugačije određuju pomenuta tri elementa, pa navode da se načelo minimizacije podataka sastoji od elemenata proporcionalnosti obrade, neophodnosti obrade i nužnosti obrade podataka. A. Diligenski, D. Prlja, D. Cerović (2018), str. 82.

Radi praktičnog razumevanja ovog načela iznećemo *dva primera. Prvo*, organ poreske uprave može prikupiti podatke o imovini više lica sa istim ličnim imenom u cilju utvrđivanja određene fiskalne obaveze. U procesu obrade podataka organ će ustanoviti lice kome treba utvrditi obavezu, dok podatke o imovini ostalih lica nema pravo da obrađuje. Ipak, organ može zadržati osnovne podatke o ostalim licima kako bi se sprečila zabuna između lica kojem se utvrđuje obaveza i njih. Međutim podaci moraju biti primereni i dovoljni samo da bi se sprečila konfuzija u sličnim situacijama.

Drugo, poslodavac može imati obavezu da čuva podatke o krvnim grupama pojedinih zaposlenih na visoko rizičnim poslovima koji mogu ugroziti zdravlje i bezbednost zaposlenih (visinski radovi). Takvi podaci su neophodni za sprečavanje nastanka štetnih posledica u vanrednim situacijama koje se mogu desiti obavljanjem poslova, što čini odgovarajući i adekvatan pravni osnov za čuvanje osetljivih podataka. Ipak, podaci mogu se koristiti, odnosno obrađivati isključivo u vanrednim situacijama kada je neophodno zaštititi život i zdravlje zaposlenih na visoko rizičnim radnim mestima.[133]

3.3.4. Načelo tačnosti

Svaka zakonita i pravilna obrada zasniva se na *tačnim i potpunim podacima o ličnosti*. Kao i u matematici, bez potpunih i tačnih sabiraka nema ni pravilnog rezultata. Načelo tačnosti ima veliki značaj u javnom sektoru (kod donošenja odluka upravnih i sudskih organa), ali i u privatnom, budući da mnoga prava i interesi građana zavise od pravilne obrade podataka. To su slučajevi dobijanje kredita od banke, lečenje građana, kandidovanje na izborima, mogućnost učestvovanja na određenoj sportskoj manifestaciji i mnoge druge životne situacije koje se zasnivaju na pravilnoj analizi činjenica, odnosno podataka o ličnosti.

Načelo tačnosti odnosi se i na samu obradu. Podaci koji se skladište u bazama podataka moraju biti ažurirani i usklađivani u odnosu na promene činjeničnog stanja.[134] U praksi, ovo načelo treba da bude primenjeno tako da rukovaoci i obrađivači preduzmu sve potrebne i odgovarajuće mere koje omogućavaju tačnost i istinitost podataka o ličnosti koji se obrađuju.

---

[133] Upor. UK Information Commissioner's Office, Principle (c): Data minimisation, *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation*3.

[134] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer, eBook, online 2017, p. 91.

Pojam tačnosti znači da rukovaoci i obrađivači moraju precizno voditi baze podataka o građanima u svom posedu. *Primera radi*, ukoliko neko lice promeni mesto prebivališta iz jednog grada u drugi, u okviru iste države, podatak koji govori da lice ima prebivalište u gradu iz kojeg se preselio nije tačan, pa ga treba ažurirati i izmeniti. Sa druge strane, tačan je podatak da je lice imalo prethodno prebivalište u prvobitnom mestu stanovanja, pa taj podatak ne treba menjati.[135]

Ipak, načelo tačnosti svoju primenu nalazi i u slučajevima kada se čuva podatak za koji je utvrđeno da nije tačan. Čuvanje netačnog podataka može biti legitimno i potrebno, radi zaštite interesa lica na koga se podaci odnose. *Primera radi*, medicinski karton određenog lica može da sadrži podatak o dijagnozi koja je data, ali za koju se kasnije ispostavilo da nije tačna. Taj podatak će se čuvati iako je netačan, budući da je od značaja za dalje lečenje tog lica i uspostavljanje pravilnog postupka lečenja. Ipak, neophodno je napraviti napomenu o netačnosti takvog podatka i razloge zbog kojih je utvrđeno da je on netačan.[136]

Dakle, rukovaoci i obrađivači koji se koriste tuđim podacima o ličnosti imaju dužnost da povremeno proveravaju tačnost podataka koje čuvaju, budući da do njihove promene može doći protekom vremena, ali i pod uticajem drugih okolnosti. Naravno, kako je tačnost u prevashodnom interesu građana, oni imaju dužnost da se sami interesuju i pokažu želju za preciznim vođenjem njihovih podataka.[137]

3.3.5. Načelo ograničenog čuvanja podataka o ličnosti

Načelo ograničenja čuvanja podataka o ličnosti postavlja vremenske granice čuvanja podataka isključivo na vreme koje je zaista potrebno da se ostvari cilj obrade. Kada je ispunjena svrha radi koje su podaci prikupljeni i obrađeni, nestaje i potreba za čuvanjem podataka, odnosno gubi se osnov obrade. Uvođenjem ovog načela u sistem zaštite podataka teži se ograničavanju

[135] Upor. UK Information Commissioner's Office, Principle (d): Accuracy, *https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy*.

[136] *Ibidem.*

[137] Takva inicijativa je neretko postavljena kao pravilo, budući da rukovaoci i obrađivači ne mogu uvek voditi računa o promeni podataka svih građana, budući da se radi o velikom broju informacija. To je slučaj sa promenom prebivališta ili boravišta građana, čiju izmenu oni sami moraju da prijave nadležnom organu. Ista je situacija i sa promenama porodičnog statusa građana (promena prezimena i slično).

mogućnosti čuvanja i korišćenja tuđih podataka, čime se smanjuje i prostor za njihovu zloupotrebu.

U sistemu zaštite podataka o ličnosti Srbije, ovo načelo upućuje na to da se podaci o ličnosti moraju čuvati u obliku koji omogućava identifikaciju lica i to samo u vremenskom periodu koji je neophodan da se ostvari svrha obrade.[138] To znači da rukovaoci i obrađivači nemaju apsolutno pravo da čuvaju podatke o ličnosti koliko žele, već samo onoliko koliko su im oni potrebni za ostvarenje svrhe obrade. Dalje, ovo načelo implicira da mora postojati svrha zbog koje se podaci čuvaju određeno vreme, što stvara obavezu da se povremeno vrši pregled podataka kako bi se obrisali oni podaci koji više nisu neophodni.

Primera radi, poslodavac treba da vrši proveru podataka o ličnosti zaposlenih koji su napustili njegovu firmu. Poslodavac ne sme da čuva sve prethodno prikupljene podatke o bivšem zaposlenom zato što je otpala svrha radi koje su se podaci čuvali. Međutim, on će moći da zadrži pojedine lične podatke u vezi sa bivšim zaposlenim, koji će mu biti potrebni za regulisanje, primera radi, penzionog staža. Svi ostali podaci koji se neće koristiti, moraju se obrisati.[139]

Dakle, postupanje u skladu sa ovim načelom nalaže potrebu da se brišu podaci koji više nisu neophodni, što smanjuje mogućnost zloupotrebe, zastarelosti i netačnosti podataka koji se čuvaju. Na taj način, doprinosi se lakšem radu rukovaoca i obrađivača, koji brisanjem nepotrebnih podataka, smanjuje troškove i angažovane resurse svog poslovanja. Kada nestane potreba za čuvanjem, podaci se mogu obrisati ili učiniti anonimnim, a kao takvi se mogu koristiti u statističke ili druge svrhe. Brisanje podataka obuhvata i uklanjanje svih tragova u vezi sa njima, kao što je slučaj sa metapodacima,[140] kako bi se maksimalno smanjila mogućnost zloupotrebe.

Stava smo da se načelo treba tumačiti i tako da je potrebno dozvoliti pristup podacima o ličnosti samo pojedinim zaposlenima (kada je reč o firmama i organima javne vlasti), koji imaju stvarnu i konkretnu potrebu za određenim podacima i to u određenom vremenskom periodu. Neovlašćenim licima mora se

[138] Čl. 5, st. 1, tač. 5 Zakona o zaštiti podataka o ličnosti.

[139] Upor. UK Information Commissioner's Office, Principle (e): Storage limitation, *https://ico. org.uk /for- organisations/guide-to -the -general -data -protection -regulation -gdpr /principles/ storage-limitation*.

[140] „Metapodaci sistemski opisuju izvore podataka i omogućuju dodatne funkcionalnosti u sastavu infrastrukture prostornih podataka – IPP. Jedna od osnovnih funkcionalnosti IPP na osnovi metapodataka je usluga pronalaženja podataka… Metapodaci daju odgovore na pitanja povezana s izvorom podataka kao što su: Ko je stvorio izvor podatka? Šta je sadržaj izvora? Kada je stvoren izvor podataka? Koje područje obuhvataju podaci? Zašto su prikupljani? Kako su podaci prikupljani?". Vid. Željko Hećimović, *Metapodaci*, Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije, Katedra za geodeziju i geoinformatiku, Split 2016, str. 7.

uskratiti pristup podacima koji im ne trebaju u vršenju delatnosti kako bi se izbegle zloupotrebe položaja i kršenje privatnosti građana.

Od načela ograničenog čuvanja podataka javljaju se izuzeci, koji znače da se podaci mogu čuvati i duže od roka koji je neophodan za ostvarivanje svrhe obrade. Razlozi zbog kojih se podaci o ličnosti mogu čuvati duže jesu arhiviranje u javnom interesu, obrada u interesu istorijskog ili naučnog istraživanja. Takođe, *ovo načelo ima svoja ograničenja u odnosu na podatke u posedu organa uprave*, jer posebni upravni zakoni obavezuju na čuvanje pojedinih vrsta podataka po službenoj dužnosti i ne mogu se brisati (jedinstveni matični broj građana, podaci o zaključenju braka, itd.). Ti razlozi opravdavaju produženo čuvanje podataka, zbog značaja koje imaju za funkcionisanje države i društva.

Naravno, mogućnost dužeg čuvanja i obrade podataka ne može biti neograničena. Vremensko ograničenje se i u ovim slučajevima može predvideti posebnim zakonom. Ukoliko posebni zakon ne odredi dužinu roka u kome se mogu čuvati i obrađivati podaci, rukovalac ima obavezu da odredi takav rok, imajući u vidu sva načela zaštite podataka i prava građana.

3.3.6. Načelo integriteta i poverljivosti

Načelo integriteta i poverljivosti odnosi se na potrebu za ustanovljavanjem neophodnih mera kako bi obrada podataka bila bezbedna i kako se podaci ne bi zloupotrebljavali. Rukovalac i obrađivač moraju vršiti obradu podataka o ličnosti na način koji podrazumeva primenu tehničkih i organizacionih mera u cilju sprečavanja gubitka, oštećenja ili drugih grešaka koje mogu nastati obradom.[141] Obrada mora biti zatvorenog tipa, a rezultati obrade i sami podaci moraju se osigurati posebnim merama koje štite od neovlašćenog pristupa i zloupotrebe drugih lica, čime se ostvaruju poverljivost i integritet obrade, vrednosti svakog sistema zaštite podataka o ličnosti.[142]

Prilikom obrade podataka i ličnosti, rukovaoci i obrađivači mogu doći do značajnih informacija o životu pojedinca čiji se podaci obrađuju. Ukoliko bi ti podaci bili izgubljeni, uništeni ili zloupotrebljeni od strane trećih lica, mogle bi nastati značajne negativne posledice po prava i interese lica čiji se podaci obrađuju, ali i njemu bliskih lica. *Primera radi*, u javnost procure podaci o verskom opredeljenju direktora ustanove, što može uticati na to lice, ali i na rad same ustanove.

[141] Čl. 5, st. 1, tač. 6 Zakona o zaštiti podataka o ličnosti i čl. 5, st. 1, tač. 6 Opšte uredbe EU.
[142] P. Voigt, A. Bussche (2017), p. 92.

U modernom informacionom društvu, podaci o ličnosti mogu se zloupotrebiti na različite načine. Moguća je zamena identiteta, nedozvoljene elektronske novčane transakcije, objavljivanje strogo poverljivih podataka o ličnosti, lažno prijavljivanje, itd. Kako bi se sprečile negativne posledice po pojedince i društvo, propisi ustanovljavaju sisteme zaštite koji se zasnivaju na pravnim, organizacionim, tehničkim i informatičkim merama koje treba da pruže zaštitu od svakog vida zloupotrebe.

Podrazumeva se, tehničke, organizacione i kadrovske mere koje čine suštinu principa integriteta i poverljivosti, najviše se ostvaruje kroz mehanizam informacione bezbednosti čiji je cilj da „osigura kontinuitet poslovanja (obrade) i potpuno smanji štetu po poslovanje sprečavajući i smanjujući mogućnost bezbednosnih incidenata“,[143] pa tako i izlaze iz čisto pravne sfere i podrazumevaju informatička i organizaciona znanja i veštine.

3.3.7. Načelo odgovornosti

Kako bi sistem pravne zaštite podataka o ličnosti mogao da ostvaruje zaštitnu funkciju neophodno je ustanoviti prava i obaveze svih lica koja učestvuju u aktivnostima obrade. U ovim aktivnostima, po pravilu, učestvuju lica čiji se podaci obrađuju (fizička lica) i lica koja obrađuje podatke o ličnosti (fizičko, pravno lice ili organ vlasti). U ovim aktivnostima mogu učestvovati i druga lica, kao što su primaoci podataka i treća lica, ali ona imaju manji značaj u odnosu na pomenuta lica.

Budući da rukovalac određuje svrhu obrade i upravlja tuđim ličnim dobrima (podacima o ličnosti), on je odgovoran za pravilnost i zakonitost obrade, kao za i eventualne posledice. Tako je i nastao jedan od osnovnih principa zaštite podataka - odgovornost rukovaoca za pravilnost obrade podataka o ličnosti. Ova odgovornost zasniva se na odnosu odgovornosti sa licem čiji se podaci obrađuju, ali i na odnosu prema celokupnoj društvenoj zajednici i javnom poretku. Na taj način se zaštitom podataka o ličnosti štite univerzalne društvene vrednosti i celokupni pravni sistemi.

Pojam odgovornosti u opštem smislu odnosi se „na postupanje prema pravilima koje propisuje neka društvena norma…Pri korišćenju pojma odgovornost, prva asocijacija je da nešto nije izvršeno od strane nekoga, a

[143] Rossouw von Solms, „Information security management: why standards are important“, *Information Management & Computer Security*, 7/1, MCB UP Ltd., UK 1999, p. 56.

postojala je obaveza da se to uradi".[144] U odnosu na opšti pojam, možemo zaključiti da u pravnom smislu odgovornost znači postupanje prema predviđenim pravnim normama i snošenje posledica zbog njihovog nepoštovanja. Prema tome, načelo odgovornosti u vezi sa zaštitom podataka ustanovljava opštu obavezu lica koje obrađuje podatke da poštuje predviđene norme i pravilnost obrade.

Ovaj princip prepoznat je još 1980 godine, od strane *Organizacija za ekonomsku saradnju i razvoj (OECD) koja je u Smernicama za zaštitu privatnosti i prekogranični protok ličnih podataka* prepoznala odgovornost rukovalaca značajnu meru za usklađivanje poslovanja prema ovim Smernicama. U domaće zakonodavstvo usvojen je kroz načelo društvene odgovornosti po ugledu na Opštu uredbu EU.[145]

Rukovalac mora u potpunosti da uskladi svoje poslovanje sa opštim propisima koji uređuju zaštitu podataka i propisima koji se odnose na oblast njegovih delatnosti. Posledično, rukovalac mora da bude u mogućnosti da dokaže usklađenost obrade sa tim pravilima. Usklađenost podrazumeva primenu pravnih, tehničkih i organizacionih mera koje su neophodne radi zaštite ličnih prava građana i njihovih podataka. Princip odgovornosti podrazumeva i dužnost rukovaoca da kontinuirano vodi računa o podacima građana u njegovom posedu, ali i da vodi računa o razvoju tehnologije i mera zaštite.

Načelo odgovornosti prevashodno je usmereno ka poboljšanju pozicije građana i njihovih podataka o ličnosti. Građani sada znaju kome mogu da se obrate ukoliko se pojavi neki problem sa njihovim podacima. Rukovaoci ne mogu više lako izbeći odgovornost za podatke građana koji se nalaze u njihovom posedu. Uz to, kao posledice odgovornosti predviđaju se značajne sankcije za nepoštovanje odredaba, u vidu materijalne (novčane), disciplinske, prekršajne, ali i krivične odgovornosti.

Kako bi se ovo načelo iz teorijskih visina spustilo na praktični teren, teorija mora da se prilagodi praksi. Na nivou EU, u okviru Mišljenja Radne grupe člana 29, predviđene su minimalne mere koje služe praktičnoj implementaciji načela zaštite podataka. Ne ograničavajući se na ove mere, Radna grupa člana 29 pominje sledeće minimalne mere za rukovaoce, putem kojih se ostvaruje princip odgovornosti:

- *Određivanje unutrašnjeg (internog) postupka, od samog početka obrade podataka o ličnosti,*

[144] Aleksandra Ilić Petković, Mile Ilić, „Odgovornost državnih službenika i zaštita njihovih prava", *Godišnjak Pedagoškog fakulteta u Vranju*, 1/2017, (ur. Sunčica Denić), Pedagoški fakultet u Vranju, Vranje 2017, str. 94.

[145] A. Diligenski, D. Prlja, D. Cerović (2018), str. 85.

- *Kreiranje strategije zaštite podataka koja se zasniva na načelima zaštite podataka,*
- *Mapiranje postupaka koji služe određenju svih aktivnosti u vezi sa podacima o ličnosti,*
- *Određivanje lica ovlašćenog za zaštitu podataka ili drugih lica koja su odgovorna za lične podatke,*
- *Omogućavanje odgovarajuće obuke, treninga i usavršavanja zaposlenih (pod kojima se podrazumevaju i IT menadžeri, programeri, menadžeri ljudskih resursa i svi drugi koji rukuju podacima o ličnosti) u vezi sa zaštitom ličnih podataka,*
- *Uspostavljanje unutrašnjih pravila u vezi sa efikasnim upravljanjem i prijavljivanjem povrede podataka o ličnosti,*
- *Uspostavljanje postupaka u kojima se ostvaruju ljudska prava u vezi sa podacima o ličnosti,*
- *Sprovođenje procene uticaja u posebnim slučajevima obrade,*
- *Implementacija i kontrola primene svih mera.*[146]

Primena ovih mera ne znači automatski i usklađivanje sa pravni propisima u ovoj oblasti. Posebne vrste podataka zahtevaju preduzimanje specifičnih mera, a u obzir treba uzeti i načine obrade, količinu podataka koji se obrađuju i druge faktore od kojih zavisi primena zaštitne mere. Svakako, pomenute mere treba da služe kao odlična polazna osnova i smernica rukovaocima u kreiranju svog internog sistema zaštite podataka o ličnosti.

3.3.8. Obrada posebnih kategorija podataka o ličnosti

Pojedine vrste podataka o ličnosti uživaju veći stepen zaštite u odnosu na zaštitu koja se uobičajeno pruža. Tako, javljaju se kategorije podataka koje se načelno ne smeju obrađivati. One uživaju posebnu zaštitu zato što se odnose na karakteristike strogo lične prirode, čijom povredom ili zloupotrebom može doći da negativnih posledica po fizičko lice na koje se odnose. Praktično posmatrajući, povreda ovih kategorija podataka može imati uticaja na društvenu poziciju, ugled i status lica.

Ova vrsta podataka obično nosi naziv (naročito) osetljivi podaci o ličnosti. Tako ih je nazivao i prethodni Zakon o zaštiti podataka o ličnosti (2008).

[146] Radna grupa člana 29, *Mišljenje 3/2010 o principu odgovornosti*, br. 00062/10/EN, WP 173, od 13. 07. 2010. godine, str. 11-12.

Aktuelni Zakon o zaštiti podataka o ličnosti određuje ovu vrstu kao „*posebnu kategoriju*“ podataka o ličnosti čija obrada nije dozvoljena. U ovu grupu spadaju podaci koji se odnose na:

1. *Rasno i etničko poreklo,*
2. *Političko mišljenje,*
3. *Versko i filozofsko uverenje,*
4. *Članstvo u sindikatu,*
5. *Genetske podatke,*
6. *Biometrijske podatke,*
7. *Podatke o zdravstvenom stanju,*
8. *Podatke o seksualnom životu i seksualnoj orijentaciji lica.*[147]

Ipak, i pored načelne zabrane obrade ovih kategorija podataka, javljaju se određene situacije u kojima njihova obrada dopuštena.[148] Te situacije odnose se na postojanje određenog oblika javnog interesa ili značajnog privatnog interesa rukovaoca, koji preteže nad interesima lica čiji se podaci obrađuju. Objektivno posmatrajući, ukoliko ne bi postojala mogućnost obrade posebnih kategorija podataka, pravni sistem ne bi mogao normalno da funkcioniše i redovni društveni tokovi bi bili sputani i usporeni. Naravno, rukovaoci i obrađivači su dužni da prilikom obrade ovih podataka obezbede odgovarajuće tehničke, organizacione i kadrovske mere u cilju zaštite prava i interesa lica čiji se podaci obrađuju, što predstavlja poseban uslov obrade posebnih vrsta podataka.

Postoji nekoliko situacija u kojima je dopuštena obrada posebnih vrsta podataka o ličnosti. Ove situacije predstavljaju izuzetak od pravila da se posebne kategorije ne smeju obrađivati.

Prvo, obrada posebnih vrsta podataka o ličnosti može se vršiti uz pristanak lica na koga se podaci odnose. Kada postoji izričita i jasna saglasnost, nema smetnje korišćenju ovih podataka. Pravila koja se odnose na pristanak u odnosu na druge podatke o ličnosti, važe i u slučaju pristanka na obradu posebnih kategorija podataka. Napominjemo da pristanak kao osnov obrade posebnih vrsta podataka o ličnosti može biti izuzet posebnim zakonom.

U vezi sa pristankom treba pomenuti i drugi slučaj koji omogućava obradu posebnih vrsta podataka. Kada je lice „očigledno učinilo javno dostupnim“ svoje podatke o ličnosti, takvi podaci mogu se obrađivati. Ovaj slučaj možemo kvalifikovati kao implicitno davanje saglasnosti, budući da u uslovima informaciono-komunikacionih tehnologija i interneta svako lice treba da bude

[147] Čl. 17, st. 1 Zakona o zaštiti podataka o ličnosti.

[148] Posebni slučajevi mogućnosti obrade posebnih vrsta podataka o ličnosti predviđeni su u čl. 17, st. 2 Zakona o zaštiti podataka o ličnosti.

svesno da podaci koji su obelodanjeni i učinjeni dostupnim svima, mogu biti korišćeni u razne svrhe. Pri svemu tome, treba imati u vidu da je gotovo nemoguće pratiti dalji protok jednom objavljenih podataka.

Primera radi, objava podataka o ličnosti, poput fotografija ili video zapisa na društvenim mrežama poput *Facebook*-a ili *Instagram-a*, uz korišćenje opcije da su takvi podaci dostupni svima, bez ograničavanja na određeni krug lica („prijatelja" ili „pratioca"), omogućava dalje korišćenje ovih podataka bez posebne saglasnosti. U teoriji se navodi da je „ovaj kriterijum dopuštenosti obrade izuzetno problematičan i da otvara mogućnost manipulacije i pravne nesigurnosti u praksi. To bi značilo da su podaci o ličnosti koji su očigledno objavljeni od strane pojedinca dopušteni za dalju obradu od strane bilo kojih rukovaoca".[149]

Zaista, javlja se dilema da li je legitimno dozvoliti svim korisnicima interneta da mogu koristiti objavljene podatke o ličnosti. Sa jedne strane, javlja se potreba za zaštitom građana u odnosu na korišćenje njihovih podataka, pa čak i u slučaju da su ih oni javno objavili. Sa druge strane, građani moraju da budu svesni mogućnosti interneta i javnog objavljivanja i objavljivanja podataka o ličnosti. Država i zakoni ostaju nemoćni da pruže zaštitu svim podacima koji su objavljeni, pa su zbog toga građani u krajnjoj liniji ti koji odlučuju da li će svoje podatke poveriti nepreglednoj i nesagledivoj internet zajednici od preko 7 milijardi korisnika.[150]

Dalje, rukovaoci u oblasti rada, socijalnog osiguranja i socijalne zaštite imaju pravo da obrađuju posebne podatke kada je takva obrada neophodna radi izvršenja obaveze njihove organizacije. Ova obrada mora biti predviđena posebnim zakonom ili kolektivnim ugovorom o radu, što znači da nije dovoljna pojedinačna odluka rukovaoca kao osnov obrade posebnih vrsta podataka o ličnosti. Zakon ili kolektivni ugovor o radu koji dozvoljava obradu posebnih vrsta podataka u prethodno pomenute svrhe mora propisati i adekvatne mere zaštite za prava i sloboda za lica na koje se podaci odnose. Razlog uspostavljanja mera leži u osetljivom karakteru radnih i socijalnih odnosa u društvu i velikog uticaja podataka o ličnosti u ovim društvenim oblastima.

Životno važni interesi lica na koje se podaci odnose, ali i drugih lica dozvoljavaju obradu posebnih vrsta podataka. Ova mogućnost posebno dobija na značaju u situacijama kada lice nije u stanju ili mogućnosti da da svoj pristanak

[149] A. Diligenski, D. Prlja, D. Cerović (2018), str. 106.

[150] Procenjuje se da u Africi internet koristi milijardu i 340 miliona ljudi, u Evropi 843 miliona, dok je najveći broj u Aziji, gde internet zajednica broji neverovatnih 4 milijarde i 294 miliona ljudi u 2020. godini. Više o statistici internet korisnika vid. Internet World Stats, Internet Users Distribution in the World – 2020 Q1, https://www.internetworldstats.com/stats.htm.

na obradu. Naravno, reč je o vanrednim situacijama koje sprečavaju lice na davanje pristanka, pa uobičajenu sprečenost lica na davanje pristanka ne treba posmatrati kao osnov koji opravdava obradu. *Primera radi*, kod pružanja hitne medicinske pomoći, opravdano je pristupiti zdravstvenim podacima radi uspostavljanja adekvatne dijagnoze i metoda lečenja.

Posebne podatke mogu obrađivati organizacije poput zadužbina, fondacija, udruženja ili drugih neprofitnih organizacija čija je delatnost usmerena na političko, filozofsko, versko ili sindikalno delovanje. Pomenute organizacije mogu koristiti podatke o ličnosti isključivo u cilju funkcionisanja i obavljanja poslova iz nadležnosti organizacije. U tom smislu, mogu se obrađivati jedino podaci članova ili sa organizacijom povezanih lica, uz dodatan uslov da se takvi podaci ne objavljuju, odnosno otkrivaju izvan organizacije. Tako crkve i verske organizacije mogu obrađivati podatke o ličnosti svojih vernika kada su dali pristanak na obradu pojedinih podataka.

U vezi sa sudskim i drugim pravnim postupcima, dozvoljena je obrada posebnih kategorija podataka koja se odvija u cilju podnošenja, ostvarivanja ili odbrane od pravnog zahteva. To znači da jedno lice može koristiti posebne kategorije podataka o ličnosti, ako one predstavljaju neophodno sredstvo u cilju odbrane od tužbenog zahteva koji je uperen protiv tog lica. Potreba pravilnog vođenja sudskog postupka i saznavanja istine u postupku zahteva temeljnu analizu svih činjenica konkretnog slučaja koje se mogu odnositi i na posebne kategorije podataka. Ukoliko sloboda jednog lica zavisi od pristupa podacima od ličnosti, logično je dozvoliti njihovu obradu da bi se zaštitilo tako značajno lično dobro.

Lica privatnog prava i organi javne vlasti mogu vršiti obradu posebnih vrsta podataka kada postoji potreba za ostvarivanjem „značajnog javnog interesa“. Javni interes utvrđuje se zakonom, a procenjuje se u zavisnosti od činjenica svakog konkretnog slučaja. Čak i kada postoji javni interes, on mora biti značajan, što je stvar slobodne ocene onog koji obrađuje podatke. Značaj javnog interesa može se procenjivati prema broju pogođenih ili ugroženih lica i pojedinačnih interesa, eventualnoj finansijskoj, materijalnoj ili drugoj vrsti posledice koja može nastati, itd. Primera radi, postavljanje video nadzora u prodavnici radi zaštite bezbednosti lica i imovine ne bi trebalo da predstavlja značajan javni interes, već se moraju pružiti i razlozi koji opravdavaju značaj bezbednosti u pogledu broja građana ili vrednosti imovine koja se štiti.

U svakom slučaju, mora se voditi računa i o principu srazmernosti, poštovanju „suštine prava“ fizičkih lica čiji se podaci obrađuju i merama zaštite podataka o ličnosti. To znači da se u svakom konkretnom slučaju mora

procenjivati domašaj i odnos pojedinih prava i sloboda građana sa jedne strane i javni interes, sa druge strane. Smatramo da se takva obrada mora temeljno obrazložiti, što znači da ne sme da se zasniva isključivo na opštim zakonskim formulacijama.

Značajan osnov koji opravdava obradu posebnih vrsta podataka odnosi se na poslove koji se obavljaju u cilju zaštite javnog zdravlja. Kao konkretni primeri zaštite javnog zdravlja možemo pomenuti situacije u kojima je potrebna zaštita od ozbiljnih prekograničnih pretnji zdravlju stanovništva, obezbeđivanje visoko standarda kvaliteta i sigurnosti zdravstvene zaštite lekova i medicinskih sredstava, itd. U vezi sa poslovima javnog zdravlja, od velike je važnosti voditi računa o institutu čuvanja profesionalne tajne koja se odnosi i na lične podatke, a što znači da se svaki podataka sa kojim se obveznik profesionalne tajne upoznao u vršenju posla iz svoje delatnosti, ne sme dalje prenositi, osim ukoliko sud to lice ne oslobodi od dužnosti njenog čuvanja.

Obrada posebnih kategorija podataka može se preduzeti radi ostvarivanja preventivnih dužnosti u medicini ili medicini rada u cilju ocenjivanja radne sposobnosti zaposlenih i budućih zaposlenih, što mora biti utemeljeno na zakonu ili kolektivnom ugovoru. Takođe, posebne vrste podataka mogu se obrađivati i u cilju uspostavljanja medicinske dijagnostike, kao i pružanja usluga zdravstvene i socijalne zaštite. Logično, većina ovih situacija će se odnositi na upravljanje medicinskim podacima u cilju postavljanja odgovarajuće dijagnoze ili terapije, što naravno ne isključuje i ostale vrste podataka koje mogu imati uticaj na metode i način lečenja, poput verske pripadnosti i implikacija takvog statusa na zdravlje lica. Naravno, mora se voditi računa o domašaju dužnosti čuvanja profesionalne tajne.

Mogućnost obrade posebnih kategorija podataka o ličnosti može se preduzeti i u cilju arhiviranja u javnom interesu, u interesu naučnog ili istorijskog istraživanja kao i u statističke svrhe.[151] Smatramo da je ova odredba postavljena široko i da dopušta relativno lak pristup posebnim kategorijama podataka. Kao dodatni uslov za vršenje ovakvih obrada predviđeno je poštovanje suštine prava na zaštitu podataka i primena odgovarajućih i posebnih mera zaštite podataka koji se obrađuju. Smatramo da ovu odredbu treba postaviti znatno uže, u smislu da bi ona trebalo da predstavlja predmet posebnog zakona koji bi predvideo dodatne uslove, poput dužnosti obrazloženja svake obrade u pomenute svrhe.

Kao što smo pomenuli, za razliku od zakona koji je trenutno na snazi, prethodni Zakon o zaštiti podataka o ličnosti (2008) ovu kategoriju je oslovljavao kao „naročito osetljive podatke“. On je sadržao dužu listu „posebnih“, odnosno

[151] Čl. 17, st. 2, tač. 10 Zakona o zaštiti podataka o ličnosti.

naročito osetljivih podataka. U odnosu na trenutno stanje stvari, kao naročito osetljivi podaci bili su predviđeni i pol, jezik, pripadnost političkoj stranci, podaci o primanju socijalne pomoći, podaci o žrtvama nasilja i podaci o osudi za učinjeno krivično delo. Značajna odredba u odnosu na obradu naročito osetljivih podataka odnosila se na to da je i mere zaštite i način arhiviranja podataka iz ove kategorije uređivala Vlada, uz prethodno pribavljeno mišljenje Poverenika. Ova odredba je izostala u novom zakonu. Smatramo da je pomenute pravilo omogućavalo stabilan nivo zaštite osetljivih podataka. Takvo stepenovanje (nivoa zaštite) treba široko prihvatati u oblasti zaštite podataka, jer što je više stepena zaštite, manja je opasnost od povrede (osetljivih) podataka.

3.4. Nosioci prava na zaštitu podataka o ličnosti

Da bi jedan podatak predstavljao podatak o ličnosti, on se mora odnositi na fizičko lice. Uz to, nije dovoljno da se radi o bilo kom licu, već podaci moraju upućivati na tačno određeno ili odredivo fizičko lice.

Može se postaviti pitanje zakonitosti takvog stava u svetlu jednakosti fizičkih i pravnih lica pred zakonom. Naime, u Srbiji sva lica su jednaka pred Ustavom i zakonom. Međutim, pravna zaštita podataka o ličnosti pruža se isključivo fizičkim licima, dok pravna lica ostaju izvan okvira pravne zaštite. Ista je situacija i u EU, gde se izričito navodi da Opšta uredba EU ne pruža zaštitu podacima koji se odnose na pravna lica, što se odnosi i na društva koja su osnovana kao pravna lica (uključujući njihov naziv, sedište, pravnu formu i podatke za kontakt).[152]

Pravnim licima se garantuje pravni subjektivitet, ali im nije omogućena zaštita podataka o ličnosti u pomenutim propisima. Sagledavajući celokupni kontekst i odnos pravnih lica i podataka o ličnosti, možemo reći da postoje argumenti za i protiv, da i pravna lica treba da budu nosioci podataka o ličnosti i samim tim subjekti prava na zaštitu. Osnovni argument da i pravna lica treba da uživaju zaštitu podataka o ličnosti jeste da i ona predstavljaju „ličnosti“, odnosno da imaju pravni subjektivitet, da svojom voljom mogu da utiču na pravne odnose i da podjednako, kao i fizička lica, učestvuju u pravnom saobraćaju. Tom logikom, podaci o ličnosti pravnih lica u pravnom prometu imaju značajnu ulogu, budući da se mogu odnositi na specifična svojstva i da mogu nositi poverljive informacije

[152] Uredba navodi i to da će se primenjivati na sva fizička lica u okviru EU, bez obzira na državljanstvo, prebivalište ili boravište lica čiji se podaci štite. Vid. tač. 14 Premabule Opšte uredbe EU.

o pravnom licu (kao što su podaci o unutrašnjoj organizaciji, interna organizacija, poslovne odluke, itd.).

Sa druge strane, osnovni argument protiv teze da i pravna lica treba da uživaju zaštitu podataka o ličnosti zasniva se na tome da ona predstavljaju „fiktivne tvorevine" koje su kreirane „veštački", odlukom nadležnog organa države (organa javne uprave ili suda). Uz to, ova lica nemaju svoju volju, već njihovu volju predstavljaju fizička lica koja imaju glavnu ulogu u svim odnosima pravnih lica. Svi podaci koji su od značaja za pravno lice moraju biti dostupni javnosti (u Srbiji podaci o pravnim licima mogu se pronaći na sajtu Agencije za privredne registre), zbog toga što se osnivaju odlukom nadležnog organa, pa se na taj način izbegavaju moguće zloupotrebe.

Možemo reći da se u praksi javljaju određene situacije u kojima može doći do zloupotrebe (ličnih) podataka koji se odnose na pravna lica. Pravno lice poseduje niz podataka koje koristi u svakodnevnom pravnom prometu (računi pravnog lica, interni akti o unutrašnjoj organizaciji, poslovne odluke, potpis zastupnika pravnog lica, podaci o ličnosti zastupnika, stanje na bankovnom računu pravnog lica i drugi). Uz to, pravna lica uživaju i određeni ugled u društvu, odnosno reputaciju.[153] Takvi podaci mogu nositi informacije koje se mogu zloupotrebiti ili se mogu koristiti u cilju narušavanja reputacije pravnog lica.

U takvim situacijama pravna lica nemaju mogućnosti da ostvare pravnu zaštitu podataka, budući da oni ne predstavljaju subjekte prava na zaštitu podataka o ličnosti. To nas dovodi do zaključka da bi radi sveobuhvatne pravne zaštite podataka o ličnosti, budući da su oni u centralnom fokusu zaštite, a ne lica na koja se odnose, trebalo proširiti pravnu zaštitu i na pravna lica. Pravna lica mogu trpeti štetne posledice zbog zloupotrebe njihovih podataka o ličnosti. Uz to, u modernim pravnim sistemima pravna lica poseduju pravni subjektivitet, te njegovi organi predstavljaju deo pravnog lica, što znači da njihove radnje predstavljaju radnje pravnog lica. Logikom stvari, podaci fizičkih lica, kada oni deluju u svojstvu predstavnika ili drugog organizacionog dela pravnog lica, predstavljaju i podatke fizičkog lica i podatke pravnog lica koji bi trebalo da uživaju pravnu zaštitu.

[153] U teoriji je prihvaćen stav da se pravnim licima priznaje pravo na čast, kao i pravo na reputaciju, odnosno dobar glas. Više o tome vid. Slavica Krneta, „Lična prava pravnih lica", *Godišnjak Pravnog fakulteta u Sarajevu*, br. XXV, Sarajevo 1977, str. 162.

3.4.1. Nosioci prava na zaštitu podataka o ličnosti u EU

U pravnom sistemu EU isključivo fizička lica uživaju zaštitu podataka o ličnosti.[154] Dakle, pravna lica ne uživaju mogućnost zaštite podataka o ličnosti. U odnosu na fizička lica, Opšta uredba EU predviđa da se njene odredbe neće primenjivati na podatke o ličnosti preminulih osoba.[155] Ova odredba je tzv. otvorena klauzula, budući je u odnosu na ovo pitanje ostavljena mogućnost državama članica da svojim propisima urede obradu podataka o ličnosti preminulih lica. Na ovaj način ne dira se u obrade podataka o ličnosti koje se vrše u arheološke i istorijske svrhe, na koje se primenjuju odredbe Opšte uredbe EU.

Za fizička lica predviđena je starosna granica od koje se stiče puna sposobnost za samostalno odlučivanje i davanje pristanka za obradu podataka o ličnosti. „Punoletstvo" za davanje saglasnosti na obradu podataka o ličnosti prema pravu EU stiče se sa 16 godina života, i to u vezi sa uslugama informacionog društva. U vezi sa ovom starosnom granicom, ostavljena je mogućnost državama članicama da predvide i nižu starosnu granicu, ali da ne ide ispod 13 godina života. Međutim, ova odredba ni na koji način ne utiče na regulativu opšteg ugovornog prava u državama članicama, što treba da omogući normalno odvijanje poslovnih tokova i zaključenje različitih ugovora.

Izmenu otvorene klauzule u vezi sa starosnom granicom za davanje saglasnosti na obradu podataka o ličnosti učinila je Francuska. To je učinjeno u Zakonu o zaštititi podataka o ličnosti Francuske, gde se za zakonitost obrade podataka zahteva da dete ima najmanje 15 godina, čime se snižava granica „digitalnog punoletstva" u francuskom pravu u odnosu na onu iz Opšte uredbe EU.[156] Osim Francuske i u Austriji je pomerena starosna granica za samostalno odlučivanje o obradi podataka u vezi sa uslugama informacionog društva. U Austriji, dete već sa 14 godina života stiče mogućnost da samostalno odlučuje o

[154] Kao što je prethodno navedeno u istraživanju, izuzetak predstavlja pravo Austrije. Zakon o zaštiti podataka o ličnosti Austrije sadrži ustavnu odredbu o jednakosti lica na koja se primenjuje zakon, pa je ostalo otvoreno pitanje, da li će austrijsko pravo pružati zaštitu i pravnim licima, iako to izlazi iz okvira Opšte uredbe EU, koja se primenjuje u svim državama članicama EU, pa tako i u Austriji.

[155] Parlament Francuske je 20. juna 2018. godine usvojio Zakon o zaštiti podataka o ličnosti br. 2018-493, čime je Francuska izmenila svoje zakonodavstvo u oblasti zaštite podataka, koje je bilo na snazi od 1978. године. Usvajanjem ovog zakona, Francuska je uskladila svoju regulativu sa odredbama Opšte uredbe EU. Tač. 27 Opšte uredbe EU.

[156] Vid. čl. 20 francuskog Zakona o zaštiti podataka o ličnosti.

obradi podataka koje se vrše u vezi sa informacionim tehnologijama.[157] U slučaju kada je dete mlađe od 16 godina života, pristanak za obradu njegovih podataka o ličnosti daje roditelj ili zakonski zastupnik. U takvim situacijama postoji posebna obaveza rukovaoca da izvrši sva neophodna ispitivanja u cilju saznanja da li je pristanak dat na zakonit način i od strane ovlašćenog lica, kako bi se zaštitio poseban interes deteta.

3.4.2. Nosioci prava na zaštitu podataka o ličnosti u pravu Srbije

3.4.2.1. Zaštita podataka o ličnosti maloletnih lica

Trenutno stanje regulative u Srbiji omogućava pravnu zaštitu ličnih podataka isključivo fizičkim licima. Međutim, postavlja se pitanje, da li je svim fizičkim licima omogućena zaštita podataka o ličnosti? U skladu sa načelom jednakosti i zabrane diskriminacije sva fizička lica uživaju zaštitu podataka o ličnosti.

Starosna granica u vezi sa pojedinim pitanjima zaštite podataka postavljen je i u Srbiji. U tom smislu, lice koje nije navršilo 15 godina života može dati pristanak za obradu njegovih podataka o ličnosti u vezi sa korišćenjem usluga informacionog društva jedino uz pristanak roditelja, odnosno zakonskog zastupnika.[158] Kada navrši 15 godina života, maloletno lice može samostalno dati svoj pristanak na obradu podataka o ličnosti u odnosu na usluge informacionog društva. To znači da je i maloletnicima garantovana zaštita, koja ima drugačiji modalitet ostvarivanja u odnosu na ostala fizička lica.

Rukovaoci i obrađivači imaju dužnost da preduzmu adekvatne i razumne mere u cilju provere da li postoji pristanak roditelja ili zakonskog zastupnika, u slučaju obrade podataka o ličnosti maloletnika koji nije navršio 15 godina. Ova dužnost organa uprave usmerena je na sprečavanje zloupotreba informacionih tehnologija kod davanja pristanka, budući da deca putem računara mogu samostalno dati pristanak, iako nisu svesna posledica takvog postupka.

[157] Vid. čl. 2, poglavlje 1., deo 1., paragraf 4., st. 4 Zakona o zaštiti podataka o ličnosti Austrije.
[158] Čl. 16 Zakona o zaštiti podataka o ličnosti.

3.4.2.2. Zaštita podataka o ličnosti preminulih lica i podobnost za nasleđivanje prava na zaštitu podataka o ličnosti

Da li samo živa fizička lica uživaju zaštitu podataka o ličnosti ili se pravna zaštita odnosi i na preminula lica? Fizičko lice rođenjem stiče pravni subjektivitet, dok smrću pravni subjektivitet prestaje. Ipak i nakon smrti u pravnom životu figuriraju određena prava i interesi u vezi sa preminulim licima, koje mogu ostvarivati njihovi naslednici.

Postupanje sa podacima preminulih lica regulisao je prethodni Zakon o zaštiti podataka o ličnosti (2008). Ovaj zakon propisivao je dve situacije u vezi sa ličnim podacima preminulih lica. Prva se odnosi na slučaj kada su podaci o ličnosti prikupljeni na osnovu ugovora ili pismene saglasnosti preminulog lica. Takvi podaci čuvali su se u skladu sa utvrđenim ugovorom, odnosno u skladu sa datom saglasnošću.

Drugi slučaj odnosio se na lične podatke prikupljene na osnovu zakona ili drugog propisa. U slučaju smrti njihovog imaoca, postojala je obaveza rukovaoca ili obrađivača da takve podatke čuva najmanje godinu dana od dana smrti tog lica. Zajedničko za oba slučaja je obaveza lica koje čuva podatke da sačini belešku prilikom njihovog uništavanja.[159]

U prethodnom zakonu postojala je i odredba koja je određivala krug lica koja su mogla da daju dozvolu za korišćenje podataka o ličnosti preminulog u tačno određene svrhe. Takvo odobrenje moglo se dati radi sačinjavanja biografije, korišćenja ličnih fotografija, upotrebe ličnog imena i tome slično. Pristanak za obradu podataka umrlih lica mogla su dati lica koje je preminuli odredio, supružnik tog lica, deca starija od 15 godina, braća i sestre i drugi zakonski naslednici. Ova lica mogla su da koriste pravna sredstva za zaštitu podataka o ličnosti tog lica.

U aktuelnom zakonodavstvu Srbije ne postoji odredba koja uređuje pitanje da li i preminula lica uživaju zaštitu podataka o ličnosti. Zakon o zaštiti podataka o ličnosti propustio je da reguliše ovo važno pitanje. Norme zakona uređuju „pravo na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti“, a fizičko lice, prema odredbama Zakona, predstavlja „fizičko lice čiji se podaci obrađuju“,[160] što ne govori o tome da li se pod fizičkim licima podrazumevaju i preminula lica.

[159] Čl. 35 Zakona o zaštititi podataka o ličnosti (2008).
[160] Čl. 4, st. 1, tač. 2 Zakona o zaštiti podataka o ličnosti.

Postupanje sa pravima preminulih osoba uređuje Zakon o nasleđivanju.[161] Ovim zakonom predviđeno je da se nasleđuje zaostavština, a zaostavštinu čine „sva nasleđivanju podobna prava koja su ostaviocu pripadala u trenutku smrti".[162] To otvara novo pitanje, da li je pravo na zaštitu podataka o ličnosti pravo koje je podobno za nasleđivanje?

Smatramo da je pravo na zaštitu podataka o ličnosti, kao pravo koje se sastoji od više užih i posebnih prava, podobno za nasleđivanje u odnosu na pojedine lične podatke. Naime, smrću lica ne prestaje potreba za zaštitom njegove ličnosti, odnosno njegovih podataka o ličnosti. Mehanizme pravne zaštite mogu inicirati naslednici preminulog. Zbog toga, naslednicima treba omogućiti pravo na zaštitu podataka o ličnosti preminulog, budući da do povrede podataka o ličnosti može doći i nakon smrti, a naslednici, kao neposredno i posredno zainteresovana lica, treba da imaju na raspolaganju mehanizme zaštite podataka o ličnosti preminulog.

[161] Zakon o nasleđivanju, „Sl. glasnik RS", br. 46/95, 101/2003.
[162] Čl. 1, st. 1 i st. 2 Zakona o nasleđivanju.

4. PRAVA GRAĐANA U VEZI SA PODACIMA O LIČNOSTI

4.1 Uvod

Osnovni cilj posebnih ljudskih prava u oblasti zaštite podataka o ličnosti jeste da se pruži zaštita privatnosti, čime se omogućava slobodan razvoj ličnosti u savremenom društvu. Na taj način štite se pojedinci, ali i društvo, odnosno celokupan pravni poredak.

Prava građana u vezi sa zaštitom podataka o ličnosti možemo odrediti kao lična prava. *Lična prava* predstavljaju deo porodice građanskih prava kojima se štiti jedinstvenost i neponovljivost čovekove ličnosti. Njihov cilj jeste da omoguće slobodan razvoj pojedinca u društvu, omogućavajući mu ispoljavanje svih posebnosti koje ga odlikuju kao jedinstveno i neponovljivo biće. Zbog toga ona predstavljaju jedan od osnovnih postulata demokratskih društava. Lična prava su „subjektivna prava na ličnim dobrima, kao što su: pravo na život, fizički integritet, zdravlje, psihički integritet, pijetet, dostojanstvo, čast, ugled, privatni život, lik, glas, lični zapis, tajnu sferu, lične podatke, identitet, ime i dr. Ona omogućavaju imaocu da svoje lično dobro ostvari, uživajući ga i raspolažući njime“.[163] Njihov osnovni cilj je da *zaštite pojedinca i njegova lična dobra od neovlašćenog uticaja svih trećih lica*. Na taj način omogućava se slobodan život i neograničeno raspolaganje ličnim dobrima.

Propisi obično navode lična prava građana, ali ne zatvaraju njihov krug, budući da se njihov broj u današnjim okolnostima neprestano povećava. Ponekad, podaci o ličnosti su zaštićeni zajedno sa drugim ličnim dobrima, odnosno pravima. Takav je slučaj sa pravom na privatnost, koje je predviđeno u Univerzalnoj deklaraciji o ljudskim pravima i Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda. S druge strane, pojedini propisi predviđaju pravo na zaštitu podataka o ličnosti kao posebno ljudsko pravo, koje je složeno i koje se sastoji iz niza ovlašćenja garantovanih njegovom imaocu.[164] Takav je

[163] Obren Stanković, Vladimir Vodinelić, *Uvod u građansko pravo*, Nomos, Beograd 2007, str. 120.

[164] Vladimir Vodinelić, „Sloboda medija kao granica zaštite podataka (medijska privilegija)“, *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005, str. 70.

slučaj sa pravnim sistemom Srbije koji garantuje pravo na zaštitu podataka o ličnosti.

Neposredan objekat prava na zaštitu podataka o ličnosti su različita lična dobra. Kako čovek predstavlja kompleksno biće, tako je i krug ličnih dobara čoveka kojima se pruža zaštita širok. Za lična dobra možemo reći da predstavljaju one vrednosti koje su usko povezane sa samom ličnošću čoveka.

U teorijskom smislu, moguće je klasifikovati dve grupe ličnih dobara, u zavisnosti od načina njihovog manifestovanja u spoljnom svetu. U prvu grupu spadaju ona lična dobra koja su sastavni delovi (elementi) ličnosti, dok u drugu grupu spadaju dobra koja su opredmećeni izrazi ličnosti.[165] Lična dobra kao što su život, glas, dostojanstvo, emocije pripadaju prvoj grupi ličnih dobara. Drugu grupu čine dobra poput slika, audio i video zapisa na kojima se nalazi određeno lice, itd.

Podaci o ličnosti predstavljaju lično dobro čoveka koje predstavlja sastavni deo njegove ličnosti. Takve podatke treba razlikovati od oblika na kome ili u kome je manifestovan podatak, kao što je to slučaj sa ličnim dokumentima (lična karta, vozačka dozvola) budući da dokumenti predstavljaju pismena koje sadrže informaciju o određenim podacima građana (nacionalnost, godinu rođenja, i tome slično). Zato se u savremenim zakonodavstvima obično navodi da pojam podataka o ličnosti ne zavisi od nosača, odnosno sredstava preko kojih se ti podaci prikupljaju, obrađuju, objavljuju i prenose.

4.2. Pravo na zaštitu podataka o ličnosti

Razvojem naučnih mogućnosti, digitalne tehnologije i ljudske svesti o potrebi zaštite ličnog života pojedinca, razvila su se i nova ljudska prava. Takav je slučaj i sa pravom na zaštitu podataka o ličnosti koje se razvilo iz prava na privatnost. Razvoj ovog prava prouzrokovan je masovnim korišćenjem interneta i podataka o ličnosti, kao jedne od najvrednijih valuta savremenog poslovnog sveta.

Danas propisi uporednih zakonodavstava uglavnom predviđaju pravo na zaštitu podataka o ličnosti kao posebno pravo. U središtu ovog prava nalaze se podaci građana. Možemo reći da je osnovni zaštitni objekt ovog prava zapravo privatnost građana koja se štiti preko podataka o ličnosti. Naime, podaci o ličnosti sami po sebi nemaju značaj ukoliko nisu povezani sa ljudskom ličnošću, odnosno konkretnim pojedincem. Tek kada se povežu pojedinac i njegovi podaci o ličnosti,

[165] *Ibid.*, 121.

tada se oni mogu koristiti u različite, pa i u protivpravne svrhe, pa se javlja potreba za zaštitom pojedinca i njegove privatnosti.

Značaj podataka o ličnosti i potreba za konkretizacijom brojnih ovlašćenja u vezi sa njihovim korišćenjem i upotrebom, uticali su na formiranje ovog prava, ali i nekoliko posebnih prava koja proističu iz njega.

Pravo na zaštitu podataka o ličnosti sastoji se iz većeg broja ovlašćenja, pa je u tom smislu to kompleksno pravo. Kako Vodinelić navodi: „Pravo na lične podatke predstavlja u osnovi ovlašćenje da čovek odlučuje o davanju i obradi podataka o sebi, nezavisno od stepena poverljivosti tih podataka. Pravo na lične podatke složeno je pravo, sastavljeno iz niza ovlašćenja. Pravo je čoveka da se podaci o njemu ne prikupljaju od drugih nego od njega samog, da se neki podaci ne prikupljaju i ne obrađuju uopšte, da oni koji se obrađuju ne budu dostupni drugima, da zna ko obrađuje podatke o njemu, da traži obaveštenje o tome da li neko obrađuje podatke o njemu, da izvrši uvid, da traži ispravljanje podataka, da traži ažuriranje, da traži upotpunjavanje, da traži obustavu, da traži brisanje, da zna kome se podaci prenose i u koje svrhe“.[166] Dakle, razumevanje pravne prirode prava na zaštitu podataka o ličnosti zahteva razumevanje prava na privatnost, ali i ovlašćenja njihovog imaoca u vezi sa obradom i korišćenjem podataka o ličnosti koje mu garantuje zaštitu od nedozvoljenog zadiranja u ličnu sferu. Zbog toga pojedini autori navode da zaštita podataka o ličnosti predstavlja „dodatnu garanciju nepovredivosti integriteta čoveka.“[167]

U pravnom sistemu Srbije privatna sfera pojedinca zaštićena je kroz pravo na zaštitu podataka o ličnosti. Najvišim opštim pravnim aktom, *Ustavom Republike Srbije* zajamčena je zaštita podataka o ličnosti, a pitanja prikupljanja, držanja, obrade i korišćenje podataka ostavljena su zakonskoj regulativi.[168] Iz ove odredbe proizlazi i mišljenje Ustavnog suda „da se samo zakonom može urediti prikupljanje, držanje, obrada i korišćenje podataka“.[169]

Dalje, Ustavom je *zabranjena i kažnjiva svaka upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni*, u skladu sa zakonom, osim za potreba vođenja krivičnog postupka ili zaštite bezbednosti Srbije. Svakom licu je garantovano *pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti*, u skladu sa zakonom i *pravo da ostvari zaštitu pred sudom zbog zloupotrebe tih podataka*.[170] Ustavni sud se oglasio i povodom ovog pitanja i naglasio da „nije u

[166] V. Vodinelić (2005), str. 69-70.
[167] Ratko Marković, *Ustavno pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2018, str. 475.
[168] Čl. 42, stav 1 i 2 Ustava RS.
[169] Odluka Ustavnog suda Srbije, U. br. 41/10 od 30.05. 2012. god.
[170] Čl. 42, stav 4. Ustava RS.

skladu sa Ustavom zakonom dato ovlašćenje carinskom službeniku da nije dužan da obavesti lice na koje se odnose podaci koje prikuplja za obavljanje poslova iz svoje nadležnosti, ako bi to onemogućilo ili otežalo izvršenje zadatka".[171]

Tumačeći odredbe Ustava možemo zaključiti da podaci o ličnosti predstavljaju suštinski element privatnosti pojedinca. Sva druga lica i organi javne vlasti moraju poštovati podatke o ličnosti i ne smeju ih zloupotrebljavati, odnosno koristiti u svrhe drugačije od onih predviđenih zakonom. Svi instituti i konkretna pitanja od značaja za zaštitu podataka moraju biti uređeni posebnim zakonom, čime se dodatno daje na značaju instituciji podataka o ličnosti.

Uočavamo da je Ustavom svakome zaštićeno pravo na zaštitu podataka o ličnosti, pa je ostalo otvoreno pitanje da li se zaštita podataka, osim fizičkim, garantuje i pravnim licima. Iako bi se u pojedinim elementima mogao braniti stav da i pravna lica treba da uživaju zaštitu podataka o (pravnoj) ličnosti, pri čemu posebno treba imati na umu preduzetnike koji se nalaze u sferi između pravnih i fizičkih lica, osnovnim zakonom u oblasti zaštite podataka otklonjena je svaka dilema i zaštita je dodeljena *isključivo fizičkim licima*.

Poseban zakon koji uređuje institute i pitanja od značaja za zaštitu podataka o ličnosti u Srbiji jeste *Zakon o zaštiti podataka o ličnosti iz 2018***.** godine. Ovim zakonom uređeno je pravo na zaštitu fizičkih lica u vezi sa obradama podataka i slobodnim protokom takvih podataka, načela obrade, prava lica na koje se podaci odnose, obaveze rukovalaca i obrađivača, pravna sredstva, odgovornost i kazne u slučaju povrede prava fizičkih lica u vezi sa obradom njihovih podataka o ličnosti i posebne situacije obrade.[172]

Uočavamo da pravo na zaštitu podataka o ličnosti suštinski predstavlja osnovno i složeno pravo u vezi sa podacima građana, iz koga se granaju posebna prava. Posebnim pravima štite se pojedini aspekti zaštite podataka o ličnosti i omogućava se ostvarivanje posebnih ovlašćenja građana. Na taj način pruža se sveobuhvatna zaštita privatnosti.

U pravu Srbije, kao posebna prava u vezi sa zaštitom podataka o ličnosti izdvajaju se: *pravo na obaveštenost, pravo na pristup, pravo na ispravku, pravo na zaborav, pravo na ograničenje obrade, pravo na prenos, pravo na prigovor i prava u vezi sa automatskom obradom podataka*.

[171] Odluka Ustavnog suda Srbije, U. br. 41/04 od 26.11. 2009. god.
[172] Čl. 1, st. 1 Zakona o zaštiti podataka o ličnosti.

4.3. Posebna prava u vezi sa zaštitom podataka o ličnosti

4.3.1. Pravo na obaveštenost

Načelo transparentnosti postavljeno je kao temelj sistema zaštite podatka o ličnosti. Kao jedan od pojavnih oblika ovog načela javlja se pravo na obaveštenost. Pravo na obaveštenost predstavlja pravom priznatu mogućnost građana da budu upoznati sa svim pitanjima u vezi sa obradom njihovih podataka o ličnosti.[173] Obaveštenost građana predstavlja nužan uslov za preduzimanje drugih (pravnih) radnju, u cilju zaštite privatnosti.

Kada građani ne bi bili obavešteni o postupanju drugih lica u vezi sa njihovim podacima, došlo bi do stvaranja atmosfere tajnosti koja predstavlja suprotnost demokratskim principima i vrednostima.

Pravo na obaveštenost može se posmatrati u širem i užem smislu. U širem smislu, pravo na obaveštenost znači da sva lica imaju pravo da na adekvatan način budu informisana o različitim pitanjima u vezi sa obradom njihovih podataka. Reč je o podacima koja se tiču konkretnog pojedinca, ali i o podacima od šireg društvenog značaja. U tom smislu ilustrativna je odredba Ustava Srbije koja predviđa da svako ima pravo da istinito, potpuno i blagovremeno bude obavešten o pitanjima od javnog značaja i sredstva javnog informisanja su dužna da to pravo poštuju.[174] Dakle, pravo na obaveštenost u širem smislu odnosi se na mogućnost dobijanja svih informacija koje se neposredno i posredno tiču pojedinca. U ovom kontekstu pravo na zaštitu podataka o ličnosti može se dovesti u vezu sa pravom na javno informisanje, odnosno pravom na dobijanje informacija od javnog značaja, kao segmentom prava na obaveštenost.[175]

Sa druge strane, pravo na obaveštenost u užem smislu označava pravo fizičkog lica da bude obavešten o svim obradama u vezi sa podacima koji se odnose na njega. Obim ovog prava ne obuhvata informacije od javnog značaja, već isključivo podatke o ličnosti koji se nalaze u posedu drugog lica – rukovaoca ili obrađivača. Možemo reći da je ovo pravo materijalno-procesne prirode.

U Zakonu o zaštiti podataka o ličnosti predviđeno je pravo na obaveštenost. Zakon ne koristi termin pravo na obaveštenost, već samo određuje

[173] M. Davinić, *Nezavisna kontrolna tela u Republici Srbiji*, Dosije studio, Beograd 2018, str. 51-52.
[174] Čl. 51, st. 1 Ustava RS.
[175] Više o pravu na javno informisanje vid. Jelena Jovičić, „Ustavno regulisanje prava na javno informisanje“, *Zbornik radova pravnog fakulteta u Nišu* (ur. Predrag Dimitrijević), Pravni fakultet Univerziteta u Nišu, Niš 2012, str. 543-552.

krug informacija koje se pružaju licu od koga se prikupljaju podaci o ličnosti.[176] Informacije sadržane u obaveštenju koje se odnose na obradu i podatke moraju biti u konciznom, razumljivom i lako čitljivom obliku, kako se pravo na obaveštenost ne bi tehnički zloupotrebljavalo (duga i komplikovana obaveštenja u kojima nije jasno da je reč o obaveštenju u smislu ovog zakona).

Dok se *konciznost i laka čitljivost* odnose na formu u kojoj se daje informacija, *razumljivost* se odnosi na način prenošenja te informacija. „Zahtev da informacija bude razumljiva znači da ona može biti shvaćena od strane prosečnog člana nameravane grupe. To znači da rukovalac mora prvo da odredi nameravanu publiku i da proceni stepen razumevanja prosečnog člana. Kako se nameravana publika razlikuje od stvarne publike, rukovalac mora uobičajeno da proverava da li je informacija prilagođena pravoj grupi (posebno kada se sastoji od dece) i po potrebi, napravi odgovarajuće izmene.“[177]

Ovo pravo lice može se koristiti od momenta prikupljanja podataka, nezavisno od toga kada je lice steklo saznanje o prikupljenim podacima. Rok za pružanje informacija iznosi 30 dana od dana prijema uredno podnetog zahteva, s tim što je taj rok moguće produžiti na ukupno 90 dana, kada je reč o naročito složenim ili obimnim zahtevima. Zakonom je prepoznat i značaj informaciono-komunikacionih tehnologija u vezi sa ostvarivanjem prava na obaveštenost. Građani mogu biti obavešteni i elektronskim putem o informacijama koje se odnose na njihove podatke i obrade u vezi sa tim podacima, a dozvoljeno je i korišćenje standardizovanih programa (u digitalnom obliku) radi pružanja obaveštenja. Programi moraju biti lako dostupni, koncizni i mašinski čitljivi.[178]

Suština prava na obaveštenost jeste da se od samog početka postupka obrade vodi računa o interesima građana. To se postiže pružanjem informacija o značajnim elementima obrade koje mogu imati uticaja na tok postupka i prava građana.

Važno je napomenuti da rukovalac nema pravo na naknadu za pružanje informacija u vezi sa podacima o ličnosti i njihovom obradom. Međutim, u pojedinim situacijama, rukovalac može da zahteva nužne administrativne troškove postupanja po zahtevu. To se odnosi na slučaj kada je zahtev lica na koji se podaci odnose *očigledno neosnovan ili preteran*, kao i u kada predstavlja zloupotrebu prava, u smislu da se zahtev za obaveštenjem neopravdano učestalo

[176] Čl. 23 Zakona o zaštiti podataka o ličnosti.

[177] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016&679*, no. 17 WP260, str. 7-8.

[178] U Srbiji, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti zadužen je za postupak utvrđivanja standardizovanih ikona. Čl. 21, st. 9 Zakona o zaštiti podatka o ličnosti.

ponavlja. Očigledna neosnovanost zahteva znači da već na prvi pogled, iz opštepoznatih činjenica ili iz činjenica samog zahteva, proizlazi da zahtev treba odbiti. Sa druge strane, preteranost zahteva znači njegovu zloupotrebu u smislu da se odnosi na znatno više podataka nego što je podnosiocu zahteva zaista neophodno za ostvarivanje njegovih prava i sloboda.

Osim što rukovalac može da zahteva naknadu za postupanje po neopravdanim zahtevima, on može i da odbije da postupi po zahtevu. U svakom slučaju, rukovalac je dužan da dokaže očiglednu neosnovanost ili preteranost zahteva i da to obrazloži podnosiocu zahteva.

Kada odbije zahtev ili odbije da postupi po njemu iz nekog razloga, rukovalac ima dodatnu obavezu da obavesti podnosioca o mogućnosti ulaganja pravnog sredstva. U zavisnosti od činjenica konkretnog slučaja, to pravno sredstvo može biti pritužba Povereniku ili tužba nadležnom sudu. Rok u kome se podnosilac zahteva mora obavestiti o odbijanju za postupanje i mogućnosti ulaganja pritužbe ili tužbe iznosi 30 dana od dana prijema zahteva.[179]

U vezi sa načinom ostvarivanja prava na obaveštenost, u sistemu zaštite podataka o ličnosti Srbije *razlikuju se dve situacije*. Razlika između ove dve situacije učinjena je u odnosu na način prikupljanja podataka. *Prvi slučaj* odnosi se na situacije u kojima se podaci o ličnosti prikupljaju od lica na koje se odnose, dok se *drugi slučaj* odnosi na situacije u kojima se podaci o ličnosti ne prikupljaju od lica na koje se odnose, već od nekog drugog lica. Takva razlika uslovljava drugačije pravne posledice i postupanje rukovaoca.

Ukoliko se podaci o ličnosti prikupljaju direktno od lica na koje se odnose, rukovalac, odnosno obrađivač *dužni su da obaveste to lice o određenim elementima obrade*. U trenutku pribavljanja podataka rukovalac ili obrađivač će pružiti informacije koje se odnose na:

1. Identitet i način ostvarivanja kontakta sa rukovaocem, odnosno njegovim predstavnikom ili licem koje je dužno da se stara o zaštiti podataka,
2. Pravni osnov i svrhu radi koje se prikupljaju podaci o ličnosti,
3. Legitimni interes rukovaoca ili treće strane kada se obrada zasniva na tim interesima, a oni pretežu nad interesima ili osnovnim pravima lica na koje se odnose,
4. Primaoce, odnosno fizička lica, pravna lica ili organe vlasti kojima se podaci o ličnosti otkrivaju,

[179] Čl. 21, st. 4, Zakona o zaštiti podataka o ličnosti.

5. Nameru rukovaoca da izvrši prenos podataka u drugu državu ili međunarodnu organizaciju i potvrdu da li je ta država ili međunarodna organizacija sigurni primalac,
6. Rok u kome se čuvaju podaci, odnosno bliže kriterijume njihovog određivanja kada nije moguće odmah ustanoviti rok,
7. Procesna prava koja lice ima u postupku (pravo na pristup, ispravku, brisanje, pravo na prenosivost, pravo na pravna sredstva),
8. Pravo na pravno sredstvo, tj. – pravo da se Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti podnese pritužba,
9. Pravni osnov davanja podataka (ugovor ili zakonska odredba) i eventualne posledice propuštanja nepružanja podataka o ličnosti
10. Mogućnost automatizovanog donošenja odluke, pri čemu se mora naglasiti i metod, odnosno logika funkcionisanja automatizovanog sistema, kao i očekivanim posledicama te obrade.[180]

Dakle, lice čiji se podaci prikupljaju mora biti obavešteno o pomenutim činjenicama već u trenutku pribavljanja podataka. Svako kasnije obaveštavanje stvara rizik po ostvarivanje prava i interesa, pa samim tim predstavlja i povredu zakonske norme. Zbog toga, važno je voditi računa o momentu u kome se prikupljaju podaci, posebno u odnosu na korišćenje informaciono-komunikacionih tehnologija.

Primera radi, građani često nisu ni svesni da se njihovi podaci prikupljaju prilikom pristupa mnogim internet sajtovima. Zbog toga, svi rukovaoci i obrađivači koji poseduju, prave i održavaju internet sajtove trebalo bi da pruže obaveštenje o privatnosti koje je lako uočljivo na svakoj stranici vebsajta. Obaveštenja koja nisu jasno uočljiva zbog prelamanja boja ili prikrivenosti fonta ne mogu se smatrati lako dostupnim. Kod softverskih aplikacija, obaveštenje o privatnosti trebalo bi da bude dostupno već na internet prodavnici, a kada se aplikacija preuzme, obaveštenje o privatnosti nikada ne bi trebalo da bude dalje od „dva klika".[181]

Elementi koje obaveštenje mora da sadrži povećavaju stepen transparentnosti obrade budući da građani dobijaju informaciju o tome ko, na koji način, na osnovu čega i zbog čega prikuplja i obrađuje njihove podatke. Iako su pojedina prava već garantovana samim zakonom, poput prava na pritužbu Povereniku, postoji obaveza rukovaoca ili obrađivača da i o ovim elementima obaveste građane. Razume se, kada je lice na koje se podaci odnose na neki način

[180] Čl. 23 Zakona o zaštiti podataka o ličnosti.

[181] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016&679*, no. 17 WP260, p. 8.

već upoznato sa pojedinim informacijama, rukovalac nema obavezu pružanja tih informacija. Ovde treba podrazumevati konkretno obaveštavanje koje je učinjeno u prethodnoj komunikaciji ili poslovnom odnosu rukovaoca ili ,1obrađivača i lica na koje se podaci odnose, a ne opštu informisanost iz medija ili drugog izvora.

Primera radi, kada je lice u postupku pregovora za zaključenje određenog ugovora obavešteno o rukovaocu, svrsi obrade, pravnom osnovu i roku čuvanja, rukovalac neće biti u obavezi da u obaveštenju navede ove elemente, ali bi trebalo da se pozove na prethodne dokumente u kojima su naznačeni ovi elementi.

Podaci o ličnosti prikupljaju se u svrhu o kojoj lice na koje se podaci odnose mora biti obavešteno. Ipak, u određenim slučajevima, kod rukovaoca može da dođe do promene u pogledu svrhe zbog koje se podaci obrađuju. U tom slučaju, kada postoji namera rukovaoca da obrađuje podatke u svrhu drugačiju od one zbog koje su podaci prvobitno prikupljeni, on mora ponoviti postupak obaveštavanja sa svim pomenutim elementima.

Druga situacija odnosi se na pružanje informacija o obradi kada podaci o ličnosti nisu prikupljeni od lica na koga se podaci odnose, već od nekog drugog lica.[182] Pored informacija koje se pružaju u prvom slučaju, *neophodno je i pružiti obaveštenje i o dodatnim činjenicama*, zbog toga što dolazi do razlikovanja imaoca podataka i izvora od koga su podaci dobijeni.

Rukovalac je dužan da pored informacija koje se pružaju u prvoj situaciji, obavesti lice na koje se podaci odnosi o izvoru iz koga ili od koga potiču podaci o ličnosti i da li ti podaci potiču iz javno dostupnih izvora.

Zakonodavac ostavlja „*razumni rok*“ koji ne može biti duži od 30 dana, da rukovalac obavesti imaoca da su njegovi podaci prikupljeni iz drugog izvora. Ipak, od razumnog roka postavljena su *dva izuzetka. Prvo*, ukoliko se prikupljeni podaci koriste za komunikaciju sa licem na koga se odnose, onda je rukovalac dužan da već tokom prve komunikacije pruži obaveštenje o njihovom prikupljanju. *Drugi izuzetak* se odnosi na situaciju u kojoj dolazi do otkrivanja podataka o ličnosti drugim primaocima, kada se lice na koje se podaci odnose mora obavestiti već prilikom prvog otkrivanja.

Smatramo da postavljanje drugačijih rokova, u odnosu na slučaj kada se podaci prikupljaju od lica na koje se odnose, nije opravdano. Nije uočljiv jasan razlog zbog čega bi se lice na koje se podaci odnose kasnije upoznalo u odnosu na momenat prikupljanja podataka. Ukoliko je rukovalac svestan svoje uloge i obaveza koje ima kao rukovalac, a pri tome iz drugog izvora saznaje za tuđe podatke o ličnosti, nema razloga da se takva informacija „krije“ određeni period od imaoca. Zbog toga *smatramo* da bi normativno trebalo poboljšati pomenuto

[182] Čl. 24 Zakona o zaštiti podataka o ličnosti.

rešenje, pomeranjem momenta pružanja obaveštavanja imaoca odmah nakon momenta prikupljanja podataka iz drugih izvora. Na taj način bi se povećala pravna sigurnost i sprečile moguće zloupotrebe koje mogu nastati u „razumnom roku", čijim se produženjem povećava i rizik od zloupotreba ili povreda podataka.

Kao i u slučaju prikupljanja podataka od lica na koje se odnose, kada postoji namera obrade podataka u druge svrhe, neophodno je ponovo pružiti sve informacije o obradi licu na koga se podaci odnose.

I pored toga što se podaci prikupljaju od lica na koje se ne odnose, u pojedinim situacijama rukovalac *nema dužnost da informiše* lice na koje se podaci odnose o elementima obrade.

Prvo, kada je imalac podataka već upoznat o prikupljanju njegovih podataka od drugog lica.

Drugo, kada pružanje informacija o elementima obrade predstavlja nemoguć zadatak za rukovaoca ili bi takvo obaveštavanje zahtevao nesrazmeran utrošak vremena i sredstava, a posebno u slučaju kada je reč o obradi u cilju arhiviranja u javnom interesu, u svrhe naučnog, istorijskog ili statističkog istraživanja. U ovoj situaciji, rukovalac ima samo obavezu da preduzme odgovarajuće mere zaštite prava i sloboda i legitimnih interesa imaoca podataka, što uključuje i javno objavljivanje informacija.[183]

U modernom svetu koji se zasniva na upotrebi informaciono-komunikacionih tehnologija i interneta teško možemo govoriti o nesrazmernom utrošku vremena i sredstava za obaveštavanje nekog lica. Naravno, i danas postoji opasnost od nemogućnosti pronalaženja kontakt informacija određenog lica i nemogućnost ostvarivanja komunikacije (primera radi preseljenje imaoca u drugu državu ili nepostojanje informacija o njegovom prebivalištu ili boravištu). Stoga, ovaj izuzetak ne sme se koristiti samo pozivanjem na pravne standarde nemogućnosti dostavljanja ili nesrazmernosti utroška vremena i sredstava. Smatramo da se u ovom slučaju mora načiniti i dokumentovati beleška u pogledu elemenata koji opravdavaju pozivanje na pomenute pravne standarde. U suprotnom došlo bi do povrede načela zakonitosti, poštenja i transparentnosti, kao ključnih principa na kojima se zasniva sistema zaštite podataka.

Treće, dužnost obaveštavanja ne postoji i u slučaju kada se prikupljanje ili otkrivanje podataka zasniva na odredbama zakona koje uređuju posebne oblasti, a koje predviđaju odgovarajuće mere zaštite legitimnih interesa lica na koje se podaci odnose. Mogućnost neobaveštavanja može se zasnivati isključivo na zakonu, ne i na aktu niže pravne snage.

[183] Čl. 24, st. 4, tač. 2 Zakona o zaštiti podataka o ličnosti.

Poslednja situacija u kojoj ne postoji dužnost obaveštavanja lica na koje se podaci odnose tiče se situacija u kojima se podaci moraju čuvati u skladu sa profesionalnom tajnom koja je predviđena zakonom. Čuvanje profesionalne tajne obično će se odnositi na delatnosti sveštenika, advokata, zdravstvenih i socijalnih radnika i druga službena lica.[184] *Primera radi*, prema *Zakonu o advokaturi*, advokat je dužan da čuva advokatsku tajnu kao profesionalnu tajnu i da se stara da to čine i zaposlena lica u njegovoj advokatskoj kancelariji.[185] Obaveza čuvanja advokatske tajne nije vremenski ograničena i traje i po prestanku zastupanja. Ove dužnosti službena lica može da oslobodi jedino sud.

4.3.2. Pravo na pristup podacima o ličnosti

Ukoliko pravo na obaveštenost posmatramo kao jednu stranu medalje načela transparentnosti, pravo na pristup podacima možemo posmatrati kao drugu stranu. Kod prava na obaveštenost građani imaju pasivnu ulogu, dok je kod prava na pristup ta uloga aktivna, budući da građani sami (aktivno) deluju u cilju dobijanja informacija o obradi i podacima o ličnosti.

Po svojoj pravnoj prirodi, *pravo na pristup podacima o ličnosti ima određene sličnosti sa pravom na slobodan pristup informacijama od javnog značaja*. Pravo na slobodan pristup informacijama od javnog značaja zasniva se na principu javnosti, koje je suprotstavljeno konceptima tajnosti i zatvorenosti.[186] Naravno, pravo na pristup informacijama od javnog značaja predstavlja drugačiju vrstu prava kojim se omogućava pristup informacijama koje su od značaja za širu društvenu zajednicu, a nalaze se u posedu organa javne vlasti. Mogućnosti dobijanja informacija od javnog značaja „proširuje se sloboda informisanja i upotpunjuje garancija ljudskog prava koja omogućava da građani dođu do informacija od kojih zavisi formiranje i iskazivanje njihove suverene političke volje. To podrazumeva i lakšu kontrolu vlasti i državne uprave.“[187] Kod prava na pristup podacima o ličnosti, građanima se dozvoljava da od rukovaoca ili obrađivača, koji ne mora isključivo da bude organ javne vlasti, zahtevaju

[184] Upor. Branko Peran, Mirko Goreta, Kristina Vukošić, Pojam i vrste tajni, *Zbornik radova* Veleučilišta u Šibeniku, br. 3-4/2015, Šibenik 2015, str. 31.

[185] Čl. 15 i 20 Zakona o advokaturi.

[186] Vladimir Vodinelić, „Pravo na slobodan pristup informacijama od javnog značaja kao ustavno pravo“, u: *Slobodan pristup informacijama – ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Beograd 2004, str. 9.

[187] Miroljub Radojković, „Za slobodan pristup informacijama“, *Prizma,* br. 4/2002, Centar za liberalno-demokratske studije, Beograd 2002, str. 29.

informacije u vezi sa njihovim podacima. Zbog toga, pomenuta prava se razlikuju u odnosu na interes koji teže da zadovolje, kao i u prirodi informacije koja se dobija.

U pravnom sistemu Srbije građani imaju ovlašćenje da zahtevaju informaciju o tome da li rukovalac poseduje pojedine podatke o licu koje ostvaruje pravo na pristup i da li se ti podaci obrađuju. Ukoliko su odgovori potvrdni, lice ima pravo da ostvari pristup svojim podacima i da dobije informacije o pitanjima koja se odnose na obradu. Te informacije se odnose na:

1. *Svrhu obrade,*
2. *Kategorije podataka o ličnosti koje se obrađuju,*
3. *Primaoce ili kategorije primalaca kojima su podaci o ličnosti otkriveni ili će im biti otkriveni, što se odnosi i na prenos podataka stranim državama i međunarodnim organizacijama,*
4. *Rokove u kojima će se podaci o ličnosti čuvati ili kriterijumima za određivanje roka, kada on nije određen propisom,*
5. *Mogućnost korišćenja prava na ispravku brisanje, prigovor ili podnošenje pravnog sredstva nadležnom organu,*
6. *Svaku dostupnu informaciji o izvoru iz koga su dobijeni podaci o ličnosti,*
7. *Mogućnost automatizovanog donošenja odluka, način primene automatizacije i eventualne posledice takve obrade*.[188]

Kada lice zatraži određenu informaciju u vezi sa obradom svojih podataka, rukovalac je dužan da takvu informaciju pruži. Treba obratiti pažnju na činjenicu da lice koje ostvaruje pravo na pristup podacima o ličnosti, *zahtev može uputiti i usmeno*. U takvim situacijama, važno je da rukovalac napravi zapisnik o zahtevu za pristup, jer bi odbijanje prihvatanja usmenog zahteva moglo da predstavlja povredu Zakona o zaštiti podataka o ličnosti. Hipotetički, zahtev može biti upućen i preko društvenih mreža rukovaoca ili obrađivača (*Facebook, Instagram, Linkedin*).[189]

Rukovalac ima dužnost da zahtevane informacije dostavi „na sažet, transparentan, razumljiv i lako dostupan način, korišćenjem jasnih i jednostavnih reči…".[190] Ovakav pristup je od posebnog značaja u vezi sa rukovaocima koji obrađuju podatke u elektronskom obliku zbog mogućnosti nerazumevanja podataka od strane podnosioca zahteva. *Primera radi*, ukoliko su podaci o ličnosti

[188] Čl. 26, st. 1 Zakona o zaštiti podataka o ličnosti.

[189] Za ovo stanovište vid. Nezavisno telo Ujedinjenog Kraljevstva, Pravo na pristup, https:// ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

[190] Čl. 21, st. 1 Zakona o zaštiti podataka o ličnosti.

podnosioca zahteva obeleženi određenim slovima ili brojevima koje koristi organizacija u cilju lakše organizacije rada i obeležavanja pojedinih parametara (U – učestvovao, PZ – podneo zahtev), rukovaoci ili obrađivači imaju dužnost da objasne podnosiocu zahteva značenje nejasnih pojmova, termina, brojeva, itd.

Rukovalac ima dužnost da postupi po zahtevu, osim u slučaju kada treba da zaštiti podatke drugih lica ili kada se ne može utvrditi identitet lica koje zahteva informacije. Takođe, rukovalac može da zahteva dodatne informacije o identitetu lica, kako bi se opravdao interes za podnošenje zahteva. *Primera radi*, kada je pisani zahtev uputio Marko Marković, bez navođenja drugih identifikacionih elemenata poput prebivališta, godine rođenja, odnosa sa kompanijom i dr., treba smatrati da nema dovoljno informacija o identitetu da bi se postupilo po zahtevu.

Posebna situacija se odnosi na prenos podataka u treću državu ili međunarodnu organizaciju. Ukoliko se vrši takav prenos, lice koje zahteva uvid u svoje lične podatke ima pravo da bude obavešteno i o merama zaštite koje se primenjuju u odnosu na međunarodni transfer podataka.[191]

Rok u kome je rukovalac dužan da postupi po zahtevu iznosi 30 dana. Za razliku od pravila upravnog i sudskog postupka, računanje roka počinje da teče od dana prijema zahteva. Rukovalac ima mogućnost da produži rok za dodatnih 60 dana, kada je to neophodno iz razloga složenosti ili brojnosti zahteva. I u ovom slučaju, on mora obavestiti podnosioca zahteva da će produžiti rok.[192] Ukoliko propusti rokove, odnosno ne postupi po zahtevu lica, rukovalac ima dužnost da o razlozima za nepostupanje obavesti podnosioca zahteva, pri čemu mora da ga obavesti i o pravu na podnošenje pritužbe Povereniku, odnosno tužbe sudu.[193] Rukovalac ima pravo da izdavanje kopije podataka i informacija uslovi naknadom nužnih troškova koje ima za izradu kopije. Kako većina građana poseduje informaciono-tehničke uređaje preko kojih se vrši elektronska komunikacija, kopija se može dostaviti i u elektronskom formatu.

[191] Čl. 26, st. 2 Zakona o zaštiti podataka o ličnosti.
[192] Rukovalac mora da obavesti podnosioca zahteva o potrebi produženja roka u roku od 30 dana od dana prijema zahteva.
[193] Čl. 21, st. 4 Zakona o zaštiti podataka o ličnosti.

4.3.3. Pravo na ispravku i dopunu podataka o ličnosti

Podaci o ličnosti koriste se u svakodnevnim društvenim i poslovnim odnosima. Oni se koriste za identifikaciju, ostvarivanje socijalne pomoći, sklapanje ugovora, podnošenje tužbi i pravnih zahteva, pokretanje upravnih postupaka i u mnogim drugim situacijama. Zbog sigurnosti pravnog prometa i poštovanja prava i interesa učesnika u prometu od velike je važnosti da podaci o ličnosti koji se u takvim odnosima koriste budu potpuni i tačni. Zbog toga, potpunost i tačnost podataka o ličnosti ostvaruju se kroz procesno pravo na ispravku i dopunu podataka. Ovo pravo izvire iz načela tačnosti podataka.

Možemo reći da osnove prava na ispravku i dopunu treba tražiti u pravu medija.[194] Sloboda medija i objavljivanja informacija predstavljaju osnove svakog modernog demokratskog društva.[195] Međutim, može se desiti da medijska sloboda dovede do objavljivanja informacija koje nisu tačne i to iz brojnih razloga (pogrešno protumačene činjenice slučaja, potreba za senzacionalističkim izveštavanjem, pogrešno dobijene informacije od izvora, itd.).

Tako je u medijskom pravu formulisano pravo na ispravku ili dopunu netačne informacije. „Pravo na ispravku jeste ovlašćenje lica čiji su pravo ili interes povređeni neistinitom, nepotpunom ili netačno prenetom informacijom da zahteva da se objavi ispravka te informacije kao neistinite, nepotpuno ili netačno prenete.“[196] Ovo posebno pravo štiti fizičko lice od neistinitih i netačnih javnosti dostupnih informacija, koje mogu dovesti do povrede časti i ugleda lica na koga se netačne informacije odnose. Ujedno, ovo pravo ostvaruje i interes javnost da sazna istinite i potpune činjenice o nekom događaju ili pojavi, jer se jedino na taj način mogu ostvarivati mnogi principi na kojima funkcioniše društvo.[197] Na sličan način, potreba za istinitim i potpunim podacima javlja se i u oblasti zaštite podataka o ličnosti. Sigurnost pravnog prometa i ostvarivanje principa zakonitosti zahtevaju tačne i potpune podatke o ličnosti u svim oblastima društvenog života.

---

[194] Više o pojmu medija u cilju razumevanja pojma medijskog prava vid. Jelena Vučković, „Ljudska prava i mediji“, *Zbornik radova Pravnog fakulteta u Nišu*, LV, Niš 2010, str. 163.

[195] Čak se i pravo na zaštitu ličnih podataka ograničava kako bi sloboda medija mogla da se ostvari. Vid. V. Vodinelić (2005), str. 69.

[196] Anđelija Adamović, „Postupak u parnicama za objavljivanje ispravke neistinite, nepotpune ili netačno prenete informacije“, *Zbornik radova Pravnog fakulteta u Nišu LXI* (ur. Milan Petrović), Pravni fakultet u Nišu, Niš 2012, str. 501.

[197] Vladimir Boranijašević, „Postupak u parnicama za objavljivanje ispravke“, *Zbornik radova „Vladavina prava i pravna država u regionu“* (ur. Goran Marković), Pravni fakultet u Istočnom Sarajevu, Istočno Sarajevo 2014, str. 539-540.

Pravo na ispravku i dopunu u oblasti zaštite podataka o ličnosti razlikuje se u odnosu na pravo na ispravku i dopunu informacije iz medijskog prava,[198] budući da je ono prevashodno usmereno na zaštitu javnosti i javnih interesa, a pravo na ispravku iz oblasti podataka o ličnosti štiti privatnost i ličnost pojedinca u njegovim odnosima sa drugim licima.

Pravo na ispravku i pravo na dopunu predstavljaju posebna procesna prava građana koja im omogućavaju korišćenje tačnih i potpunih podataka u pravnom prometu. Na taj način, štite se podaci građana i njihovi privatni interesi, ali i pravni poredak, budući da se svim učesnicima pravnog prometa pruža sigurnost i pouzdanost u pravnom promet. Skrećemo pažnju na to da je druga strana ovog prava dužnost rukovaoca da u odgovarajućim vremenskim intervalima proveri tačnost podataka o ličnosti koje obrađuje.

Suštinski posmatrano, pravo na ispravku i dopunu sastoji se iz dva posebna prava, prava na ispravku i prava na dopunu. Naravno, oba prava teže istovetnoj svrsi – istinitim i potpunim činjenicama u pravnim odnosima. Zbog toga se obično pojavljuju zajedno, u jedinstvenom obliku. Teorijski, između pomenutih prava postoji razlika, pa ćemo analizirati svako pravo zasebno. Skrećemo pažnju da su rokovi za ostvarivanje ovog prava i način postupanja rukovaoca identični kao i kod prava na pristup podacima o ličnosti.

Pravo na ispravku zasniva se na tome da svako fizičko lice ima pravo da zahteva ispravku pogrešnog ili netačnog podatka o ličnosti. Ispravka se zahteva od lica koje čuva i koristi podatke, dakle od rukovaoca ili obrađivača. O greškama u vezi sa podacima o ličnosti možemo govoriti kada se u konkretnom slučaju ne radi o podatku koji činjenično postoji (u stvarnosti), već je reč o nekom drugom koji ne odgovara činjenicama konkretnog slučaja. Naravno, kada lice podnese zahtev za ispravku, ono mora da priloži i dokaze (ukoliko se do njih ne može doći javnim pristupom) u vezi sa činjenicama koje govore o tome kako i na koji način treba izmeniti podatke.

Primera radi, umesto Republike Srbije, kao države rođenja, stoji Beograd (grad), te se radi o pogrešnom podatku, budući da je informacija pogrešna, jer se država i grad razlikuju po svojoj prirodi. Kako se ovi podaci koriste u ličnim kartama, pa mogu predstavljati podatke o ličnosti zbog identifikacije, postoji i interes lica na koga se podatak odnosi da zahteva njegovu ispravku od policijske uprave, koja je rukovalac ovih podataka.

[198] Više o pravu na odgovor i ispravku iz medijskog prava, vid. Jovica Trkulja, „Deficiti medijskog zakonodavstva u Srbiji“, *Zbornik radova Pravnog fakulteta u Nišu*, LXI (ur. Milan Petrović), Niš 2012, str. 11.

Netačnost podataka može se javiti u još jednoj situaciji. To je slučaj kada nije netačan ceo podatak o ličnosti, koji u većini odgovara stvarnim činjenicama, ali neki od njegovih elemenata nije pravilan, odnosno nije tačan, pa ga treba ispraviti. *Na primer*, umesto datuma rođenja 01.01.1992. unet je datum rođenja 01.02.1992. U ovom slučaju, radi se o podatku (godini rođene), kod kojih su pojedini elementi netačni, pa treba pristupiti njihovoj ispravci, kako bi podataka u celosti odgovarao stvarnom stanju.

U specifičnim situacijama i pored netačnosti podatka, ne treba prihvatiti zahtev za njegovim brisanjem, budući da on može da bude od koristi za ostvarivanje nekog drugog prava ili interesa lica. *Primera radi*, ako u medicinskoj dokumentaciji pacijenta stoji podatak o tome da je pokušano lečenje određene dijagnoze, za koju se u kasnijem postupku lečenja utvrdi da nije tačna, podatke o ranijoj dijagnozi ne bi trebalo brisati, jer su oni pomogli otkrivanju tačne dijagnoze ili pomažu u traženju tačne.

Građani imaju pravo da zahtevaju i dopunu podataka o ličnosti koji su kod drugih lica koja ih obrađuju. To se dešava u slučajevima kada je posle prikupljanja podataka, naknadno, došlo do određene promene u ličnom statusu građana ili pojedinim elementima podataka o ličnosti, ali ta promena nije zavedena u podacima o ličnosti koji se koriste. *Na primer*, nakon venčanja žena je svom prezimenu dodala muževljevo prezime, ali u određenom ličnom dokumentu stoji samo ženino devojačko prezime (kao podatak o ličnosti). U odnosu na ovaj podatak, žena ima pravo da traži promenu prezimena u evidenciji, kako bi podatak o ličnosti (o njenom prezimenu) bio upotpunjen i usklađen sa stanjem u praksi. U ovakvim situacijama, građani imaju pravo da zahtevaju da se unese promena, a to mogu učini i davanjem dopunske izjave.[199]

4.3.4. Pravo na brisanje podataka o ličnosti (pravo na zaborav)

Uobičajeni „životni tok“ podatka kod rukovaoca završava se ispunjenjem svrhe zbog koje je prikupljen. Kako se rukovaoci koriste velikim brojem podataka, može se javiti situacija da se nastavi sa čuvanjem i korišćenjem podataka iako je ispunjenja svrhe obrade. Kako podaci o ličnosti predstavljaju lično dobro građana, njima se mora dati mogućnost da spreče bespredmetne obrade. Značajnu ulogu u tom pogledu ima pravo na zaborav. Pravo na zaborav u pravu Srbije poznato je pod nazivom pravo na brisanje podataka o ličnosti.

[199] Čl. 29 Zakona o zaštiti ličnih podataka.

Pravo na zaborav predstavlja jedno od osnovnih prava u vezi sa zaštitom podataka o ličnosti u modernom dobu. U svetu informaciono-komunikacionih tehnologija kada jedan podatak uđe u digitalni etar, teško ga je potpuno izbrisati. Imajući u vidu ogroman broj korisnika interneta, potrebno je zaštiti građane od nezakonite obrade podataka, kada više ne postoji potreba da se koriste od strane drugog lica. To znači da se pravo na zaborav zasniva na težnji da građani ne trpe posledice zbog korišćenja i upotrebe podataka u prošlosti. Ovo pravo predstavlja svojevrsno ostvarenje načela tačnosti podataka u situaciji kada određeni podatak više nije potreban, pa ga treba izbrisati, odnosno „zaboraviti".

U teoriji se navodi da je pravo na zaborav šire pravo koje se sastoji iz više elemenata. Prvi element se odnosi na *krivično-pravni aspekt*, odnosno na zaborav podataka o učinjenim prestupima, prekršajima, krivičnim delima i osuđujućim presudama. Drugi element se odnosi na zaborav podataka o ličnosti koji su *u posedu drugih lica*, dok se treći element odnosi na pravo *„digitalnog zaborava"*, sa ciljem da se izbrišu informacije i podaci plasirani na društvenim mrežama i internetu.[200]

Institut rehabilitacije iz krivičnog prava funkcionalno je sličan pravu na zaborav. Rehabilitacijom se briše osuda i prestaju sve njene pravne posledice, a osuđeni se smatra neosuđivanim.[201] Na sličan način deluje i pravo na zaborav, koje omogućava da se obrišu svi podaci koje se nalaze kod drugog i da se to lice „zaboravi" u istoriji onog ko je obrađivao podatke. Ipak, osnovna intencija prava na zaborav usmerena je na zaštitu pojedinca. Rehabilitacijom se štite širi društveni interesi, kao što su normalno funkcionisanje društvene zajednice i povratak kažnjenih lica u normalne društvene tokove.

Pravo na zaborav izaziva i druge polemike u teoriji. Sporno je koji su tačno elementi ovog prava, da li je adekvatan naziv, iz kog pravnog instituta potiče, itd. Pojedini autori prave razliku između „prava na brisanje" i „prava na zaborav".[202] Takođe, javljaju se dve grupe mišljenja u odnosu na pitanje pravne prirode „prava na zaborav". Jedni smatraju da pravo na zaborav predstavlja

[200] Cécile de Terwangne, „Internet Privacy and the Right to Be Forgotten/Right to Oblivion", Monograph "VII International Conference on Internet, Law & Politics- Net Neutrality and other challenges for the future of the Internet", *Revista de internet, derecho y politica,* Universitat Oberta de Catalunya, Barcelona 2012, p. 109.

[201] Čl. 97 Krivičnog zakonika Srbije, „Sl. glasnik RS", br. 85/2005, 94/2016.

[202] Više o razlici između „prava na zaborav" i prava na brisanje" vid. Meg Leta Ambrose, Jef Ausloos, „The Right to Be Forgotten Across the Pond", *Journal of Information Policy,* vol. 3, Pennsylvania State University Press, Penssylvania 2013, p. 14-16.

pojavni oblik prava na privatnost.[203] U skladu sa takvim stanovištem, pravo na zaborav pomaže u zaštiti privatnosti lica čiji su podaci o ličnosti objavljeni. Drugi smatraju da pravo na zaborav *potiče iz prava na čast i ugled*.[204] Ovo stanovište objašnjava se time da svako ima pravo na čast i ugled, te da objavljene informacije koje nisu tačne vređaju čast i ugled lica i moraju biti izbrisane, odnosno zaboravljene.

Nezavisno od teorijskih razmatranja, možemo reći da „pravo na zaborav" predstavlja jedno od nosećih stubova sistema zaštite podataka o ličnosti. Ljudi se koriste velikim brojem podataka o ličnosti koje upotrebljavaju za učestvovanje na društvenim mrežama, forumima i internet sajtovima. U takvom „moru informacija" teško je odrediti koje su informacije tačne, ažurne i zakonito upotrebljene, pa građanima treba omogućiti da spreče nezakonite i nepravilne obrade podataka koji drugim licima nisu potrebni.

Iako pravo na zaborav deluje kao prirodni deo sistema zaštite podataka, potreba za ovim pravom i uspostavljanjem u uporedno-pravnim zakonodavstvima, iskristalisala se zahvaljujući sudskoj praksi, a posebno odluci Suda pravde EU poznatoj pod nazivom *Google v. Costeja.* Ova odluka uticala je na to da pravo na zaborav nađe svoje mesto u uporedno-pravnim propisima koji uređuju zaštitu podataka.

Pravo na brisanje podataka o ličnosti ostvaruje se putem zahteva rukovaocu da obriše podatke koje poseduje o podnosiocu zahteva.[205] Dakle, neophodna je aktivna uloga lica na koje se podaci odnose. Kako bi se omogućila efikasna primena ovog prava, rukovalac je dužan obriše podatke „bez nepotrebnog odlaganja". Pravni standard „nepotrebnog odlaganja" znači da je rukovalac dužan da obriše podatke odmah nakon prijema zahteva, uz uvažavanje drugih obaveza, što znači da ima na raspolaganju određeni period vremena u kome može izvršiti preče aktivnosti u vezi sa podacima. Svakako, ovaj period se ne sme zloupotrebljavati.

Rukovalac će obrisati lične podatke samo u određenim slučajevima.

---

[203] Antoon De Baets, „A historian's view on the right to be forgotten", *International Review of Law, Computers & Technology*, Vol. 30, Nos. 1-2, Routledge- Taylor & Francis group, online 2016, p. 57.

[204] Jeffrey Abramson, „Searching for Reputation: Reconciling Free Speech and the „Right to be Forgotten"", *North Carolina Journal of Law & Technology*, vol. 17, issue 1, online 2015, p. 47.

[205] Pojedini autori smatraju da ovom pravu nedostaje automatsko brisanje podataka nakon izvesnog perioda, na šta treba da sugeriše formulacija „prava na zaborav". Više o tome vid. Nicolai Culik, Christian Döpke, „About Forgetting and Being Forgotten", u *Big Data in Context- Legal, Social and Technological Insights,* (eds. Thomas Hoeren, Barbara Kolany-Raiser), Springer, online 2018, p. 23-24.

Prvo, lice na koje se podaci odnose ima pravo da zahteva brisanje podataka koji se nalaze kod rukovaoca, a *više nisu neophodni za ostvarivanje svrhe zbog koje su prikupljeni*. Podaci se uvek prikupljaju u konkretnu svrhu i ne mogu se koristiti u druge svrhe, osim u slučaju zakonom propisanih situacija. To znači da kada je ispunjena svrha zbog koje su podaci prikupljeni, otpada i pravni osnov njihovog čuvanja kod rukovaoca, pa samim tim ne postoji ni potreba za daljim čuvanjem.

Primera radi, nakon zaključenja ugovora između lica na koje se podaci odnose i rukovaoca, ugovor je u potpunosti ispunjen, pri čemu ta lica nisu u stalnom poslovnom odnosu, pa više ne postoji razlog čuvanja podataka. Podrazumeva se, ova odredba može doći u koliziju sa drugim institutima i odredbama posebnih zakona koje obavezuju rukovaoca (primera radi- obaveza čuvanja ugovora), u kom slučaju se čuvanje podataka vezuje za neku drugu zakonsku obavezu. *Drugi primer* kada podaci više nisu neophodno za ostvarivanje svrhe zbog koje su prikupljeni jeste kada jedno fizičko lice pređe sa korišćenja usluga jednog mobilnog operatera kod drugog, tada bivši operater više nema pravo da zadržava podatke o ličnosti bivšeg klijenta.

Druga situacija u kojoj se može tražiti ostvarivanje prava na brisanje podataka, jeste kada je *lice na koje se podaci odnose opozvalo pristanak na osnovu koga je obrada izvršena*, pri čemu ne postoji drugi pravni osnov koji opravdava obradu. Pristanak predstavlja „labilan“ pravni osnov, pa ga samim tim treba izbegavati u praksi, budući da traje samo do opoziva lica na koje se odnose podaci, što se može desiti u svakom trenutku. Jasno je, kada se obrada podataka o ličnosti zasnivala na ovom pravnom osnovu, njen status traje dok traje i punovažan pristanak.

Treće, *pravo na prigovor* u vezi sa obradom podataka o ličnosti može prouzrokovati brisanje tih podataka. Naime, lice na koje se podaci odnose može u svakom trenutku podneti prigovor na obradu njegovih podataka o ličnosti, pri čemu je rukovalac dužan da prekine sa obradom. U samom prigovoru na obradu, može se podneti i zahtev za brisanjem podataka.

Četvrto, *nezakonita obrada podataka* stvara osnov za njihovo brisanje. Ni jedan podataka o ličnosti ne sme se obrađivati suprotno zakonskim normama. U slučaju da dođe do nezakonite obrade ili makar ukoliko lice na koje se podaci odnose smatra obradu nezakonitom, podaci se moraju zaštiti, makar i naknadno, njihovim brisanjem.

Peta situacija koja stvara dužnost da se podaci brišu, javlja se *u slučaju potrebe za izvršenjem neke od zakonskih obaveza rukovaoca*. Ova obaveza može se zasnivati na odredbama posebnih zakona. To će biti čest slučaj u vezi sa

podacima koje čuvaju i obrađuju organi uprave, budući da zakonskih osnova za čuvanje podataka o građanima ima više, kao što je slučaj sa jedinstvenim matičnim brojem građana, mestom prebivališta i boravišta, itd.

Šesto, podaci o ličnosti se moraju obrisati ukoliko su *prikupljeni u vezi sa uslugama informacionog društva koje su ponuđene deci*. Deca predstavljaju kategoriju koja uživaju posebnu zaštitu u vezi sa podacima, pa se država preventivno stara o njihovoj privatnosti. To znači da kada maloletno lice koje je navršilo 15 godina života i samostalno dalo pristanak na kupovinu određenog proizvoda putem interneta, rukovalac, odnosno prodavac takvog proizvoda ima obavezu da obriše lične podatke kupca, kako se oni ne bi zloupotrebljavali.

Međutim i u ovim slučajevima javljaju se izuzeci, pa podaci o ličnosti neće biti obrisani u onom delu u kome su neophodni za ostvarivanje slobode izražavanja i informisanja. To će biti slučaj u oblasti medija, koji u pojedinim situacijama moraju koristiti podatke o ličnosti kako bi mogli da obavljaju svoj rad. Poštovanje zakonske obaveze rukovaoca kojom se zahteva obrada ili izvršenje poslova u javnom interesu ili izvršenje službenih ovlašćenja rukovaoca predstavlja izuzetak od prava na brisanje podataka o ličnosti. Ove situacije treba tražiti u posebnim zakonima. Takođe, ostvarivanje javnog interesa u oblasti javnog zdravlja, arhiviranje u javnom interesu, naučno ili istorijsko istraživanje predstavlja razlog zbog koga se u određenoj meri podaci ne brišu. Ista je situacija i sa slučajem potrebe podataka za podnošenje, ostvarivanje ili odbranu od pravnog zahteva rukovaoca.[206]

4.3.5. Pravo na ograničenje obrade

Načelo ograničenja svrhe obrade ima svoj pojavni oblik u pravu kojim se ograničava obrada podataka o ličnosti. Pravo na ograničenje obrade je samostalno pravo koje pomaže ostvarivanju pravne sigurnosti kada nije izvesno da će obrada podataka biti zakonita u budućem periodu. Lice na koje se podaci odnose može zahtevati od rukovaoca da ograniči obradu podataka o ličnosti u nekom od sledećih slučajeva:

1. *Kada lice na koje se podaci odnose osporava tačnost podataka koji se obrađuju (u ovom slučaju obrada se može ograničiti u onom periodu koji je neophodan organu da ispita tačnost navoda i tačnost podataka),*

[206] Čl. 30, st. 5 Zakona o zaštiti podataka o ličnosti.

2. *Ukoliko je obrada nezakonita, ali lice na koje se podaci odnose ne traži brisanje tih podataka, već traži ograničenje njihove upotrebe (radi zadovoljenja njegovih ličnih interesa),*
3. *Kada više ne postoji svrha radi koje su se podaci obrađivali, ali ih lice na koje se podaci odnose zahteva, radi ostvarivanja nekog drugog interesa (radi podnošenja ili odbrane od pravnog zahteva u drugom upravnom ili sudskom postupku),*
4. *Lice na koje se podaci odnose je uložilo prigovor na obradu podataka, u kom slučaju organ ima obavezu da prekine sa obradom, osim ako predoči da postoje legitimni osnovi za obradu koji pretežu nad interesima lica čiji se podaci obrađuju. U ovom slučaju obrada se ograničava do konačne ocene po pitanju da li pravni osnov rukovaoca preteže nad privatnim interesom lica čiji su podaci.*[207]

U vezi sa ovim pravom javlja se obaveza rukovaoca da obavesti lice na koje se podaci odnose o prestanku dejstva prava na ograničenje obrade. Kako je ovo pravo privremenog karaktera, organ mora uputiti obaveštenje pre nego što ustanovljena ograničenja prestanu da važe.

Skrećemo pažnju odluku upravnog suda na teritoriji EU, Upravnog suda Stade (pokrajina Donja Saksonija, Nemačka),[208] koja se tiče osporavanja tačnosti podataka (prva grupa situacija u kojima se može ograničiti obrada podataka). U konkretnom slučaju, lice koje je podnelo zahtev za ograničenje obrade bio je podnosilac zahteva za azil. On je tvrdio da podaci koji se obrađuju o njemu nisu tačni (podnosilac je tvrdio da potiče iz države Sijera Leone, a ne iz države Gvineje), pa je zahtevao ograničenje obrade podataka. Sud je utvrdio da ova situacija kod podnosioca zahteva ne postoji, budući da je on trebalo da „ospori" tačnost podataka, a to u konkretnom slučaju nije učinjeno. Naime, osporavanje podrazumeva obrazloženje podnosioca o netačnosti podataka koje je potkrepljeno dokazima, što kod podnosioca zahteva nije bio slučaj. Podnosilac je naveo samo da ima poreklo države Sijera Leone i da je rezervni pasoš Gvineje protivpravno stekao. Na osnovu toga, Sud je odbio zahtev i utvrdio važnu praksu za organe uprave koji nemaju dužnost da prihvate zahtev za ograničenje obrade, ukoliko zahtev nije obrazložen i potkrepljen dokazima.[209]

[207] Čl. 18, st. 1 Zakona o zaštiti podataka o ličnosti.
[208] Upravni sud Stade, Odluka br. Az. 1 B 1918/18, od 09.10.2018. god.
[209] Za više o činjeničnim elementima ovog slučaja vid. Kanzlei Bahr, *Kein Recht auf Einschränkung der Datenverarbeitung nach Art. 18*, DSGVO, online 2018, *https://www.datenschutz.eu /urteile/ Kein - Recht - auf - Einschraenkung - der - Datenverarbeitung -nach - Art -18 - DSGVO-Verwaltungsgericht-Stade-20181009/#.*

U svakom slučaju, kada je podnet zahtev za ostvarenje prava na ograničenje obrade, podaci se mogu obrađivati (u ograničenom obimu), ali samo ukoliko postoji pristanak lica na koga se odnose. Takođe, podaci se mogu obrađivati i ukoliko to nalažu interesi zaštite prava drugih lica, kao i u slučaju zaštite „značajnih javnih interesa". Dakle, interesi moraju biti od šireg značaja za društvenu ili državnu organizaciju, što rukovalac posebno mora obrazložiti i opravdati.

4.3.6. Pravo na prenosivost podataka

Brza komunikacija i mogućnost prenosa velike količine podataka predstavljaju „zaštitnik znak" modernog digitalnog društva. Građani među sobom, sa kompanijama i organima vlasti svakodnevno razmenjuju velike količine podataka. U određenom broju slučajeva javlja se potreba za brzim prenosom podataka od jednog lica do drugog. Prilikom prelaska sa jednog proizvoda na drugi, odnosno sa jedne usluge koja se na tržištu nudi na drugu, građani imaju potrebu da njihovi podaci o ličnosti koji su potrebni prate takve „tržišne transfere". Kako bi se izbegli dodatni troškovi njihovog prenosa u vidu vremena i novca građana i fizičkog prenosa podataka, u modernim pravima stvara se mogućnost za prenosom bez učešća građana. Takva mogućnost formulisana je u pravu na prenosivost podataka. Pravo na prenosivost podataka omogućava i ostvarivanje širih društvenih interesa, kao što su brži ekonomski razvoj, podsticanje konkurencije i umrežavanje podataka sa drugim granama prava (kompanijskim pravom, intelektualnom svojinom, potrošačkim pravom, itd.).[210]

Osnovni cilj ovog prava jeste da pruži dodatne mogućnosti građanima u kontroli nad svojim podacima koji se nalaze kod drugih lica. Zbog toga je uvođenje ovog prava u pravni sistem značajno. „Zakonodavcu je na umu bilo stvaranje okruženja u kojem bi ispitanici mogli nesmetano seliti svoje podatke sa usluge na uslugu, bez obaveze da nastave koristiti lošiju uslugu samo zato što im se tamo nalaze podaci. Trenutno je situacija takva da se korisnici teško odvažuju na promjenu računa, e-pošte, kalendara i sličnih aplikacija zbog podataka koji se tamo nalaze. Cilj prenosivosti podataka jest doskočiti tom problemu…"[211]

---

[210] Paul De Hert, *et al*, „The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer law & security review* (ed. Steve Saxby), Amsterdam – Boston – London 2018, p. 194.

[211] GDPR Informer, Službene smjernice o prenosivosti podataka, online 2018, *https://gdprinformer.com/hr/gdpr-clanci/sluzbene-smjernice-o-prenosivosti-podataka.*

Suština ovog prava može se razložiti na dva posebna ovlašćenja. Prvo ovlašćenje omogućava licu da dobije svoje podatke od rukovaoca koji ih je obrađivao. U ostvarivanju ovog prava nije važan način čuvanja podataka (u digitalnom ili fizičkom obliku). U odnosu na ovo ovlašćenje, pravo na prenosivost podataka približava se pravu na pristup podacima. Drugo ovlašćenje odnosi se na mogućnost građana da zahteva od rukovaoca da njegove podatke o ličnosti neposredno prosledi (transferiše) drugom rukovaocu.[212] Pravu na prenosivost podataka korespondira obaveza rukovaoca da dostavi podatke drugom, izabranom rukovaocu u „struktuiranom, uobičajenom i mašinski (elektronski) čitljivom formatu". To znači da podaci moraju biti uobličeni u formatu koji dozvoljava lako snalaženje, koji se obično koristi u pravnom prometu i koji može biti računarski obrađen.

Primena ovog prava zavisi od *dva uslova*. *Prvi* se odnosi na slučaj kada se obrada podataka vrši na osnovu pristanka lica, dok se *drugi* tiče automatske obrade podataka. U ovim slučajevima, mogu da se prenesu samo određeni podaci, što se može ustanoviti sa licem koje zahteva prenos. Anonimni podaci ne spadaju u obim ovog prava.[213]

Naravno, ovo pravo se ne sme vršiti maliciozno, već mora biti u saglasnosti sa pravima i interesima drugih lica. Kada postoje podaci koji se tiču više lica, rukovalac ima dužnost da prenese sve podatke, ali novi rukovalac nema pravo da obrađuje podatke drugih lica, već samo onog lica na koga se prenos odnosi. Kako se navodi „ne postoji obaveza finansijske institucije da odgovore na zahtev za prenos podataka o ličnosti kao deo njihove obaveze na prenos, kada to može dovesti do povrede njihove obaveze sprečavanja pranja novca ili drugih finansijskih zločina".[214]

Primer za situaciju u kojoj je moguće da dođe do ostvarivanja prava na prenosivost tiče se promene mobilnog operatera čije usluge koriste fizička lica. U slučaju bolje ponude ili nekog drugog razloga, građanin se može opredeliti da promeni operatera, uz primenu prava na prenosivost, budući da je dovoljno da operateri izvrše razmenu podataka, a ne da se sam klijent, odnosno lice na koga se podaci odnose, angažuje oko takvog prenosa.

Rukovalac je dužan da postupi po zahtevu za prenos podataka u roku od 30 dana od prijema zahteva, sa mogućnošću produženja roka na ukupno 90 dana kada postoje činjenice koje zahtevaju takvo produženje – složenost i broj zahteva.

---

[212] Čl. 36, st. 1 Zakona o zaštiti podataka o ličnosti.

[213] Article 29 Data Protection Working Party, *Guidlines on the right to data portability*, 16/EN WP 242 rev.01, online 2017, 9, *file:///C:/Users/Win/Downloads/wp242_rev01_enpdf.pdf*.

[214] *Ibid*., 8.

Pored toga, rukovalac ima dužnost da pruži pomoć licu na koga se podaci odnose, budući da je reč o novom pravu, koje nije svima poznato, pa ni jasno. Kada je reč o očigledno neosnovanim i preteranim zahtevima, rukovalac ima pravo da naplati nužne troškove postupanja po zahtevu, pa čak i da odbije da postupi po zahtevu, ali u ovim situacijama na njemu leži teret dokazivanja potrebe naknade troškova. Kao i kod drugih posebnih prava, kada ne postupi po zahtevu lica na koga se podaci odnose, rukovalac treba da pruži obaveštenje o mogućnostima ostvarivanja pravne zaštite pred Poverenikom ili sudom.

4.3.7. Prava u vezi sa automatskom obradom podataka o ličnosti

Razvoj modernih tehnologija doveo je do napretka automatizacije, odnosno „samostalnog" rada računara. Automatizovani sistemi funkcionišu na osnovu prethodno postavljenih pravila i ulaznih parametara, u okviru kojih je program sposoban da samostalno, analizom unetih elemenata i sopstvenom logikom, dođe do predviđanja određene situacije ili pojave.

Računarski programi, koji automatskim putem dolaze do predviđanja rezultata, pokazali su se kao korisno sredstvo u donošenju različitih poslovnih odluka, saniranju ekonomskih gubitaka i u procesu odlučivanja u svakodnevnim stvarima. Takvo odlučivanje pomaže oko izbora najkraćeg puta do cilja, obaveštavanja o promenama na berzi, promenama vremenskih prilika, izboru najpovoljnije ponude na tržištu i tome slično. Zbog toga, automatsko donošenje odluka nalazi svoje mesto u oblasti finansija, medicine, obrazovanja, sporta, turizma i mnogim drugim.

Ilustracije radi, automatizovana odluka bila bi u slučaju programa koji – na osnovu prethodnog života lica, broja učinjenih prestupa i prekršaja, ranije osuđivanosti, ličnih prilika u kojima to lice živi, porodice i drugih faktora, – ustanovi da nije opravdano pustiti konkretno lice na uslovni otpust u slučaju izdržavanje kazne zatvora. To je čisto automatska odluka, koja je zasnovana na obradi podataka o ličnosti i doneta na osnovu prethodno postavljenih pravila. Automatsko donošenje odluka bazira se na podacima koji služe kao polazni elementi na osnovu kojih se vrši analiza i donose odluke. Zbog toga, uvođenje ovih tehnologija može ugroziti privatnost građana. Takođe, ako se postave pogrešni polazni parametri, moguće je da se donese i pogrešna odluka. *Primera radi*, lice ne bude pušteno na uslovni otpust iz zatvora, iako bi trebalo primeniti taj institut zbog dobrog vladanja.

Računarski programi funkcionišu na bazi ustanovljenih algoritama bez ulaženja u dublji društveni kontekst konkretnog slučaja, što eliminiše iz takvog odlučivanja moralnu i emotivnu komponentu. *Primera radi*, može se dogoditi da računarski programi nemaju u vidu celokupnu društvenu situaciju građana, pa rezultati mogu dovesti do neopravdanih podela među ljudima, odnosno diskriminacije, „etiketiranja" lica i tome slično. Zato je važno ustanoviti pravo građana da se zaštite od „računara", odnosno od potpuno automatski donetih odluka.

Kako bi zaštitili građane od neželjenih posledica automatskih odluka računarskih programa, sistemi zaštite podataka priznaju građanima posebno pravo u vezi sa takvim načinom donošenjem odluka. Takav je slučaj i sa pravnim sistemom Srbije u kome je garantovano pravo lica da odluči o tome da li će se na njega primenjivati odluka koja je donesena isključivo na osnovu automatske obrade podataka o ličnosti, dakle od one obrade koju je uradio računarski program. Odluka mora imati određeni pravni značaj, pa se imaju u vidu samo one odluke koje proizvode pravne posledice ili koje značajno utiču na prava i interese određenog fizičkog lica.

Osim automatske obrade podataka, građani imaju pravo da odluče da li će se na njih primenjivati i odluke koje se zasnivaju na „*profilisanju*". Profilisanje se određuje kao način automatske obrade podataka koji koristi podatke *radi predviđanja i razumevanja pojedinih ličnih aspekata života i navika određenog lica*, a posebno u vezi sa predviđanjem kvaliteta ličnih i profesionalnih sposobnosti, finansijskom situacijom, zdravstvenim stanjem, afinitetima i drugim karakteristikama koje govore više o samom profilu (ličnosti) određenog lica.

Kako se navodi u *Smernicama o automatizovanom donošenju pojedinačnih odluka i izrade profila Radne grupe člana 29*: „Izricanje novčanih kazni za prebrzu vožnju na temelju dokaza prikupljenih kamerama za merenje brzine predstavlja postupak automatizovanog donošenja odluka koji ne uključuje nužno i izradu profila. Međutim, to bi se pretvorilo u donošenje odluka na temelju izrade profila ako bi se ponašanje pojedinaca u vožnji pratilo tokom vremena, na primer, ako bi iznos izrečene novčane kazne proizlazio iz procene koja uključuje druge činjenice, da li je prekoračenje dopuštene brzine ponovljeni prekršaj ili je vozač u poslednje vreme učinio druge prekršaje u saobraćaju."[215]

Kao primer za odlučivanje na osnovu profilisanja i automatske obrade podataka možemo navesti računarske programe u zdravstvu, kao važnom

[215] Radna grupa člana 29, *Smernice o automatizovanom donošenju pojedinačnih odluka i izradi profila za potrebe Uredbe 2016/679*, 17/HR, WP251REV.01, 2018, https://azop.hr /images/ dokumenti/217/wp251rev01_hr.pdf.

segmentu javnog sektora. Računarski programi u zdravstvu mogu svrstati određeno lice u kategoriju lica koja je najpodložnija srčanim bolestima. Ovo profilisanje ne znači da lice već boluje ili će bolovati od pomenutih oboljenja. Zato, lice može dati izjavu kojom prihvata automatsku obradu podataka o ličnosti, zasnovanu na prethodno postavljenim zdravstvenim parametrima.[216]

Lice čiji se podaci koriste u automatskoj obradi podataka mora imati mogućnost da iznese svoj stav u vezi sa konkretnom odlukom (ukoliko je to potrebno), kao i da uloži pravna sredstva ukoliko smatra da odluka nije pravilna ili zakonita. Sa druge strane, rukovalac mora preduzeti adekvatne mere da bi zaštitio prava i interese lica čiji se podaci koriste kod automatske obrade podataka. On će to činiti uključivanjem ljudskog faktora u kontrolu procesa automatizovane obrade i revizijom donetih odluka (zaključaka) računara, od strane nadležnog lica. Zaštitne mere zahtevaju i da se izbegne neopravdano pravljenje razlike između ljudi, odnosno da ne dođe do diskriminativnih odluka.

Zahvaljujući ovom pravu građani imaju mogućnost da samostalno odlučuju o tome da li će poveriti odlučivanje o ličnim pitanjima računarskim programima.[217] Na taj način ostvaruju se osnovni principi zaštite podataka o ličnosti kao što su transparentnost, zakonitost obrade, zaštita legitimnih interesa lica čiji se podaci obrađuju, itd.

Podrazumeva se, dužnost je rukovaoca da prilikom primene automatizovane obrade primeni odgovarajuće mere koje pružaju bezbednost podacima o ličnosti koji su osnovne sredstvo takve obrade.

U određenim slučajevima građani ne mogu da izbegnu primenu rezultata automatske obrade podataka. Postoje tri grupe slučaja u kojima se moraju prihvataju rezultati automatske obrade podataka.

Prva grupa odnosi se na situaciju kada je *odluka doneta na osnovu posebnog propisa* koji dozvoljava automatsku obradu podataka. Na ovaj način ostavlja se mogućnost da se u pojedinim slučajevima, kada organi uprave obavljaju važne društvene poslove (kao što je nacionalna bezbednost i javno zdravstvo primer radi), omogući automatska obrada podataka o ličnosti kao pravilo. Svakako, propis koji dozvoljava automatsku obradu podataka mora biti posebno obrazložen, zasnovan na legitimnim očekivanjima građana i u skladu sa sistemom zaštite podataka.

---

[216] *Ibid*, str. 18.

[217] O kritikama u vezi sa pravom na automatsku obradu vid. Sandra Wachter, Brent Mittelstadt, Luciano Floridi, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, *International Data Privacy Law,* No. 2/2017 (ed. Nora Ni Loideain), Oxford 2017, p. 76-99.

Druga grupa tiče se situacija u kojima je automatska obrada podataka *potrebna radi sklapanja i izvršenja pravnog odnosa* između lica čiji su podaci i rukovaoca. Ponekad, rukovalac ima potrebu da se osloni isključivo na automatske načine obrade podataka, a lica čiji se podaci obrađuju imaju potrebu da sa rukovaocem stupe u određeni pravni odnos. *Primera radi*, kod raspisivanja konkursa za posao u organima javne uprave može se prijaviti veliki broj kandidata. Poslodavac se može odlučiti da automatski napravi uži krug kandidata na osnovu prethodno unetih parametara. U toj situaciji opravdana je upotreba automatske obrade, budući da kandidati žele da stupe u poslovni (pravni) odnos sa rukovaocem. To znači da kandidati svojom prijavom, implicitno pristaju na automatsku obradu podataka.

Treći i poslednji slučaj odnosi se na *davanje izričitog pristanka* na automatizovanu obradu lica čiji se podaci obrađuju. Budući da pristankom lice iznosi svoj stav o tome da smatra da su mu zaštićena prava i interesi, nema prepreke za vršenje automatske obrade podataka.

Daljim usavršavanjem informaciono-komunikacionih tehnologija i posebno veštačke inteligencije, razvijaće se i stepen pravilnosti i tačnosti rezultata automatizovanih obrada. Do tada, neophodno je pružiti građanima sigurnost u odnosu na automatsku obradu njihovih podataka o ličnosti.

4.3.8. Pravo na pravno sredstvo u vezi sa obradom podataka o ličnosti

Osnovno pravo građana putem koga se obezbeđuje zakonitost obrade i odluka u vezi sa podacima građana predstavlja pravo na pravni lek. „Pod pojmom pranog leka podrazumeva se svaki onaj način na koji se određeno lice može obratiti domaćem sudu ili organu uprave i tražiti zaštitu povodom povrede nekog svog prava“.[218] Dakle, pravni lek predstavlja ovlašćenje nezadovoljnog lica da ospori određenu pojedinačnu odluku koja proizvodi pravna dejstva tako da ta odluka bude ispitana od strane nadležnog organa.

Značaj prava na pravno sredstvo prepoznat je u najvažnijim međunarodnim dokumentima. Tako, Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda[219] posvećuje pažnju *pravu na delotvorni pravni lek*.[220]

[218] Bojan Tubić, „Lokalni pravni lekovi u praksi Evropskog suda za ljudska prava“, *Zbornik radova Pravnog fakulteta u Novom Sadu* 3/2006, Novi Sad 2006, str. 414.
[219] Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda, Savet Evrope, Rim, 1950.
[220] Čl. 13 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda.

Pravo na pravni lek predstavlja nezaobilazni element u svim granama prava, pa postoji u krivičnom, građanskom, upravnom i drugim procesnim pravima. Prema tome, pravni sistem ne može se zamisliti bez mogućnosti ulaganja pravnog leka. Jedino se na taj način može ostvariti kontrola zakonitosti i pravilnosti rada u različitim oblastima života, pa i u vezi sa obradom podataka o ličnosti.

U pravnom sistemu Srbije, Ustavom je garantovana jednaka zaštita prava građana. To znači da svako ima pravo na žalbu ili drugo pravno sredstvo protiv odluke kojom se odlučuje o njegovom pravu, obavezi ili na zakonom zasnovanom interesu.[221] Zakon o zaštiti podataka o ličnosti poznaje „pravo na prigovor" kao pravno sredstvo protiv obrada podataka o ličnosti i odluka za koje lice smatra da su nepravilne ili nezakonite.

„Ako smatra da je to opravdano u odnosu na posebnu situaciju u kojoj se nalazi, lice ima pravo da u svakom trenutku podnese prigovor na obradu podataka o ličnosti koji se na njega odnose (*u vezi sa obradom koja je neophodna u cilju obavljanja poslova u javnom interesu ili izvršenja ovlašćenja rukovaoca, obradu koja je neophodna u cilju ostvarenja opravdanih interesa rukovaoca ili trećih lica* (dodali autori)), uključujući i profilisanje koje se zasniva na ovim odredbama. Rukovalac ima obavezu da prekine sa obradom podataka o licu koje je podnelo prigovor, osim ako je predočio da postoje legitimni osnovi za obradu koji pretežu nad interesima, pravima ili slobodama lica na koje se podaci odnose, ili su u vezi sa podnošenjem, ostvarivanjem, odnosno odbranom od pravnog zahteva".[222] Prigovor se, dakle, može podneti u svakom trenutku obrade, što znači da on ne može biti preuranjen ili neblagovremen.

Rukovalac ima dužnost da, već kod uspostavljanja prvog kontakta sa licem na koje se podaci odnose, pruži obaveštenje o mogućnosti podnošenja prigovora. To treba učiniti na jasan način i odvojeno od ostalih informacija koje mu se pružaju.

Po uloženom prigovoru, rukovalac mora da prestane sa obradom podataka kako bi se sprečio eventualni nastanak štete. To znači da je osnovno dejstvo prigovora u sprečavanju daljih radnji obrade podataka o ličnosti. Ipak, rukovalac može nastaviti sa obradom ako dokaže legitimnu potrebu za obradom koja preteže nad interesima lica čiji su podaci. Takođe, kada je reč o obradi podataka koja se vrši u cilju pripremanja ili odbrane od pravnog zahteva, rukovalac nema obavezu da prekine sa obradom.

Treba pomenuti da je pravo na prigovor apsolutno pravo u vezi sa obradom podataka u cilju direktnog marketinga, odnosno oglašavanja. Naime,

[221] Čl. 36, st. 2 Ustava RS.
[222] Čl. 37, st. 1 Zakona o zaštiti podataka o ličnosti.

građani imaju pravo da podnesu prigovor u svakom trenutku u slučaju korišćenja njihovih podataka u svrhu direktnog marketinga, pri čemu se posle podnošenja prigovora njihovi podaci ne mogu obrađivati u tu svrhu.[223]

Za rukovaoca predviđen je rok od 30 dana, od dana prijema zahteva, da obavesti lice o osnovanosti zahteva. Rok se može produžiti za isti vremenski period do 60 dana, ukoliko je zahtev složen ili se odnosi na značajan broj podataka. Ako propusti pomenute rokove, za rukovaoca nastaje obaveza da obavesti lice koje je uložilo prigovor da ima pravo na pritužbu Povereniku, kao i pravo da podnese tužbu nadležnom sudu. Ipak, Zakon ne sadrži detaljnije odredbe u vezi sa načinom postupanja rukovaoca sa prigovorom.

Podnošenje prigovora rukovaocu ne utiče na pravo lica čiji se podaci (nepravilno ili nezakonito) obrađuju da podnese pritužbu Povereniku zbog povrede neke od odredbi Zakona o zaštiti podataka o ličnosti u odnosu na njegove podatke. Takođe, prigovor rukovaocu ne utiče ni na mogućnosti ostvarivanja sudske zaštite prava lica na koje se podaci odnose. Hipotetički, to znači da jedno fizičko lice može istovremeno da podnese prigovor rukovaocu, pritužbu Povereniku i tužbu sudu.

4.3.9. Ograničenje prava u vezi sa obradom podataka o ličnosti

Ljudska prava garantuju građanima zaštitu od mešanja drugih lica i posebno organa javne vlasti u njihov lični život, pa zbog toga predstavljaju osnovni pojavni oblik principa vladavine prava i pravne države. Ipak, njihovo važenje nije apsolutno, pa se u propisima širom sveta neretko predviđaju situacije koje opravdavaju ograničenje pojedinih ljudskih prava i sloboda. Situacije u kojima je moguće ograničiti ljudska prava i slobode, obično se vezuju za neke neuobičajene državne i društvene prilike, poput *vanrednih situacija, vanrednog i ratnog stanja*.

Tada se javlja neophodnost ograničenja pojedinih prava kako bi se osiguralo efikasno funkcionisanje zajednice pod takvim neprilikama i što pre omogućio povratak na „normalno stanje“. Jednostavno, u takvim situacijama nije realno očekivati uobičajeno funkcionisanje države, pa samim tim ni prava koja ona garantuje.

Načini i mogućnost odstupanja od ljudskih prava poznati su i u međunarodnim dokumentima. Univerzalna deklaracija o ljudskim pravima navodi

[223] Čl. 37, st. 2 i 3 Zakona o zaštiti podataka o ličnosti.

da „u vršenju svojih prava i sloboda svako se može podvrgnuti samo onim ograničenjima koja su predviđena zakonom u cilju obezbeđenja nužnog priznanja i poštovanja prava i sloboda drugih i opšteg blagostanja i u cilju zadovoljenja pravičnih zahteva morala, javnog poretka i opšteg blagostanja".[224] Mogućnost ograničenja ljudskih prava predviđena su i Evropskom konvencijom za zaštitu ljudskih prava i osnovnih sloboda. Međutim, Konvencija predviđa i granicu ograničenja koja su dozvoljena, pa navodi da se predviđena ograničenja neće primenjivati u druge svrhe, osim onih koje su dozvoljene Konvencijom.[225] Pravila pomenutih međunarodnih dokumenata prihvatile su i države širom sveta.

Mogućnost odstupanja od ljudskih prava predviđa se i u oblasti zaštite podataka o ličnosti. U vanrednim okolnostima uživanje prava u vezi sa podacima o ličnosti neće biti moguće, budući da drugi, prevashodno *javni interesi, pretežu nad pojedinačnim pravima u takvim okolnostima*. Međutim, i tada je važno voditi se najmanjim mogućim stepenom odstupanja od pojedinog prava, odnosno „najnužnijom merom koju zahteva situacija".[226] To znači i da prava treba vratiti građanima čim se za to ukaže odgovarajuća prilika, odnosno čim opasnost prođe.

Zakon o zaštiti podataka o ličnosti poznaje institut ograničenja prava, ali i obaveza u vezi sa podacima o ličnosti. Osnovni uslov za ograničenje prava građana u vezi sa podacima o ličnosti jeste da „ta ograničenja ne zadiru u suštinu osnovnih prava i sloboda i ako to predstavlja neophodnu i srazmernu meru u demokratskom društvu".[227] Treba pomenuti da ograničenje ne mora da bude uvedeno zakonom, već se može uvesti i aktom niže pravne snage, tumačeći odredbe Zakona o zaštiti podataka o ličnosti. Svakako, kada donosi odluku o uskraćivanju pojedinog prava „treba imati u vidu da se i u tim slučajevima organ uprave nalazi pod pravnim poretkom, što znači da prilikom biranja između više alternativa u konkretnom slučaju, mora da izabere onu koja, po njegovoj oceni najbolje, odgovara javnom interesu, a ne interesu nekog pojedinca ili neke uže grupe".[228]

---

[224] Čl. 29, st. 2 Univerzalne deklaracije o ljudskim pravima.

[225] Čl. 18 Evropske konvencije za zaštitu ljudskih prava i osnovnih sloboda. U pogledu prava na privatnost, Konvencija je predvidela da se javne vlasti neće mešati u privatnost građana, osim ukoliko je to u skladu sa zakonom i ako potrebe demokratskog društva to zahtevaju, a posebno interesi nacionalne i javne bezbednosti, ekonomskog razvoja, javnog zdravlja i morala, kao i prava i sloboda građana.

[226] Milan Paunović, Boris Krivokapić, Ivana Krstić, *Međunarodna ljudska prava*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013, str. 65.

[227] Čl. 40, st. 1 Zakona o zaštiti podataka o ličnosti.

[228] Dragan Vasiljević, *Zakonitost uprave i diskreciona ocena*, Kriminalističko-policijska akademija, Beograd 2012, str. 99.

Ograničenje prava može se uvesti radi zaštite nekog od širih društvenih interesa, kao što je nacionalna bezbednost, odbrana, javna bezbednost, sprečavanje istrage i otkrivanje krivičnih dela, gonjenje učinilaca krivičnih dela, drugih važnih opštih javnih interesa, a posebno važnih državnih ili finansijskih interesa Republike Srbije (monetarna politika, budžet, poreski sistem, javno zdravlje, socijalna zaštita), nezavisnosti pravosuđa i sudskih postupaka, sprečavanje, istraživanje, otkrivanje i gonjenje povreda profesionalne etike, funkcije praćenja nadzora ili vršenja regulatorne funkcije, zaštite lica na koje se podaci odnose, i ostvarivanja potraživanja u građanskim stvarima.[229]

Kao primer ograničenja ljudskih prava u vezi sa podacima o ličnosti navodimo slučaj pandemije virusa COVID-19, kada su mnoge države uvele restriktivne mere, između ostalog i digitalno praćenje komunikacije potencijalnih zaraženih i zaraženih kako bi se sprečilo dalje širenje epidemije, odnosno zaštitilo javno zdravlje.[230] Republika Srbija nije uvodila ovakve ograničavajuće mere u pogledu podataka o ličnosti.[231]

Kako bi odluka o ograničenju prava i sloboda bila zakonita, ona mora biti zasnovana na analizi i proceni određenih (minimalnih) elemenata. Smatramo da ove elemente treba obrazložiti, svaki posebno, u odluci kojom se uvodi ograničenje kako bi takva odluka bila legitimna i zakonita. Elementi koje treba uzeti u obzir priliko uvođenja ograničenja su:

1. *Svrha ili vrsta obrade,*
2. *Vrste podataka o ličnosti,*
3. *Obim ograničenja,*
4. *Mere zaštite u cilju sprečavanja zloupotrebe, nedozvoljenog pristupa ili prenosa podatka,*
5. *Osobenosti rukovaoca,*
6. *Vremenski period čuvanja i primene mere zaštite,*
7. *Rizike po prava i slobode lica,*
8. *Pravo na informisanje o ograničenju.*[232]

Dakle, mogućnost ograničenja prava u vezi sa zaštitom podataka uveo je zakon, ali on dozvoljava da o ograničenjima odlučuju organi javne vlasti (pojedinačnim ili podzakonskim opštim aktima). To znači da je zakonodavac sa

[229] Čl. 40, st. 1 Zakona o zaštiti podataka o ličnosti.

[230] PC Press, Odobreno korišćenje špijunskih softvera", 22.03.2020. god., https:// pcpress.rs/izrael-odobrio-koriscenje-spijunskih-softvera.

[231] O detaljnom postupanju za vreme pandemije vid. SHARE fondacija, *Vodič za zaštitu podataka o ličnosti za vreme pandemije*, SHARE fondacija, Beograd 2020, https: // pandemija. mojipodaci. rs.

[232] Čl. 40, st. 2, Zakona o zaštiti podataka o ličnosti i čl. 23, st. 2, Opšte uredbe EU.

postavljenim kriterijumima uspostavio ograničenja, odnosno parametre za diskrecionu ocenu, jer je nemoguće očekivati da se zakonom urede sve moguće situacije, zbog čega se odluka u vanrednim okolnostima prepušta organima javne vlasti, koji su bliži građanima i praksi.

5. PROPISI U OBLASTI ZAŠTITE PODATAKA O LIČNOSTI

5.1 Evropski propisi koji uređuju pitanja zaštite podataka o ličnosti

Evropska Unija (EU) predstavlja međuvladinu i nacionalnu uniju koja se sastoji od 27 država članica. Države članice međusobno usko sarađuju i vode zajedničku politiku u različitim oblastima. U okvirima EU uspostavljeno je jedinstveno tržište koje omogućava slobodan protok ljudi, kapitala, roba i usluga. Radi pravilnog funkcionisanja i ostvarivanja ciljeva, jedinstveno tržište podrazumeva efikasnu razmenu brojnih podataka između država članica, ali i drugih subjekata. Među ovim podacima nalaze se i podaci velike većine lica koja imaju prebivalište ili boravište na teritoriji EU ili obavljaju poslovne aktivnosti na ovoj teritoriji. Imajući to u vidu, potrebu za zaštitom ljudskih prava i potrebu za pravilnim funkcionisanjem institucija EU, važno pravo koje štiti građane jeste pravo na privatnost i pravo na zaštitu podataka o ličnosti.

Oblast zaštite podataka o ličnosti na nivou EU prvi put je uređena 1995. godine. Tokom narednih godina, različiti spoljni i unutrašnji faktori, poput razvoja informaciono-komunikacionih tehnologija, sve veće upotrebe interneta, razvoj međunarodne saradnje i trgovine, sve veća upotreba podataka u poslovanju, ali i značajna kršenja prava privatnost uticali su na javljanje potrebe da se ova oblast detaljno uredi. Razvila se svest o potrebi ustanovaljvanja posebnog prava koji će zaštititi podatke o ličnosti. Tako je usvajanjem Povelje o osnovnim pravima EU,[233] koja predstavlja propis koji uređuje brojna građanska, ekonomska, politička i kulturna prava građana u okviru EU, prvi put u istoriji EU, pa i evropskih propisa, predviđeno posebno pravo na zaštitu podataka o ličnosti. Članom 8 Povelje o osnovnim pravima EU, predviđeno je da svako ima pravo na zaštitu podataka o svojoj ličnosti. Takođe, predviđeno je da podaci o ličnosti moraju biti obrađivani pošteno, za unapred određenu svrhu i na osnovu informisanog pristanka osobe, ili na nekom drugom legitimnom osnovu koji se

[233] Povelja o osnovnim pravima EU, „Sl. glasnik EU“, br. 326/391. Tekst Povelje na engleskom jeziku dostupan je na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX: 12012P/TXT&from=EN.

zasniva na zakonu. Kao posebna prava u vezi sa pravom na zaštitu podataka o ličnosti, Povelja o osnovnim pravima EU poznaje pravo svakog lica da pristupi prikupljenim podacima o svojoj ličnosti i pravo da zatraži njihovu ispravku od lica koje obrađuje podatke. Kontrola za postupanje po predviđenim pravilima data je nezavisnim organima.[234] Povelja o osnovnim pravima EU stupila je snagu usvajanjem Lisabonskog ugovora, što suštinski znači da Sud pravde EU ima ovlašćenje da postupa po tužbama u vezi sa povredama ovog propisa od strane organa, tela i agencija EU.[235]

Zahvaljujući Povelji o osnovnim pravima EU, otvoren je prostor za razgovore o usvajanju propisa koji će na jedinstven način, na teritoriji čitave EU, regulisati pitanja od značaja u vezi sa zaštitom podataka o ličnosti. Nakon dugotrajne borbe građana i nevladinih organizacija, Evropski parlament i Veće EU predložili su donošenje propisa koji će unifikovati i osnažiti zaštitu svih lica u okviru EU. Kao posledica, usvojena je, možda i najznačajnija uredba u novijoj istoriji EU – Opšta uredba EU, 27. aprila 2016. godine, a svoju primenu je započela 25. maja 2018. godine.

5.1.1. Opšta uredba EU

U pravnom sistemu EU, uredbe predstavljaju akte opšte pravne snage koji se direktno primenjuju u svim državama članicama, bez potrebe za implementacijom u nacionalna zakonodavstva. Donošenje ove Uredbe uslovljeno je buđenjem građanske svesti o važnosti zaštite podataka o ličnosti i težnjom za približavanjem evropskih institucija građanima. Jedna od osnovnih ideja Uredbe jeste da nadzor nad korišćenjem podataka o ličnosti učini dostupnim građanima, koji će sami moći da kontrolišu i vode računa o svojim podacima koje koriste druga lica. Ipak, javljaju se i mišljenja da EU nije donela Opštu uredbu EU samo radi zadovoljenja potreba i interesa građana, već i zbog punjenja sopstvenog budžeta, imajući u vidu astronomske kazne i odredbe koje nije lako implementirati u poslovanju.

O velikom značaju ove Uredbe svedoči i dugačka Preambula koja se sastoji od preko 170 tačaka. U preambuli, kao svojevrsnom uvodu u materijalne odredbe, ukazuje se na razloge, načela i ciljeve kojima su se vodili njeni tvorci prilikom donošenja. Odredbe Preambule govore o tome na koji način treba

[234] Vid. čl. 8 Povelje o osnovnim pravima EU.

[235] Zoran Radivojević, „Sud pravde Evropske Unije posle Lisabonskog ugovora“, *Zbornik radova Pravnog fakulteta u Nišu br. 73*, Niš 2016, str. 34.

primeniti materijalne odredbe. Možemo reći da odredbe Preambule predstavljaju svečani uvod sa zaključcima i ciljevima donosioca, dok materijalne odredbe precizno regulišu ponašanje različitih subjekata u ovoj materiji.

Preambula upućuje na Povelju EU o osnovnim pravima i Ugovor o funkcionisanju EU gde je ustanovljeno pravo svakog na zaštitu podataka o ličnosti. Naglašeno je da se Uredbom želi doprineti uspostavljanju slobode, sigurnosti i pravde u okviru EU, kao i jačanju i približavanju država članica na unutrašnjem tržištu. Pravo na zaštitu podataka o ličnosti nije predviđeno kao apsolutno pravo, već se mora posmatrati u odnosu na društvenu funkciju, te mu se mora pristupiti u skladu sa načelom proporcionalnosti (u odnosu na druga osnovna ljudska prava i slobode). Pored zaštite pojedinca i društva, jedan od razloga donošenja Opšte uredbe EU leži i u digitalnoj ekonomiji, koja zahteva sigurnost i pouzdanost razmene podataka.

Opšta uredba EU u okviru Preambule promoviše princip neutralnosti tehnologija. Zaštita prava privatnosti i podataka o ličnosti mora biti tehnološki neutralna, što znači da ona ne sme da zavisi od tehnologije koja se koristi u tom trenutku. Nezavisno od toga da li se primenjuje automatizovana ili ručna obrada podataka, zaštita podataka mora biti primenjena. U Preambuli je zauzeto stanovište da se Opšta uredba EU odnosi isključivo na žive osobe. Pored pomenutih, značajan je i princip identiteta. Principi identiteta govori o tome da se Opšta uredba EU odnosi samo na osobe koje su konkretno identifikovane ili se kao takve mogu identifikovati. Sa druge strane, to znači da se ona ne odnosi na podatke o ličnosti koji se nalaze pod pseudonimima.[236]

U Preambuli Opšte uredbe EU ukazano je i na značaj Suda pravde EU i Evropskog suda za ljudska prava. U vezi sa pravilom da pravni osnovi obrade podataka o ličnosti ne moraju biti eksplicitno propisani u zakonu, predviđa se da „takav pravni osnov ili zakonodavna mera mora biti jasna i precizna, a njena primena trebalo bi da bude predvidljiva licima na koje se primenjuje, u skladu sa sudskom praksom Suda pravde Evropske Unije i Evropskog suda za ljudska prava.“[237]

U Preambuli se promoviše niz novih instituta koji služe kvalitetnijoj zaštiti podataka o ličnosti. U tom smislu, promovisano je pravo na zaborav. Njegova primena odnosi se na brisanje svih podataka o ličnosti čija je svrha ispunjena, kao i uklanjanje svih veza i kopija. Primećujemo da pažnja Preambule nije usmerena isključivo na pravne aspekte zaštite podataka o ličnosti. Javljaju se

[236] Ipak, Uredba daje određeni značaj pseudonimizaciji podataka, prihvatajući je kao adekvatno sredstvo za zaštitu ličnih podataka. Vid. tač 28 i 29 Preambule Opšte uredbe EU.

[237] Tač. 41 Preambule, Opšte uredbe EU.

i obaveze primene tehnoloških i organizacionih mera, koje bi trebalo da pomognu u zaštiti podataka o ličnosti. Procena rizika zauzima važno mesto u čitavom sistemu. Značajan deo preambule usmeren je na pitanja u vezi sa nadzornim telima u oblasti zaštite podataka. Nadzorno telo treba da postoji u svakoj državi članici i nadležnost mu je da vodi računa o adekvatnoj primeni pravila u vezi sa zaštitom podataka o ličnosti. Naravno, promoviše se visok stepen saradnje između nadzornih tela različitih država članica.

Iako odredbe Preambule ne predstavljaju materijalne odredbe koje se direktno primenjuju, njena važnost je od suštinskog značaja za razumevanje kompletnog sistema zaštite podataka EU, kao i za rešavanje nedoumica i pravnih praznina koje će se javljati prilikom primene.

5.1.1.1. Cilj, predmet i teritorijalno važenje

Osnovni cilj Opšte uredbe EU jeste stvaranje pravila kojima se pruža zaštita pravu na zaštitu podataka o ličnosti, odnosno podacima o ličnosti fizičkih lica. Uz to, uredba predviđa i pravila u vezi sa prenosom i slobodnim protokom podataka o ličnosti.

Teritorijalno važenje znači da se njene odredbe primenjuju na sve obrade podataka o ličnosti u okviru poslovnih aktivnosti rukovaoca i obrađivača sa sedištem u EU, nezavisno od toga da li se obrada obavlja na teritoriji EU ili van nje. Pod obradom podataka, podrazumeva se kako automatska, tako i ručna obrada podataka.

Opšta uredba EU poznaje i eksteritorijalno važenje. Naime, njene odredbe primenjuju se i na obradu koju vrše lica koja nemaju sedište u EU, ukoliko su aktivnosti povezane sa: 1. Ponudom robe ili usluga licima u EU, 2. Praćenjem ponašanja dokle god se njihova delatnosti odvija unutar EU, 3. U slučajevima primene normi međunarodnog javnog prava.[238]

Dakle, odredbe Opšte uredbe EU primenjuju se i na lica koja obrađuju podatke o ličnosti izvan teritorije EU, ali su na određeni način povezani (robom i uslugama) sa licima na njenoj teritoriji. Na taj način, znatno se proširuje teritorijalna primena na mnoge države koje nisu članice EU, ali imaju jaku ekonomsku vezu sa njenim tržištem, pa će se na njih i njihove građane i privredne subjekte primenjivati norme Opšte uredbe EU. Takav je slučaj i sa Republikom Srbijom, koja je kandidat za članstvo u EU i kao takva ostvaruje jaku poslovnu i finansijsku saradnju sa subjektima na teritoriji EU.

[238] Čl. 3 Opšte uredbe EU.

Poseban deo Opšte uredbe EU posvećen je određenju, odnosno, definisanju pojmova koji se koriste u tekstu. Cilj definicija jeste da olakša primenu u praksi i odredi domašaj njenih odredbi. Posvetićemo pažnju značajnijim pojmovima za sistem zaštite podataka o ličnosti.

5.1.1.2. Osnovni pojmovi u Opštoj uredbi EU

Prvi i najvažniji pojam, koji predstavlja centar ovog univerzuma zaštite podataka o ličnosti, jeste pojam podataka o ličnosti. Uredba određuje da su podaci o ličnosti svi oni podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Pojedinac čiji se identitet može utvrditi je osoba koja se može direktno ili indirektno lično identifikovati uz pomoć identifikatora, kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više činilaca svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.[239] Može se zaključiti da se Opšta uredba EU odnosi isključivo na živa fizička lica (ne primenjuje se na pravna lica), čiji se identitet može utvrditi na osnovu određenih ličnih karakteristika. To znači da se Uredba neće odnositi na lica koja se ne mogu identifikovati, odnosno na lica koja se predstavljaju drugačijim identitetom, što je od posebne važnosti za internet zajednicu i one koji se „skrivaju" iza lažnih internet profila.

Budući da je njen osnovni predmet zaštita, određeno je šta će se smatrati povredom podataka o ličnosti. Pod povredom podataka o ličnosti podrazumeva se svako kršenje bezbednosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima koji su preneseni, pohranjeni ili na drugi način obrađeni.[240] Dakle, zakonita primena podrazumeva da svaka aktivnost onih koji obrađuju podatke o ličnosti mora biti u skladu sa odredbama Opšte uredbe EU i osnovnim ljudskim pravima i slobodama.

Obrada podataka se odnosi na svaku aktivnost ili skup aktivnosti koji se preduzimaju u vezi sa podacima o ličnosti ili skupovima takvih podataka, automatski ili ručno, kao što su prikupljanje, beleženje, organizacija, strukturiranje, čuvanje, izmena, pronalaženje, obavljanje uvida, upoređivanje, otkrivanje prenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombinovanje, ograničavanje, brisanje ili uništavanje.[241] Vidimo da Opšta uredba EU navodi brojne aktivnosti koje potpadaju pod pojam obrade. Faktički to znači da se svako korišćenje, odnosno upotreba podataka može klasifikovati u radnje obrade.

[239] Čl. 4, st. 1, tač. 1 Opšte uredbe EU.
[240] Čl. 4, st. 1, tač. 12 Opšte uredbe EU.
[241] Čl. 4., st. 1, tač. 2 Opšte uredbe EU.

Već je pomenuto da se funkcionisanje Opšte uredbe EU odvija na osnovu posebnih načela. Reč je o načelima zakonitosti, pravednosti i transparentnosti, ograničenja u odnosu na svrhu obrade, korišćenja najmanjeg mogućeg obima podataka, tačnosti i potpunosti, ograničenog čuvanja podataka, integriteta i poverljivosti, kao i na načelu odgovornosti.

Sistem zaštite podataka koji stvara Opšta uredba EU podrazumeva i predviđanje procesnih i materijalnih prava građana u vezi sa zaštitom podataka o ličnosti. Kroz promovisanje tih prava naglašava se težnja Opšte uredbe EU da sistem kontrole i nadzora nad obradom podataka o ličnosti bude više u rukama građana. Značajan broj prava predstavlja konkretizaciju načela, koja se kroz njih ostvaruju u praksi. U tom smislu, zajamčeni su pravo na obaveštenost, odnosno pravo na dobijanje informacije o podacima, pravo na ispravku i dopunu, pravo na ograničenje obrade ličnih podataka, pravo na zaborav, prava u vezi sa automatskom obradom podataka, pravo na prenosivost podataka i pravo na pravno sredstvo.

5.1.1.3. Rukovalac

Osnovni subjekti koji su u fokusu procesa zaštite podataka su: rukovalac, obrađivač i lice čiji se podaci obrađuju. Rukovalac može biti fizičko ili pravno lice, organ vlasti, agencija ili drugo telo koje određuje svrhu i način obrade podataka o ličnosti. Ovo lice je glavno odgovorno za obradu podataka o ličnosti, pa u skladu sa tim ima dužnost i obavezu da pravilno primeni odredbe Opšte uredbe EU. Pravne mere nisu jedine na koje rukovalac podacima treba da obrati pažnju prilikom obrade. On mora da predvidi i implementira tehničke, organizacione i kadrovske mere, pri čemu mora da bude u mogućnosti i da dokaže njihovu primenu u svakom konkretnom slučaju.[242] Prilikom implementiranja mera, treba imati u vidu prirodu, obim, okolnosti i svrhu obrade, kao i moguće rizike od štetnih posledica. Sve mere koje se primenjuju treba da podležu vremenskom i materijalnom preispitivanju, što znači da ih treba ažurirati u odgovarajućim vremenskim ciklusima. Napredak tehnologije neminovno utiče na razvoj opasnosti po podatke o ličnosti i prava građana, pa je zbog toga neophodno da i odbrambeni sistemi zaštite tehnološki prate razvoj opasnosti.

Uvažavajući zahtevnu poziciju rukovaoca, Opšta uredba EU predviđa i mogućnost da više rukovalaca zajednički usmeravaju i vode postupak obrade. U tom slučaju se primenjuju odredbe o zajedničkim rukovaocima. Za primenu instituta zajedničkog rukovođenja, neophodno je da rukovaoci učine javnim

[242] Čl. 24, st. 1 Opšte uredbe EU.

(transparentnim) međusobni sporazum o odgovornosti i nadležnosti u vezi sa obradom. Detalji takvog sporazuma moraju biti dostupni licu čiji se podaci obrađuju. Na ovaj način, Uredba teži da omogući ostvarivanje svih prava na jasan i transparentan način. Nezavisno od pomenutih sporazuma, lice čiji se podaci obrađuju može ostvarivati svoja prava u odnosu na svakog rukovaoca posebno, što predstavlja značajno pravno sredstvo u rukama građana.

5.1.1.4. Obrađivač

Rukovalac podataka može odrediti lice koje će u njegovo ime vršiti obradu podataka. To lice se naziva obrađivač podataka.[243] Obrađivač jeste pravno ili fizičko lice, organ vlasti, agencija ili drugo telo koje obrađuje podatke o ličnosti u ime rukovaoca. Rukovalac može sarađivati isključivo sa licem čije znanje, sposobnosti i opremljenost garantuju primenu pravila Opšte uredbe EU. To znači da obrađivač mora biti spreman da preduzme adekvatne tehničke i organizacione mere.

Obrada od strane obrađivača mora se urediti ugovorom ili drugim pravno obavezujućim aktom, u skladu sa pravom države članice ili Unije. Opštom uredbom EU predviđaju se i obavezni elementi ovog ugovora. To su: predmet i trajanje obrade, priroda i svrha obrade, vrsta podataka o ličnosti i kategorije lica na koja se podaci odnose, obaveze i prava rukovaoca. Opšta uredba EU propisuje i posebne odredbe koje ugovor ili drugi obavezujući akt mora da poseduje. Reč je o obavezama na strani obrađivača koje se tiču postupanja prema dokumentovanim uputstvima rukovaoca, preduzimanja odgovarajućih mera, poštovanje uslova o angažovanju drugog obrađivača, pomaganju rukovaocu u pružanju mera, obezbeđivanju usklađenosti i stavljanju informacija na uvid.[244]

Iako je reč o sporazumnom odnosu, Uredba predviđa konkretne obaveze za obrađivača koje moraju naći mesto u ugovoru. Na taj način, pruža se dvostruka zaštita, zakonska i ugovorna, što naglašava značaj uloge rukovaoca i obrađivača. Time se stavlja poseban akcenat na obaveze koje su neophodne za adekvatnu preventivu u ovoj oblasti.

Dok rukovalac ima pravo da angažuje lice koje će obrađivati podatke u njegovo ime, obrađivač ne sme samovoljno da odredi podobrađivača. Za takvo angažovanje mora dobiti opšte ili posebno odobrenje od rukovaoca koje je sačinjeno u pisanoj formi. Ukoliko se odobrenje daje kao opšte, obrađivač ima dužnost da rukovaoca blagovremeno obavesti o svim promenama u vezi sa

[243] Vid. čl. 4, st. 1, tač. 8 Opšte uredbe EU.
[244] Čl. 28 Opšte uredbe EU.

obradom podataka i licem koje podatke obrađuje, kako bi rukovalac mogao da uloži prigovor na takve radnje. U slučaju da obrađivač angažuje podobrađivača da u ime rukovaoca vrši posebne aktivnosti obrade ličnih podataka, podobrađivač podleže istoj ugovornoj i zakonskoj odgovornosti kao i obrađivač.[245]

Osim subjektivne, Opšta uredba EU poznaje i sistem objektivne odgovornosti i predviđa da obrađivač ostaje u potpunosti odgovoran rukovaocu za izvršenje obaveza podobrađivača. Ovakav sistem odgovornosti nosi dvostruku korist. Pre svega, građani čiji se podaci obrađuju moraju u svakom trenutku znati ko obrađuje njihove podatke i kome se mogu obratiti u slučaju povrede. Takođe, rukovalac mora biti siguran da će obrađivač i podobrađivač primeniti najadekvatnije mere zaštite, kako bi proces obrade podataka bio u najvećoj mogućoj meri pouzdan i siguran.

Brz napredak tehnologije ne može uvek da bude praćen adekvatnom zaštitom. Zbog toga, Uredba omogućava obrađivaču i podobrađivaču da izbegnu odgovornost dokazivanjem da su postupali u svemu prema odobrenim kodeksima ponašanja, odnosno odobrenim mehanizmima sertifikacije. Pružanjem dokaza da su primenjivali mere predviđene kodeksom ponašanja odnosno sertifikovanim mehanizmima obrade, obrađivač i podobrađivač dokazuju da su postupali savesno i legalno, pružajući najviši mogući stepen zaštite podataka o ličnosti u tom trenutku.

5.1.1.5. Princip integrisane privatnosti i podrazumevane privatnosti (Privacy by default & Privacy by design)

Veliku pažnju u stručnoj javnosti privukla su dva principa koja Opšta uredba EU ustanovljava u vezi sa obavezama rukovaoca. To su princip podrazumevane privatnosti (*Privacy by default*) i princip ugrađene privatnosti (*Privacy by design*). Ovi principi usko su povezani sa novim tržištima, digitalnom ekonomijom i industrijom 4.0. Na taj način razvoj tehnologije i tehnike prepoznat je i u pravnim okvirima.

Princip podrazumevane privatnosti odnosi se na proaktivni pristup u vezi sa zaštitom podataka o ličnosti, još od prvih faza razvijanja pojedine usluge ili dobra. Dakle, u cilju poštovanja ovog principa potrebno je voditi računa o merama zaštite i bezbednosti podataka o ličnosti, već prilikom planiranja sredstava i načina obrade, što podrazumeva i njihovu implementaciju tokom procesa obrade. Zato je neophodno izvršiti procenu proporcionalnosti tehničkih i organizacionih mera koje se mogu implementirati. U tom smislu, Opšta uredba

[245] Čl. 28, st. 4 Opšte uredbe EU.

EU navodi: „Uzimajući u obzir najnoviji tehnološki razvoj, troškove sprovođenja i prirodu, obim, kontekst i svrhe obrade, kao i rizike različitih stepena verovatnoće i ozbiljnosti za prava i slobode fizičkih lica koji proizlaze iz obrade podataka, rukovalac prilikom određivanja sredstava obrade i prilikom same obrade primenjuje odgovarajuće tehničke i organizacione mere, poput pseudonimizacije, koje su osmišljene za delotvorno sprovođenje načela zaštite podataka, kao što je korišćenje najmanjeg mogućeg obima podataka, i u obradu uključuje zaštitne mere radi ispunjenja zahteva iz ove uredbe i zaštite prava lica na koja se podaci odnose.[246]

Ovaj princip ima veliku upotrebnu vrednost u oblasti digitalnih društvenih mreža. Kako se navodi, „društvene mreže bi trebalo da podstiču uređivanje profila na društvenim mrežama na način kojim se štiti privatnost, na primer, da u startu ograniče mogućnost pristupa profilu, tako da on nije podrazumevano (*by default*) dostupan neodređenom broju licu“.[247]

Princip ugrađene privatnosti znači da rukovalac treba da primeni adekvatne mere isključivo nad podacima o ličnosti koje su neophodne za ostvarivanje svrhe obrade. Kod ovog principa reč je o merama koje se „ugrađuju“ tokom procesa obrade, imajući na umu količinu prikupljenih podataka, obim njihove obrade, rok čuvanja i dostupnost drugim licima. Suštinski najznačajnija posledica ovog principa treba da bude sigurnost od automatske dostupnosti podataka o ličnosti neodređenom broju lica. Posmatrajući iz druge perspektive, lice na koje se podaci odnose treba da odredi da li će svoje podatke podeliti sa većim određenim ili neodređenim krugom lica.

Primer implementacije principa ugrađene privatnosti je upotreba pseudonimizacije (zamene podataka o ličnosti podložne identifikaciji elementima koji se ne mogu ukazati o kom licu je reč) ili enkripcije (kodiranje poruka elektronske komunikacije tako da samo lice koje je poslalo poruku i primalac mogu jasno da je razumeju).[248]

Najviše pažnje poštovanju ovih principa treba da posvete oni koji proizvode računarske sisteme i programe, budući da se u ovim oblastima unapred mogu postaviti određena podešavanja kojima se utiče na privatnost građana. Takođe, i ostale industrije, poput robotske, avio, automobilske i svih drugih industrija – koje na neki način koriste podatke o građanima koji koriste njihove

[246] Čl. 25, st. 1 Opšte uredbe EU.

[247] Primer je naveden prema European Commission, "What does data protection „by design“ and „by default“ mean?", https:// ec. europa.eu / info / law / law-topic / data - protection / reform / rules - business - and - organisations / obligations / what - does - data - protection - design - and - default-mean_ en.

[248] Primer je naveden prema: *Ibidem.*

usluge – moraju da vode računa o ovim obavezama, kako bi izbegli plaćanje ogromnih kazni.

5.1.1.6. Vođenje evidencije o obradi podataka o ličnosti

U cilju zakonite i transparentne obrade, rukovalac ima dužnost vođenja evidencije aktivnosti obrade podataka o ličnosti.[249] Ista dužnost predviđena je i za predstavnika rukovaoca. Evidencija mora biti u pisanom obliku koji podrazumeva i elektronsku formu. Na zahtev nadzornog organa, rukovalac i obrađivač moraju omogućiti uvid u evidenciju. Na ovaj način, Opšta uredba EU teži da se kod obrade podataka obezbedi što više dokaza u slučaju zloupotrebe ili curenja podataka. Jedino praćenjem aktivnosti odgovornih lica može se proceniti da li eventualna greška u obradi ili zloupotreba imaju uzrok u nepažljivom postupanju odgovornog lica, odnosno rukovaoca ili predstavnika rukovaoca. Vođenje evidencije sa izloženim elementima omogućava pregled važnijih aktivnosti i činjenica u vezi sa obradom. Time se unapred stvaraju dokazi u slučaju nezakonitosti ili zloupotreba. Pomoću takvih dokaza može se ispitivati da li uzrok nastanka zloupotrebe leži u nekoj od aktivnosti rukovaoca ili se nalazi u uzroku na koji rukovalac nije mogao uticati.

Dužnost vođenja evidencije postoji za obrađivača i predstavnika obrađivača u vezi sa obradama koje se vrše u ime rukovaoca. Njihove evidencije sadrže slične elemente kao i evidencije rukovaoca, modifikovane u skladu sa posebnom ulogom i obavezama obrađivača. Vođenje evidencije može predstavljati veliki teret za rukovaoca ili obrađivača. Zbog toga je Opšta uredba EU predvidela određene uslove pod kojima se evidencije ne moraju voditi. Organizacije ili preduzeća imaju dužnost vođenja evidencija samo u slučaju kada imaju više od 250 zaposlenih. Čak i kada imaju manje od 250 zaposlenih, dužnost vođenja evidencije će postojati u slučaju postojanja verovatnoće da će obrada koju vrše, predstavljati visok stepen rizika za prava i slobode lica na koje se podaci odnose. Takođe, istu dužnost ima i obrađivač u slučaju kada obrada podataka nije povremena delatnost ili ako se obrada podataka odnosi na naročito osetljive podatke, odnosno podatke koji se odnose na krivičnu ili prekršajnu odgovornost.[250]

[249] Evidencija se sastoji od: imena i kontakt podataka rukovaoca, navedenih svrha obrade, opisa kategorija lica na koje se podaci odnose, kategorija korisnika kojima su podaci o ličnosti otkriveni, informacije o eventualnom prenosu podataka u treću državu ili međunarodnu organizaciju, rokova za brisanje podataka, kao i opšteg opisa tehničkih i organizacionih mera.

[250] Vid. čl. 30, st. 5 Opšte uredbe EU.

5.1.1.7. Mere za bezbednost podataka

Kao što je pomenuto, kako bi ostvarili potreban stepen zaštite podataka i samog procesa obrade, rukovaoci i obrađivači imaju dužnost primene različitih mera organizacionog, tehničkog i kadrovskog karaktera. Naravno, te mere moraju biti u skladu sa postojećim stanjem razvoja tehnologije, društvenim zahtevima, ali i mogućnostima rukovaoca ili obrađivača, što stvara potrebu za vaganjem većeg broja interesa prilikom uvođenja sistema bezbednosti. Opšta uredba EU predviđa nekoliko konkretnih mera kojima se ostvaruje veća bezbednost procesa obrade i samih podataka. Te mere se odnose na:

1. Pseudonimizaciju i enkripciju podataka,

2. Mogućnost trajne poverljivosti, celovitosti, dostupnosti i otpornosti sistema i usluga obrade,

3. Sposobnost ponovnog i blagovremenog uspostavljanja dostupnosti podataka o ličnosti i pristupa, u slučaju fizičkog ili tehničkog incidenta,

4. Obezbeđivanje postupka redovnog testiranja, ocenjivanja i procene delotvornosti tehničkih i organizacionih mera za postizanje bezbednosti obrade.[251]

Osim pomenutih, rukovaoci i obrađivači treba da imaju u vidu i one mere koje se implementiraju usvajanjem pravnih mehanizama u formu odobrenih kodeksa ponašanja, sertifikacije i određivanja lica ovlašćenog za zaštitu podataka.

5.1.1.8. Lice za zaštitu podataka (DPO)

Kao jedna od posebno značajnih mera zaštite podataka izdvaja se imenovanje lica za zaštitu podataka (eng. *Data Protection Officer – DPO*). Imenovanje ovog lica uglavnom je koncipirano na principu dobrovoljnosti, osim u pojedinim slučajevima, kada se ovo lice mora imenovati.[252] Lice mora posedovati odgovarajuće stručne i tehničke kvalifikacije koje ga preporučuju za obavljanje dužnosti. Kvalifikacije se odnose na poznavanje pravnih propisa i pravne prakse u

[251] Čl. 32, st. 1 Opšte uredbe EU.

[252] Obaveza imenovanja lica ovlašćenog za zaštitu podataka postoji:
1. Kada obradu vrši organ javne vlasti ili javno telo, osim sudova koji postupaju u okviru svoje sudske nadležnosti. 2. Kada se osnovne delatnosti rukovaoca ili obrađivača sastoje iz radnji obrade koje, zbog svoje prirode, obima ili svrha, zahtevaju redovno i sistematsko masovno praćenje lica na koje se podaci odnose. 3. Kada se osnovne delatnosti rukovaoca ili obrađivača sastoje iz masovne obrade posebnih kategorija podataka i podataka o ličnosti koji se odnose na krivičnu i prekršajnu odgovornost.

oblasti zaštite podataka.[253] Pomenute kvalifikacije služe za obavljanje više različitih poslova ovlašćenog lica za zaštitu podataka:

– Informisanje i savetovanje rukovaoca ili obrađivača i zaposlenih koji vrše obradu o njihovim obavezama po Opštoj uredbi EU i drugim odredbama prava EU ili prava države članice, u vezi sa zaštitom podataka,

– Praćenje usklađenosti poslovanja sa Opštom uredbom EU i drugim odredbama prava EU ili prava države članice o zaštiti podataka, kao i politikama rukovaoca ili obrađivača u vezi sa zaštitom podataka o ličnosti, uključujući i podelu odgovornosti, podizanje svesti i osposobljavanje osoblja koje učestvuje u radnjama obrade, i sa tim povezane revizije, pružanje saveta, kada je to traženo, u pogledu procene uticaja u vezi sa zaštitom podataka i praćenje izvršavanja obrade pri uvođenju novih tehnologija, saradnja sa nadzornim organom, delovanje kao kontakt osoba za nadzorni organ o pitanjima koja se tiču obrade, što uključuje i prethodne konsultacije, kao i savetovanje o drugim pitanjima.[254]

Kao što se može videti, lice za zaštitu podataka vrši internu pomoć kod analize zakonitosti i pravilnosti procesa obrade podataka o ličnosti. Njegov rad zasniva se na praćenju stanja stvari u zakonodavnoj, sudskoj i upravnoj praksi i konkretnoj primeni pravnih normi unutar organizacije koja obrađuje podatke. Zato možemo reći da ono predstavlja svojevrsni „interni nadzorni organ". Imenovanje ovog lica doprinosi sistemu zaštite na nivou same organizacije koja obrađuje podatke.

Obaveza imenovanja lica za zaštitu podataka predstavlja preventivni mehanizam usklađivanja poslovanja sa normama koje uređuju zaštitu podataka, što doprinosi lakšem, efikasnijem i bezbednijem radu rukovaoca i obrađivača. Naravno, kako bi uspešno obavljalo svoje dužnosti, lice za zaštitu podataka mora, u potpunosti i blagovremeno, da bude upoznato sa svim pitanjima koja se tiču zaštite podataka. Zato, ovo lice mora imati pristup svim podacima, unutrašnjim aktima i informacijama o načinu obrade i drugim postupcima u vezi sa obradom podataka. U prilog tome je postavljena i odredba Opšte uredbe EU koja navodi da lice za zaštitu podataka odgovara neposredno najvišem nivou rukovodstva rukovaoca ili obrađivača i da ne sme primati instrukcije u obavljanju svojih zadataka.[255]

---

[253] Ovo lice može da bude deo personala rukovalaca ili obrađivača podataka, ali može da bude i lice izvan organizacije, pri čemu se sa takvim licem zaključuje ugovor o delu. Kontakt podaci ovog lica moraju biti objavljeni, a ostali podaci od značaja za obavljanje njegove funkcije moraju biti dostavljeni nadzornom organu.

[254] Čl. 39, st. 1 Opšte uredbe EU.

[255] Čl. 38, st. 1 i 2 Opšte uredbe EU.

Na kraju, napominjemo da lice nije odgovorno za proces obrade podataka o ličnosti, već je i pored njegovog imenovanja, odgovoran rukovalac. Imenovanje ovog lica (kada je dobrovoljno) pokazatelj je želje za usklađivanjem i poštovanjem propisa u oblasti zaštite podataka, što i nadzorna tela, upravni organi i sudovi treba da imaju u vidu prilikom vršenja kontrolnih ovlašćenja.

5.1.1.9. Nezavisna nadzorna tela

U cilju pravilne i potpune primene, Opšta uredba EU predviđa obavezu država članica da ustanove jedan ili više organa koji će biti odgovorni za praćenje primene njenih odredaba. Reč je o nezavisnim nadzornim organima (eng. *Data Protection Authoritie – DPA*). Nezavisnost ovih tela obezbeđuje se izborom, finansijskim instrumentima i nespojivošću te delatnosti sa obavljanjem drugih poslova.[256] Opšta uredba EU dozvoljava da ova tela u okvirima država članica imenuju parlamenti, vlada, šefovi država ili nezavisno telo koje je pravom države članice ovlašćeno da vrši to imenovanje.

Kako bi nadzorni organ adekvatno obavljao svoju funkciju i vršio nadzor nad primenom propisa o zaštiti podataka o ličnosti, svaka od država članica mora obezbediti odgovarajuće uslove za rad nezavisnim telima. To znači da svaki nadzorni organ mora imati na raspolaganju ljudske, tehničke i finansijske resurse potrebne za uspešno obavljanje svojih dužnosti.

Pomenute odredbe su izuzetno važne, budući da nadzorni organi treba da indirektno štite lične podatke građana. Uz to, treba imati na umu da se većina podataka o ličnosti nalazi u elektronskoj formi, i to da se razmena podataka prevashodno odvija putem informaciono-komunikacionih uređaja. To znači da nadzorni organ mora biti opremljen odgovarajućim tehnološkim sredstvima i tehničkim znanjima kako bi mogao da obavlja nadzor i primenjuje svoja ovlašćenja. Zbog toga je od izuzetne važnosti poseban budžet ovih tela i njihova nezavisnost – organizaciona, funkcionalna i tehnička. Naravno, članstvo u odboru podrazumeva i određene obaveze, od kojih je najznačajnija dužnost čuvanje profesionalne tajne. Tokom trajanja mandata, kao i nakon prestanka funkcije u nadzornom odboru, članovi nadzornog odbora moraju čuvati kao profesionalnu tajnu, svaku poverljivu informaciju do koje su došli u obavljanju svoje funkcije. Dužnost čuvanja profesionalne tajne ima i drugo osoblje nadzornog organa.

Nezavisna nadzorna tela predstavljaju možda i najznačajniju instituciju u vezi sa zaštitom podataka u državama članicama. Ova institucija stara se o pravilnoj primeni odredbi vezanih za zaštitu podataka, vrši inspekcijska

[256] Čl. 52 Opšte uredbe EU.

ovlašćenja, stara se o podizanju svesti među građanima o značaju zaštite privatnosti, a uz to i pomaže građanima da ostvare svoja prava u ovoj razgranatoj oblasti. Njihova uloga je i savetodavna, budući da imaju ovlašćenje da preporučuju izmene i dopune u vezi sa propisima iz njihove nadležnosti. Takođe, oni su ovlašćeni i da sarađuju sa nezavisnim nadzornim telima ostalih država članica. Nezavisna nadzorna tela imaju u nadležnosti brojne zadatke, koje prate i značajna ovlašćenja.[257]

5.1.1.10. Evropski odbor za zaštitu podatka

Još jedno značajno telo koje je ustanovljeno na nivou čitave EU jeste Evropski odbor za zaštitu podataka (u daljem tekstu: Evropski odbor).[258] Evropski odbor predstavlja nezavisno evropsko telo koje se stara o pravilnoj primeni pravila u vezi sa zaštitom podataka o ličnosti na teritoriji čitave EU čije je sedište u Briselu u Belgiji. Pored toga, ovo telo treba da podstiče saradnju nezavisnih nadzornih organa država članica EU.

U sastav ovog tela ulaze rukovodeća lica nadzornog organa svake države članice, kao i Evropski supervizor za zaštitu podataka, koji između sebe biraju predsednika i dva zamenika. Radi uspešnog obavljanja poslova Evropski odbor ima i Sekretarijat koga obezbeđuje Evropski supervizor za zaštitu podataka. Kao osnovne zadatke i dužnosti ovog tela navodimo davanje opštih smernica u cilju razumevanja legislative u oblasti zaštite podataka, savetovanje Evropske komisije o pitanjima iz ove oblasti i potrebi izmene normativnih akata, izdavanje smernica, preporuka i primera najbolje prakse, promovisanje saradnje, donošenje odluka u vezi sa prekograničnom zaštitom podataka, itd.[259]

5.1.1.11. Pravna sredstva, odgovornost i sankcije

Jedan od najvažnijih elemenata svakog pravnog sistema jeste omogućavanje mehanizama zaštite u slučaju štete ili nezakonitog delovanja prema ličnom dobru pojedinca. Takav je slučaj i u sistemu zaštite podataka EU koji predviđa pravo na pravno sredstvo, prigovor ili žalbu kada je fizičkom licu povređeno pravo, sloboda ili pravni interes. Povredu normi Opšte uredbe EU prate izuzetno visoke (novčane) sankcije koje imaju za cilj da dodatno motivišu rukovaoce, obrađivače i sva druga lica da poštuju njene odredbe.

[257] Više o ovlašćenjima i zadacima ovih tela vid. čl. 57 i 58 Opšte uredbe EU.
[258] Evropski odbor za zaštitu podataka, https://edpb.europa.eu/edpb_en.
[259] Vid. čl. 70 Opšte uredbe EU.

Jedno od osnovnih prava u vezi sa zaštitom podataka o ličnosti jeste pravo na pravno sredstvo. Pravnim sredstvima omogućava se građanima da sopstvenom inicijativom pokrenu mehanizme zaštite u vezi sa svojim podacima o ličnosti.

Možemo razlikovati tri vrste pravnih sredstava koje poznaje Opšta uredba EU. Ova pravna sredstva se razlikuju u zavisnosti od toga kom licu se izjavljuju. U tom smislu, Opšta uredba EU poznaje pravo na pritužbu nadzornom organu, pravo na delotvorno pravno sredstvo protiv odluke nadzornog organa i pravo na pravno sredstvo protiv rukovaoca ili obrađivača. Pored toga, svako lice koje je pretrpelo materijalnu ili nematerijalnu štetu zbog kršenja Opšte uredbe EU ima pravo na njenu naknadu.

Pravom na pritužbu nadzornom organu omogućava se podnošenje pritužbe nezavisnom nadzornom telu u državi uobičajenog boravišta, radnog mesta ili mesta kršenja prava, ukoliko to lice smatra da se obradom podataka o ličnosti krše pravna pravila Opšte uredbe EU.[260] Pravom na pravno sredstvo protiv nadzornog organa omogućava se pravno relevantno iskazivanje nezadovoljstva protiv pravno obavezujuće odluke nadzornog organa, kada se ta odluka odnosi na lice koje ulaže sredstvo.[261] Ono se odnosi i na nepostupanje ovog organa u, zakonom ili Opštom uredbom EU, predviđenim rokovima. Lice na koje se podaci odnose ima pravo na delotvorno pravno sredstvo protiv rukovaoca ili obrađivača, ukoliko smatra da su njegova prava iz opšte uredbe EU prekršena obradom podataka o ličnosti koja je vršena suprotno odredbama Opšte uredbe EU.[262]

Ulaganjem pravnog sredstva u bilo kojem od navedenih slučajeva, ne dovodi se u pitanje upotreba drugih upravnih ili drugih pravnih sredstava koje omogućava pravo države članice. Uređena je i sudska nadležnost u vezi sa pomenutim sredstvima. U postupku protiv nadzornog organa nadležan će biti sud u kojoj nadzorni organ ima sedište, a u postupku protiv rukovaoca ili obrađivača biće nadležan sud sedišta rukovaoca, odnosno obrađivača. Omogućena je i alternativna nadležnost prema sudu države članice u kojoj lice na koje se podaci odnose ima uobičajeno boravište, osim ukoliko je obrađivač organ javne vlasti i primenjuje javna ovlašćenja, gde će jedini nadležni sud biti sud sedišta tog organa.[263]

[260] Čl. 77 Opšte uredbe EU.
[261] Čl. 78 Opšte uredbe EU.
[262] Čl. 79 Opšte uredbe EU.
[263] Čl. 79, st. 2 Opšte uredbe EU.

Mogućnost naknade štete zbog kršenja Opšte uredbe EU proizlazi iz načela odgovornosti. Ostvarivanje prava na naknadu štete može se vršiti i preko organizacija, tela ili udruženja neprofitnog karaktera, čija je svrha zaštita javnog i privatnog interesa u konkretnom slučaju. Ta tela, organizacije ili udruženja, osnivaju se u skladu sa pravom države članice i mogu podnositi pritužbe u ime i za račun lica koje ih na to ovlasti, ukoliko to čine bez namere ostvarivanja profita.[264] Na naknadu štete primenjuju se pravila odštetnog prava država članica.

Kao što smo pomenuli, jedna od najupečatljivijih odluka Opšte uredbe EU jesu ogromne zaprećene kazne. Za izricanje takozvanih administrativnih kazni zaduženi su nadzorni organi država članica. Prilikom određivanja kazni oni moraju uzeti u obzir sve okolnosti, poput svrhe obrade, vrste i količine prikupljenih i obrađivanih podataka, primenjenih mera zaštite, načina saznanja, postupanja u cilju saniranja štete i druge.[265]

U slučaju povrede obaveze rukovaoca i obrađivača, povrede obaveza u vezi sa sertifikatima i sertifikacionim telima, kao i povrede obaveza postavljenim od strane nadzornog organa u vezi sa kodeksom ponašanja, nadzorna tela mogu da izreknu kazne u iznosu do 10.000.000 EUR, odnosno kada je reč o pravnim licima do 2% ukupnog godišnjeg prometa, i to u svetu, za prethodnu finansijsku godinu. Napominjemo da će se primeniti onaj iznos koji je veći.

Ukoliko je došlo do povrede osnovnih načela obrade ili pristanka, prava lica na koje se podaci odnose, povrede pravila o prenosu podataka u strane države ili međunarodne organizacije ili povrede neke od obaveze koju uvode države članice, mogu se izreći kazne u iznosu do 20.000.000 EUR, odnosno kada je reč o pravnim licima do 4% ukupnog godišnjeg prometa, i to u svetu, za prethodnu finansijsku godinu, u zavisnosti od toga koji je iznos veći.[266]

Reč je zaista o ogromnim kaznama koje imaju jako preventivno dejstvo i podstiču rukovaoce i obrađivače da se usaglase sa pravilima Opšte uredbe EU, ali i sa zakonodavstvom države u kojoj obavljaju delatnosti. Proces usklađivanja još uvek traje i trajaće duže vreme, u čemu će veliku pomoć pružiti upravna i sudska praksa koja se ustanovljava na nivou država članica.

[264] Čl. 80 Opšte uredbe EU.
[265] Čl. 83, st. 2 Opšte uredbe EU.
[266] Čl. 83, st. 4 i 6 Opšte uredbe EU.

5.1.1.12. Prenos podataka u strane države ili međunarodne organizacije

Opšta uredba EU uređuje i pitanje prenosa podataka o ličnosti u državu koja nije članica EU ili međunarodnu organizaciju. Prenos se mora vršiti tako da rukovalac i obrađivač postupaju u skladu sa pravilima o prenosu podataka predviđenim Uredbom.[267] Uređivanjem pravila prenosa, Opšta uredba EU pokušava da izbegne situaciju u kojoj se ne primenjuju ostvareni pravni standardi u ovoj oblasti. Ova pravila moraju se poštovati i prilikom naknadnog prenošenja podataka iz treće zemlje ili organizacije.

Značajnu ulogu u prenosu podataka ima Komisija EU. Komisija odlučuje o tome da li treća zemlja, teritorija ili određeni sektor u okviru ovih entiteta, pruža sigurnost u pogledu nivoa zaštite podataka o ličnosti. Posebno odobrenje Komisije nije potrebno, ako je odlučila da druga strana van EU pruža adekvatan sistem pravne zaštite.

U tu svrhu, Opšta uredba EU predviđa kriterijume koje Komisija uzima u obzir prilikom procene da li postoji adekvatan nivo zaštite. To su opšti principi vladavine prava, nivoa zaštite i poštovanja ljudskih prava i osnovnih sloboda, kao i stanje propisa u relevantnim oblastima, efikasna i delotvorna pravila upravnog i sudskog postupka u vezi sa zaštitom podataka. Još jedan važan element je postojanje delotvornih nezavisnih nadzornih organa. Takođe, Komisija uzima u obzir i međunarodne obaveze koje treća država ili međunarodna organizacija ima na osnovu prihvaćenih međunarodnih ugovora. Komisija donosi akt o sprovođenju (odluku o adekvatnosti) kojim odlučuje o ispunjenosti postavljenih kriterijuma.

Stav Komisije o adekvatnosti sistema zaštite u državi van EU ili međunarodnoj organizaciji, revidira se na period koji nije duži od četiri godine. Naravno, ukoliko se dođe do saznanja da treća država ili međunarodna organizacija ne pruža adekvatan nivo pravne zaštite, Komisija može staviti van snage ili suspendovati odluku o ispunjenosti kriterijuma druge strane. Svoje odluke o kriterijumima, listi zemalja i međunarodnih organizacija koje ispunjavaju kriterijume, Komisija objavljuje u *Službenom listu* Evropske Unije i na svojoj internet prezentaciji.

Druga situacija se javlja kada nije doneta odluka o adekvatnosti prenosa. U tom slučaju rukovalac ili obrađivač koji imaju sedište u EU mogu da prenesu lične podatke trećoj zemlji ili međunarodnoj organizacije jedino ukoliko su primenili odgovarajuće mere zaštite takvog prenosa i ukoliko lica na koja se

[267] Čl. 44 Opšte uredbe EU.

odnose podaci imaju na raspolaganju odgovarajuća prava i sredstva pravne zaštite. Odgovarajuće zaštitne mere obezbeđuju se putem pravno obavezujućih i izvršnih instrumenata javne vlasti, obavezujućim korporativnim pravilima, standardnim klauzulama o zaštiti podataka, odobrenim kodeksima ponašanja i odobrenim mehanizmima sertifikacije.[268]

Uz posebno ovlašćenje nadzornog organa, posebne mere zaštite mogu biti regulisane ugovorom između rukovaoca ili obrađivača i korisnika podataka o ličnosti u trećoj zemlji ili organizaciji, kao i ugovorima (upravnim sporazumima) između organa javne vlasti država koje učestvuju u razmeni podataka o ličnosti.

Pored toga, Uredba predviđa i određene slučajeve prenosa podataka kada ne postoji akt o adekvatnosti razmene podataka ili odgovarajuće zaštitne mere rukovaoca ili obrađivača. U tim slučajevima, prenos podataka se može vršiti samo pod nekim od predviđenih uslova i situacija:

- Lice na koje se podaci odnose je izričito pristalo na predloženi prenos nakon što je upoznato sa mogućim rizicima takvih prenosa za lica na koja se podaci odnose zbog nepostojanja odluke o adekvatnosti i odgovarajućih mera,
- Prenos je potreban za izvršenje ugovora između lica na koje se podaci odnose i rukovaoca ili primenu predugovornih obaveza na zahtev lica na koje se podaci odnose,
- Prenos je potreban radi sklapanja ili izvršenja ugovora sklopljenog u interesu lica na koje se podaci odnose između rukovaoca i drugog fizičkog ili pravnog lica,
- Prenos je potreban za ostvarivanje ili odbranu od pravnih zahteva,
- Prenos je potreban za zaštitu važnih životnih interesa lica na koje se podaci odnose ili drugih lica ako lice na koje se podaci odnose fizički ili pravno nije sposoban da dâ pristanak,
- Prenos se vrši iz baza podataka koji prema pravu Unije ili pravu države članice služi za pružanje informacija javnosti i koji je dostupan za uvid javnosti ili bilo kom licu koje može da dokaže postojanje legitimnog interesa, ali samo ako su ispunjeni uslovi propisani pravom EU ili pravom države članice.[269]

[268] Čl. 46, st. 2 Opšte uredbe EU.
[269] Čl. 49, st. 1 Opšte uredbe EU.

5.1.1.13 Posebni slučajevi obrade

U zavisnosti od toga koja se vrsta podataka o ličnosti obrađuje može se napraviti razlika između pojedinih vrsta obrade. Tako se javljaju i posebni slučajevi obrade koji uživaju specijalno normativno uređenje. Opšta uredba EU navodi da se posebne situacije obrade podataka o ličnosti tiču slobode izražavanja i informisanja, pristupa dokumentima u posedu organa javne vlasti, obrade nacionalnog identifikacionog broja, obrade podataka u vezi sa radnim odnosima, obrade u istorijske, naučne ili statističke svrhe i obrade podataka verskih udruženja.

5.1.1.14. Zaključak

Pored pomenutih materijalnih odredbi, Opšta uredba EU sadrži i nekoliko završnih procesnih odredbi. U njima se obrazlaže osvrt na druge propise, kao što je stavljanje Direktive 95/46EZ van snage i načini primene prethodno zaključenih međunarodnih sporazuma u ovoj oblasti. Predviđena je obaveza da se drugi akti EU preispitaju i usklade prema novoustanovljenim pravilima. Kao element koji govori u prilog tezi da će se ovaj propis primenjivati, duže vreme navodimo i obavezu Komisije EU da na svake četiri godine podnosi izveštaj Evropskom parlamentu i Savetu o oceni i preispitivanju ove uredbe.[270]

Značaj Opšte uredbe EU je izuzetno veliki. Ustanovljena su pravila koja će važiti na čitavoj teritoriji EU koja obuhvata preko 300 miliona stanovnika, a pored toga ona ima uticaj i na države kandidate za članstvo, kao i na ostale države i međunarodne organizacije koje sarađuju sa EU. Zato možemo reći da je Opšta uredba EU po svom značaju premašila okvire EU, što znači da ona ima svetski, pa i istorijski značaj.

Predviđena pravila nude građanima mogućnost da zaštite svoja prava u vezi sa podacima o ličnosti koji predstavljaju jedno od najvažnijih sredstava rada i poslovanja u ovom veku. Ogromne zaprećene, ali i određene kazne govore da će se u godinama koje dolaze dosta raditi na poštovanju pravila Opšte uredbe EU, što će podići nivo zagarantovanih ljudskih prava, ali istovremeno pomoći i u punjenju budžeta država članica EU.

[270] Čl. 97 Opšte uredbe EU.

5.1.2. Direktiva o privatnosti i elektronskim komunikacijama i Predlog Uredbe o privatnosti i elektronskim komunikacijama

U modernim društvima podaci o ličnosti prevashodno, prirodno se dovode u vezu sa digitalnim uređajima i informaciono-komunikacionim tehnologijama. Sve ove pojave zajedno kreiraju novo, digitalno, tržište koje okuplja značajna društvena i materijalna sredstva. U takvim okolnostima svakodnevno se povećava broj fizičkih lica koja učestvuju na tom tržištu. Imajući to u vidu, potrebno je pružiti sigurnost fizičkim licima koja na njemu učestvuju, što se posebno odnosi na pravo privatnosti i zaštitu podataka o ličnosti, kao „prava modernih tehnologija". Iz tog razloga je, na nivou EU, 2002. godine usvojena Direktiva 2002/58/EZ Evropskog parlamenta i Saveta o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija – *Direktiva o privatnosti i elektronskim komunikacijama (u daljem tekstu: Direktiva o e-privatnosti*).[271]

Osnovni cilj ove Direktive o e-privatnosti jeste da uskladi zakonodavstva država članica po pitanju poštovanja prava na privatnost u oblasti elektronskih komunikacija. Direktiva o e-privatnosti teži da stvori sigurno pravno okruženje za slobodan prenos podataka i elektronske komunikacione opreme i usluga na teritoriji čitave EU. Ona se primenjuje na obradu podataka o ličnosti za koju se koriste javno dostupne elektronske komunikacione mreže u EU.[272] Ovim propisom predviđena je obaveza pružaoca elektronskih komunikacionih usluga da predvide i implementiraju odgovarajuće tehničke i organizacione mere u cilju zaštite bezbedne komunikacije. Uz to, predviđena je i obaveza obaveštavanja korisnika usluga o opasnosti od narušavanja bezbednosti komunikacija i mreže, što predstavlja pojavni oblik principa transparentnosti. Podaci koji se odnose na pretplatnike i korisnike komunikacionih mreža moraju se anonimizirati ili obrisati kada prestane svrha zbog koje se obrađuju, odnosno kada više nisu potrebni u cilju ostvarivanja komunikacije.

Zanimljivo je pomenuti da *u svrhu reklamiranja (marketinga) elektronskih komunikacija ili pružanja usluge sa posebnom tarifom*, pružalac usluge može obrađivati podatke pretplatnika i korisnika u vremenskom obimu

[271] Direktiva 2002/58/EZ Evropskog parlamenta i Saveta o obradi podataka o ličnosti i zaštiti privatnosti u sektoru elektronskih komunikacija, poznatija kao Direktiva o privatnosti i elektronskim komunikacijama, „Sl. list EU", br. L 201/37, od 12. 07. 2002. god., https://eur-lex.europa.eu/legal-content/hr/ALL/?uri=CELEX:32002L0058.

[272] Čl. 3 Direktive e-privatnost.

koji je nužan za ostvarivanje reklamiranja (marketinga), ali samo ako postoji pristanak lica čiji se podaci obrađuju.[273]

Osim za pružaoce usluga, predviđene su i obaveze za države članice. Države imaju dužnost da zabrane svim licima koja nisu korisnici da slušaju, prisluškuju, čuvaju ili presreću komunikacije i podatke iz takvih komunikacija, osim kada za takve radnje postoji poseban zakonski osnov. Ipak, ovo se ne odnosi na zakonski dopušteno snimanje komunikacije u cilju ostvarivanja dokaza o poslovnim transakcijama i komunikacijama, što je od značaja za privredne subjekte i omogućavanje nesmetanog poslovanja. Uz to, države članice treba da osiguraju mogućnost da svaki pretplatnik može da spreči automatsko prosleđivanje poziva na njegov terminal koji vrši treće lice.[274]

` Pretplatnici i korisnici imaju pravo na detaljno obrazložen račun za korišćenje komunikacijskih usluga, što osnažuje njihovu slabiju poziciju u odnosu na pružaoce usluga.

Predviđena je i obaveza *pružaoca usluga da ponudi licu koje poziva da jednostavno i bez naknade spreči prikazivanje svog broja prilikom poziva*, kada postoji ponuda za takvu opciju. Isto tako, pozvani pretplatnik mora biti u mogućnosti da na istovetan način odbije pozive u situaciji kada se ne prikazuje broj lica koje poziva.

Značajne su i one odredbe u vezi sa *GPS lokacijom korisnika usluga*. Podaci o takvim lokacijama mogu se obraditi samo nakon što su anonimizirani ili kada postoji pristanak korisnika, pri čemu ta lica moraju da budu u mogućnosti da pristanak povuku bez većih poteškoća.

Posebna pažnja posvećena je *neželjenim vidovima komunikacije*. Upotreba automatskih sistema pozivanja, bez intervencija čoveka, poput govornih automata, faksova ili elektronske pošte, u svrhu direktnog marketinga, dopuštena je samo kod onih korisnika koji su prethodno dali pristanak. Na taj način još jednom je ukazano na značaj instituta pristanaka u oblasti zaštite podataka. *Zabranjena je praksa slanja elektronske pošte u svrhu direktnog marketinga kada nije poznat identitet pošiljaoca*, odnosno bez adekvatne adrese na koju primalac može da pošalje zahtev za prestanak takve komunikacije.[275]

Protekom vremena, razvojem digitalnih usluga i mogućnosti i usvajanjem Opšte uredbe EU – javila se potreba za revizijom Direktive o e-privatnosti. Tokom 2017. godine sačinjen je *Predlog Uredbe Evropskog parlamenta i Saveta o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim*

[273] Čl. 6, st. 3 Direktive e-privatnosti.
[274] Čl. 11 Direktive o e-privatnosti.
[275] Vid. čl. 13 Direktive o e-privatnosti.

komunikacijama – Uredba o privatnosti i elektronskim komunikacijama (u daljem tekstu: Uredba o e-privatnosti), koja bi stavila van snage Direktivu 2002/58/EZ.[276] Na veliki broj pitanja ove Uredbe primenjivaće se odredbe Opšte uredbe EU, što dodatno potvrđuje značaj tog osnovnog propisa iz koga će se stvarati posebne oblasti zaštite podataka.

Uredba o e-privatnosti će na opšti način, u svim državama članicama EU, predvideti pravila u vezi sa zaštitom osnovnih prava i sloboda fizičkih, ali i pravnih lica prilikom pružanja i korišćenja elektronskih komunikacionih usluga, a posebno prava na poštovanje privatnog života, komunikacije i zaštite fizičkih lica kod obrade podataka o ličnosti.[277] Pored toga, ona teži da ostvari slobodno kretanje elektronskih podataka u vezi sa komunikacijom unutar EU, uz naglasak na poštovanje prava privatnosti. Uviđamo da će Uredba o e-privatnosti, za razliku od Opšte uredbe EU, imati širi domašaj budući da pruža zaštitu i pravnim licima, pri čemu se ne odnosi isključivo na podatke o ličnosti, već i na druge podatke iz komunikacije. Njeno teritorijalno važenje prostire se na pružanje elektronskih komunikacionih usluga krajnjim korisnicima u EU, kao i na upotrebu takvih usluga i zaštitu informacija u vezi sa opremom takvih korisnika. Ukoliko pružalac usluge nema sedište u okviru EU, on će morati da imenuje predstavnika na njenoj teritoriji.

Jedan od osnovnih postulata jeste poverljivost podataka koji proizlaze iz elektronskih komunikacija. Sledeći takvo pravilo, zabranjeno je svako zadiranje u podatke iz takve komunikacije, osim u posebnim slučajevima, kao što je nužnost prenosa komunikacije, odnosno nužnost održavanja sistema bezbednosti mreže. Predviđeni su i slučajevi u kojima se mogu obrađivati metapodaci elektronskih komunikacija, što predstavlja novinu.[278]

Iz Direktive o e-privatnosti ostala je zabrana prikupljanja i obaveza brisanja ili anonimiziranja podataka o ličnosti prikupljenih u okviru elektronske komunikacije. Takođe, zabranjena je upotreba kapaciteta terminalne opreme za obradu i prikupljanje informacija iz ovakve opreme krajnjih korisnika, što podrazumeva i informacije o softveru i hardveru, osim u posebnim slučajevima (nužnosti, pristanka, itd.).[279] Na institut pristanka primenjuju se pravila Opšte uredbe EU.

---

[276] Predlog Uredbe Evropskog parlamenta i Saveta o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama – Uredba o privatnosti i elektronskim komunikacijama (u daljem tekstu: Uredba o e-privatnosti)., https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A52017PC0010.

[277] Čl. 1, st. 1 Predloga Uredbe o e-privatnosti.

[278] Vid. čl. 6, st. 2 Predloga Uredbe o e-privatnosti.

[279] Čl. 8 Predloga Uredbe o e-privatnosti.

Poseban deo Uredbe o e-privatnosti posvećen je pravima fizičkih i pravnih lica u vezi sa elektronskim komunikacijama. Tako se promovišu prava u vezi sa prikazivanjem i ograničenjem prikaza pozivatelja i broja pozvane linije, blokiranje dolaznih poziva, prava fizičkih lica na davanje saglasnosti u vezi sa upisom u javno dostupne imenike, davanje informacija korisnicima o otkrivenim sigurnosnim rizicima itd. Iz Direktive o e-privatnosti preuzete su odredbe o neželjenim elektronskim komunikacijama u svrhe direktnog marketinga. Nezavisna nadzorna tela država članica, kao i Evropski odbor za zaštitu podataka imaju obavezu u vezi poštovanja prava vezanih za podatke o ličnosti i po ovom propisu, što je posebno naglašeno.

Pravna sredstva, odgovornosti i sankcije su istovetno uređeni kao u Opštoj uredbi EU, što podrazumeva i velike zaprećene kazne u iznosima 10.000.000, odnosno 20.000.000 eura, ili 2%, tj. 4% ukupnog godišnjeg prometa na svetskom nivou. To govori o ozbiljnosti namere za primenu ovog propisa.

Svoje mišljenje na tekst predloga Uredbe o e-privatnosti dao je i Evropski supervizor za zaštitu podataka, koji navodi da „bez Uredbe o e-privatnosti okvir EU koji se odnosi na zaštitu privatnosti i podataka ne bi bio potpun. Iako Opšta uredba EU predstavlja veliko ostvarenje, potrebno nam je posebno pravno sredstvo kojim ćemo zaštiti pravo na privatni život, zajamčeno čl. 7. Povelje EU, čiji je osnovnim element poverljivost komunikacija“.[280]

Na osnovu svega navedenog, možemo zaključiti da Uredba o e-privatnosti predstavlja svojevrsan „poseban propis“ u oblasti zaštite podataka o ličnosti, koji dodatno utemeljuje pojedina prava građana i propisuje pravila u vezi sa elektronskim komunikacijama, bez kojih se moderni život ne može zamisliti. Osim toga, značaj ove Uredbe je i u tome što se i posle Opšte uredbe EU radi na zaštiti podataka o ličnosti i ostvarivanju prava privatnosti u okvirima EU.

5.1.3. Policijska direktiva

Imajući u vidu specifičan položaj države i njenih bezbednosnih organa u odnosu prema podacima o ličnosti, jasno je da se sistem zaštite podataka u ovoj oblasti razlikuje u odnosu na opšti režim. Reč je o tome da organi bezbednosti obavljaju zahtevne zadatke poput zaštite državnih granica, zaštite bezbednosti građana i institucija, gonjenja učinilaca krivičinih dela, i drugo. Prilikom obavljanja ovih poslova neretko se kao sredstvo rada koriste podaci o ličnosti.

[280] Sažetak Mišljenja Evropskog supervizora za zaštitu podataka o predlogu Uredbe o e-privatnosti, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri= CELEX%3A52017XX0720 %2801%29.

U ovoj situaciji javlja se potreba za omogućavanjem normalnog rada i funkcionisanja bezbednosnih organa, što obezbeđuje javnu bezbednost i sigurnost države i građana, a sa druge strane postoji potreba za zaštitom podataka građana. Zbog toga, posebna pažnja posvećuje se zaštiti podataka u sektoru bezbednosti koji čini posebni podsistem zaštite. Na teritoriji EU usvojena je direktiva koja se odnosi na pomenuti podsistem. Reč je o *Direktivi 2016/80 Evropskog parlamenta i Veća o zaštiti pojedinaca u vezi sa obradom podataka o ličnosti od strane nadležnih organa u cilju sprečavanja, istrage, otkrivanja ili gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija i o slobodnom kretanju takvih podataka, poznatija kao „Policijska direktiva" (u daljem tekstu: Policijska direktiva), koja je usvojena 27. 04. 2016. god*.[281] Direktivom je van snage stavljena Okvirna odluka Veća 2008/977/PUP.

Zajedno sa Opštom uredbom EU, ova Direktiva predstavlja deo nove normative u oblasti zaštite podataka, pa su oba propisa započela sa primenom u isto vreme – maja 2018. godine. U značajnom broju odredbi Policijska direktiva se oslanja na principe i institute predviđene Opštom uredbom EU. Ipak, iz pomenutih razloga, Policijska direktiva predviđa značajan broj odredbi kojima se odstupa od opšteg sistema zaštite podataka koji je predviđen Opštom uredbom EU. Kako je ovaj rad posvećen osnovama sistema zaštite podataka, a Policijska direktiva uvodi poseban podsistem zaštite u oblast bezbednosti, pomenućemo samo neke od značajnijih elemenata.

Predmet Policijske direktive predstavljaju pravila u vezi sa zaštitom fizičkih lica u odnosu na obradu podataka o ličnosti koje vrše nadležni organi u cilju sprečavanja, istrage, otkrivanja ili gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija, što podrazumeva i zaštitu od pretnji javnoj bezbednosti i sprečavanje ovakvih krivičnih dela.[282] Na osnovu odredaba Policijske direktive prevashodno će postupati ministarstva unutrašnjih poslova, tužilaštva, krivični sudovi, kao i zavodi za izvršenje krivičnih sankcija. Važno je napomenuti da Opšta uredba EU važi i za ove subjekte kada ne obavljaju neki od pomenutih „bezbednosnih zadataka", što znači da kada obavljaju neke druge, primera radi upravne poslove, oni će morati da primenjuju Opštu uredbu EU.

Pojedine odredbe iz Policijske direktive manje štite prava građana i omogućavaju veći prostor za primenu slobodne (diskrecione) ocene u odnosu na

[281] Direktiva 2016/80 Evropskog parlamenta i Veća o zaštiti pojedinaca u vezi sa obradom ličnih podataka od strane nadležnih organa u cilju sprečavanja, istrage, otkrivanja ili gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija i o slobodnom kretanju takvih podataka, „Sl. list EU" L 119/89 od 04.05.2016. god.

[282] Vid. čl. 1 Policijske direktive.

slične institute predviđene Opštom uredbom EU. Reč je o tome da ne važi u svakoj situaciji princip transparentnosti obrade, da je ublažena obaveza korišćenja minimuma podataka o ličnosti, da se prava lica na koje se podaci odnose mogu u značajnoj meri ograničiti, itd.[283] Osim toga, Policijska direktiva predviđa i nekoliko posebnih instituta. Reč je obavezi kategorizacije lica čiji se podaci obrađuju, što važi i za njihove podatke, obavezi vođenja evidencije o svakom pojedinačnom pristupu podacima i njihovoj obradi, obavezi utvrđivanja rokova čuvanja podataka, kao i prenošenju podataka u strane države ili međunarodne organizacije.[284]

Naravno, kao i druge direktive, Policijska direktiva mora da bude implementirana u nacionalna zakonodavstva država članica EU. To znači da će svaka država doneti poseban zakon koji uređuje ovu specifičnu oblast.

5.1.4. Konvencija Saveta Evrope br. 108. o zaštiti lica u pogledu automatske obrade podataka o ličnosti

Jedan od istorijski najznačajnijih međunarodnih dokumenata i prvi obavezujući međunarodni ugovor u oblasti zaštite podataka usvojen je pod okriljem Saveta Evrope. Reč je o *Konvenciji br. 108 o zaštiti lica u odnosu na automatsku obradu podataka (Konvencija 108*)[285] koja je usvojena u Strazburu 28. januara 1981. godine. Nešto kasnije, 2001. godine, u Strazburu je usvojen i *Dodatni protokol uz Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka, u vezi sa nadzornim organima i prekograničnim protokom podataka*.

Osnovni cilj usvajanja Konvencije 108 bio je da se na teritoriji svake države ugovornice garantuje svim fizičkim licima, nezavisno od njihove nacionalne pripadnosti ili mesta stanovanja, poštovanje osnovnih prava i sloboda, a posebno prava na privatnost u pogledu automatske obrade podataka o ličnosti. Drugim rečima, cilj je bio zaštititi podatke o ličnosti u novonastalim uslovima informaciono-komunikacionih tehnologija i interneta. Automatska obrada podrazumeva korišćenje računarskih i drugih tehnologija koje su u mogućnosti da

[283] Jelena Pejić, Šta je „Policijska direktiva Evropske unije“? – Kako organi sprovođenja zakona (treba da) štite lične podatke, Beogradski centar za bezbednosnu politiku, 2019, str. 4.

[284] *Ibidem*.

[285] Konvencija Saveta Evrope o zaštiti lica u odnosu na automatsku obradu podataka (Konvencija 108), Savet Evrope, Strazbur, 1981., https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.

same ili po nalogu korisnika, vrše aktivnosti obrade podataka, nezavisno od toga da li se u ulozi rukovaoca nalaze fizička lica, pravna lica ili organi javne vlasti.

Automatska obrada podataka o ličnosti, prema Konvenciji, zasniva se na određenim principima. Podaci o ličnosti moraju se prikupljati i obrađivati na legalan i legitiman način. Prikupljanje i obrada podataka mora se zasnivati na određenoj svrsi, a prikupljeni podaci moraju biti primereni, relevantni i srazmerni u odnosu na svrhu obrade. Uz to, podaci o ličnosti moraju biti tačni i čuvani onoliko vremena koliko je neophodno da se ispuni svrha zbog koje su prikupljeni.[286]

Imajući u vidu da se radi o međunarodnoj konvenciji ostavljen je veliki broj „otvorenih klauzula" koje omogućavaju državama potpisnicama da same pronađu modalitet ostvarivanja pojedinih instituta. Tako je dozvoljena obrada posebnih kategorija podataka o ličnosti (rasno poreklo, versko ubeđenje, zdravstveno stanje, itd.) ukoliko nacionalna zakonodavstva predvide odgovarajuće mehanizme zaštite. To znači da države članice imaju obavezu da predvide adekvatne mere u cilju zaštite podataka. Uočavamo i začetke pojedinih prava građana u pogledu prava na pristup podacima, prava na ispravku, pravo na dobijanje obaveštenja o obradi, itd.[287] Svaka strana ugovornica preuzela je obavezu da predvidi odgovarajuća pravna sredstva, ali i sankcije za slučaj kršenja osnovnih načela zaštite i pojedinih rešenja.[288]

Posebno poglavlje u okviru Konvencije 108 posvećeno je prekograničnoj razmeni podataka o ličnosti. Ni jedna strana ugovornica nema pravo da zabrani ili uslovi specijalnim dozvolama prekogranični protok podataka o ličnosti na teritoriju drugih država, osim u slučaju primene posebnih pravila u vezi sa pojedinim kategorijama podataka. Na ovom polju važna je i međusobna pomoć država članica za koju su nadležni organi koje svaka država imenuje (obično su to nezavisna nadzorna tela – poverenici, agencije, itd.). Ovi organi imaju dužnost da razmenjuju podatke o pravnom sistemu i praksi u okviru svojih država, što doprinosi ujednačavanju celokupne prakse u vezi sa zaštitom podataka na teritoriji Saveta Evrope i šire.

Ustanovljen je i *Savetodavni komitet* koji čine po jedan predstavnik i njegov zamenik svake države članice. Ovaj komitet je ustanovljen s ciljem davanja predloga radi olakšanja ili poboljšanja primene Konvencije i davanja mišljenja o predlozima amandmana ili primeni određenog člana Konvencije.

---

[286] Nikola Protrka, „Normativna uređenost zaštite osnovnih podataka u Republici Hrvatskoj", *Policijska sigurnost*, god. 22, br. 4, Zagreb 2002, str. 513.

[287] Čl. 8 Konvencije 108.

[288] Čl. 10 Konvencije 108.

Poslednje izmena Konvencije 108 učinjena je *Protokolom 223* kojim se menja Konvencija o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti, koji je usvojen 18. maja 2018. godine u Strazburu.[289] Protokol je usvojen kao odgovor na razvoj tehnologije i nove informacione izazove. „Najvažnije novine sadržane u Protokolu odnose se na zahteve u pogledu načela proporcionalnosti i zakonitosti, kao i transparentnosti obrade, zatim proširenja kategorije osetljivih podataka na genetske i biometrijske podatke, propisivanja obaveza prijavljivanja povrede podataka, ali i nova prava lica u kontekstu upotrebe algoritama u donošenju odluka, a koja su posebno značajna u vezi sa razvojem veštačke inteligencije".[290]

Iako predstavlja izvor prava u Republici Srbiji, kao potvrđeni međunarodni ugovor, Konvencija 108 i protokoli danas imaju nešto manji značaj. Naime, oni su bili značajniji u doba kada su usvojeni, budući da države nisu uređivale oblast zaštite podataka. Danas, u Republici Srbiji i drugim državama Saveta Evrope, postoje ustanovljeni sistemi zaštite podataka i regulativa koja uređuju daleko veći broj pitanja nego što to čini Konvencija.

Ipak, Konvencija 108 ima istorijski značaj kao prvi obavezujući međunarodni ugovor u ovoj oblasti. Ona služi kao uzor za nove ideje o novoj međunarodnoj konvenciji koja bi mogla da pomogne unifikaciji zaštite prava u vezi sa podacima o ličnosti. Saradnja i razmena iskustava na međunarodnom planu predstavljaju osnov za napredak u ovoj oblasti koja se neprestano razvija.

5.2 Regulativa u oblasti zaštite podataka o ličnosti u zemljama bivše Jugoslavije

Zaštita podataka o ličnosti predstavlja globalni fenomen koji je poslednjih nekoliko godina prouzrokovao značajna dešavanja na normativnom planu država širom sveta. Prateći takva dešavanja i države u regionu (*Hrvatska, Crna Gora, Bosna i Hercegovina, Slovenija, Severna Makedonija*) donosile su propise u ovoj oblasti. Propisi ovih država, u najvećem delu, oslanjaju se na Opštu uredbu EU, Konvenciju 108 Saveta Evrope i druge propise EU u ovoj oblasti. To je i logično, imajući u vidu da su Hrvatska i Slovenija države članice EU, Crna Gora i Severna

[289] Tekst Protokola 223 kojim se menja Konvencija o zaštiti lica u odnosu na automatsku obradu ličnih podataka, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.

[290] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Srbija potpisala Protokol kojim se menja Konvencija o zaštiti lica u odnosu na automatsku obradu ličnih podataka Saveta Evrope, https://www.poverenik.rs/sr-yu/aktuelnosti/3204/.

Makedonija su zvanično države kandidati za članstvo, a Bosna i Hercegovina predstavlja potencijalnog kandidata koji je predao aplikaciju za članstvo. Jasno je da ove države teže da usklade svoje zakonodavstvo sa evropskim, pa otuda i slična normativna praksa.

5.2.1. Hrvatska

Hrvatska kao država članica EU ima obavezu primene Opšte uredbe EU. U cilju adekvatne primene ovog propisa, Hrvatska je usvojila *Zakon o primeni Opšte uredbe o zaštiti podataka* (*Zakon o provedbi Opće uredbe o zaštiti podataka*) 2018. godine.[291] Ovim zakonom ustanovljena je *Agencija za zaštitu ličnih podataka* (*Agencija za zaštitu osobnih podataka*)[292] kao nezavisno državno telo, sa sedištem u Zagrebu, koje odgovara za svoj rad Saboru. Predviđeno je da radom agencije upravlja direktor koga imenuje Hrvatski sabor na predlog Vlade Republike Hrvatske (na osnovu javnog poziva za dostavljanje kandidatura). Pored ovih, uređena su i druga pitanja u vezi sa imenovanjem direktora i njegovih zamenika, ovlašćenjima Agencije, načinom njenog finansiranja, itd.

Dalje, konkretizovane su pojedine odredbe Opšte uredbe EU u vezi sa obradom posebnih kategorija podataka. Tako je predviđena granica od 16 godina za davanje pristanka na usluge informacionog društva, zabranjena je obrada genetskih podataka radi izračunavanja izgleda bolesti i drugih zdravstvenih aspekata kod ugovora o životnom osiguranju, kao i uslovi pod kojima se može vršiti obrada biometrijskih podataka u okvirima organa javne vlasti i privatnom sektoru.

Pored toga, uređena su pitanja video nadzora radnih prostorija i stambenih zgrada, kao i mogućnosti obrade podataka o ličnosti u statističke svrhe. Posebna pažnja posvećena je mogućnosti izricanja novčanih kazni za povredu Opšte uredbe EU i ovog zakona, kao i način njihovog izvršavanja.

5.2.2. Slovenija

Slovenija je kao i Hrvatska članica EU, pa na njenoj teritoriji važe odredbe Opšte uredbe EU. Što se tiče nacionalnih propisa, trenutno je na snazi *Zakon o zaštiti ličnih podataka (Zakon o varstvu osebnih podatkov – ZVOP- 1) iz*

[291] Zakon o primeni Opšte uredbe o zaštiti podataka, NN 42/2018, https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka.

[292] Agencija za zaštitu ličnih podataka Hrvatske, https://azop.hr/.

2007. godine.[293] Naravno, ovaj zakon nije usklađen sa Opštom uredbom, pa je Slovenija pristupila usvajanju novog Zakona o zaštiti ličnih podataka (*ZVOP-2*)[294] koji je trenutno u postupku usvajanja i koji će konkretizovati pojedine norme Opšte uredbe EU.

U Sloveniji, funkciju nezavisnog nadzornog tela vrši *Poverenik za informacije* (*Informacijski pooblaščenec),* koji ima sedište u Ljubljani.[295] Prema *Zakonu o Povereniku za informacije*,[296] Poverenika bira Narodna skupština na predlog Predsednika Republike. Ovaj zakon uređuje i druga pitanja od značaja za status, ovlašćenja i delatnosti Poverenika za informacije Slovenije. Stari zakon trebalo bi da bude izmenjen usvajanjem novog Zakona o zaštiti ličnih podataka, čije se usvajanje očekuje u skorije vreme.

5.2.3. Crna Gora

Crna Gora je kandidat za članstvo u EU, što znači da regulativa EU nije izvor prava. Ipak, crnogorsko zakonodavstvo teži da se uskladi sa evropskim, što je jedan od preduslova pridruživanja. Novi zakon u oblasti zaštite podataka o ličnosti koji bi bio usklađen sa novim evropskim propisima nije još donet, ali je u postupku usvajanja. Trenutno je na snazi Zakon o zaštiti podataka o ličnosti iz 2008. godine,[297] koji ne predviđa sva prava i institute kao novo evropsko zakonodavstvo.

Poslove nezavisnog nadzornog tela u Crnoj Gori obavlja *Agencija za zaštitu ličnih podataka i slobodan pristup informacijama*, koja ima dva organa. To su *Savet Agencije i direktor Agencije*.[298] Savet Agencije ima predsednika i dva člana koje imenuje Skupština Crne Gore. Sa druge strane, direktor se imenuje od strane Saveta Agencije na period od četiri godine. Direktor se bira na osnovu raspisanog javnog konkursa.

---

[293] Zakon o zaštiti ličnih podataka Slovenije, „Uradni list RS“ br. 94/07, http://pisrs.si/Pis.web/ pregledPredpisa?id=ZAKO3906.

[294] Za više informacija o novim rešenjima slovenačkog prava u vezi sa zakonom koji se usvaja vid. Linklaters, Data Protected – Slovenia, https://www.ip-rs.si/en.

[295] Poverenik za informacije Slovenije, https://www.ip-rs.si/en.

[296] Zakon o Povereniku za informacije Slovenije, „Uradni list RS“ št. 113/05, engleska verzija teksta, https://www.ip-rs.si/en/legislation/information-commissioner-act.

[297] Zakon o zaštiti podataka o ličnosti, „Sl. list CG“, br. 79/08, 70/09, 44/12, 22/17.

[298] Agencija za zaštitu ličnih podataka i slobodan pristup informacijama, http://www.azlp.me/ me/o-agenciji.

5.2.4. Severna Makedonija

Severna Makedonija takođe je kandidat za članstvo u EU. U Severnoj Makedoniji novi *Zakon o zaštiti ličnih podataka (Закон за заштита на личните податоци)*[299] usvojen je početkom 2020. godine. Osnovni cilj ovog zakona jeste zaštita prava privatnosti i podataka o ličnosti građana, kao i usaglašavanje sa evropskim propisima u ovoj oblasti. Rukovodioci i obrađivači podataka dobili su rok od 18 meseci od stupanja zakona na snagu da usaglase svoje aktivnosti i poslovanje sa odredbama ovog zakona.

Agencija za zaštitu ličnih podataka je dobila status nezavisnog nadzornog državnog organa koji se stara o pravilnoj i zakonitoj primeni ovog zakona.[300] Njeno sedište je u Skoplju. Ona vrši nadzor nad primenom pravila u vezi sa zaštitom ličnih podataka. Rukovodilac Agencije je direktor koga bira i razrešava Narodna skupština (Собрание) na predlog Komisije za imenovanja Narodne skupštine. Direktor se bira na osnovu javnog konkursa, na period od 5 godina. Direktor Agencije bira zamenika direktora.

5.2.5. Bosna i Hercegovina

Bosna i Hercegovina je potencijalni kandidat za članstvo u EU, pa se može reći da je u početnim fazama usklađivanja zakonodavstva. Takav je slučaj i sa sistemom zaštite podataka o ličnosti koji nije u potpunosti usklađen sa Opštom uredbom EU. Trenutno je na snazi Zakon o zaštiti ličnih podataka iz 2006. godine.[301]

Ovim Zakonom osnovana je *Agencija za zaštitu ličnih podataka*,[302] kao samostalna upravna organizacija koja je osnovana da bi se obezbedila zaštita ličnih podataka i koja je potpuno nezavisna u izvršenju dužnosti koje su joj poverene.[303] Njeno sedište je u Sarajevu, a može imati odeljenja i organizacione jedinice. Za rukovođenje Agencijom zadužen je direktor koji ima jednog zamenika. Njih imenuje Parlamentarna skupština BiH na mandat od pet godina uz mogućnost ponovnog imenovanja. Delatnosti i ovlašćenja Agencije podudaraju se

[299] Zakon o zaštiti ličnih podataka Makedonije, „Сл. весник РСМ“, br. 42/2020., https://dzlp.mk/sites/default/files/u4/zakon_za_zastita_na_licnite_podatoci.pdf.
[300] Agencija za zaštitu ličnih podataka Makedonije, https://dzlp.mk.
[301] Zakon o zaštiti ličnih podataka BiH, „Sl. glasnik BiH“, be. 49/2006, 76/2011 i 89/2011.
[302] Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, http://www.azlp.ba/ Default.aspx?langTag=sr-SP-Cyrl&template_id=147&pageIndex=1.
[303] Čl. 35 Zakona o zaštiti ličnih podataka BiH.

sa delatnostima i ovlašćenjima koje imaju ostali nezavisni organi na evropskom nivou.

5.2.6. Zaključak

Kao što se može primetiti, zakonodavstva država na teritoriji bivše Jugoslavije teže da se usklade sa zakonodavstvom EU. Strateška i politička usmerenost prouzrokovala je i preuzimanje evropskih vrednosti u pogledu zaštite prava i sloboda građana. Ipak, čini se da je većina država više pratila normativna dešavanja, nego što je u društvu sazrela svest o neophodnosti zaštite podataka o ličnosti. Naravno, samo usvajanje zakona i predviđanje nezavisnih nadzornih tela predstavlja veliki korak u pravcu zaštite privatnosti i transparentnog funkcionisanja svih društvenih faktora u pogledu obrade podataka.

5.3 Regulativa u oblasti zaštite podataka o ličnosti u Srbiji

Razvoj tehnologije, sve veća upotreba podataka u različitim oblastima društvenog života i, posebno, normativna dešavanja na evropsku tlu, uslovila su i normativnu reakciju Srbije u vezi sa zaštitom podataka o ličnosti. Zbog toga je Srbija 2018. godine usvojila Zakon o zaštiti podataka o ličnosti, koji je zamenio prethodni istoimeni zakon koji je važio od 2008. godine. Kao što je navedeno u obrazloženju zakona: „Razlozi za donošenje novog Zakona o zaštiti podataka o ličnosti su brojni i mogu se razmatrati kako zbog potreba Republike Srbije, tako i zbog potreba međunarodne saradnje, kao i zbog procesa pridruživanja Republike Srbije Evropskoj uniji. Sa stanovišta unutrašnjeg prava, postojeći pravni okvir zaštite podataka o ličnosti ne može adekvatno da obezbedi nesmetano ostvarivanje prava na zaštitu podataka o ličnosti u svim oblastima, zbog čega je neophodno izvršiti izmene i dopune normativnog okvira u ovoj oblasti. Kada je u pitanju međunarodna saradnja, odnosno proces pridruživanja Republike Srbije Evropskoj uniji, usklađivanje nacionalnog zakonodavstva sa pravom Evropske unije predstavlja međunarodno pravnu obavezu Republike Srbije, dok status Republike Srbije kao kandidata za članstvo u Evropskoj uniji ukazuje da su evropske integracije ključne za spoljnu i unutrašnju politiku zemlje. Imajući u

vidu navedene razloge, neophodno je doneti novi zakon koji će urediti ovu oblast.“[304]

5.3.1. Zakon o zaštiti podataka o ličnosti

Kao što se može zaključiti, osnovni cilj Zakona o zaštiti podataka o ličnosti bio je usklađivanje sa Opštom uredbom EU i Policijskom direktivom, koje su usvojene dve godine ranije. To je i evidentno u odnosu na veliku većinu članova Zakon o zaštiti podataka o ličnosti, koji predstavljaju preslikanu Opštu uredbu EU. Ipak, pojedina pitanja nisu uređena na istovetan način, pa su ostale pravne praznine koje treba popuniti i pitanja na koje treba dati odgovor. Na prvom mestu, Zakon o zaštiti podataka o ličnosti ne sadrži preambulu kao Opšta uredba EU, što znači da ne postoji ni zakonska razrada osnovnih principa, prava građana i instituta, od kojih su mnogi prvi put našli mesto u domaćem pravnom sistemu. Postavljene su znatno blaže sankcije nego što je to slučaj u Opštoj uredbi EU, a javljaju se i pitanja u vezi sa načinom primene sankcija. Važno pitanje video nadzora nije dobilo pažnju u ovom zakonskom tekstu. Osim toga, potrebno je urediti i brojna pitanja u posebnim oblastima, kao što je primena odredaba ovog zakona od strane organa javne uprave.

I pored postojećih propusta i dilema, Zakon o zaštiti podataka o ličnosti iz 2018. godine, prvi put u istoriji Srbije uspostavlja temeljan sistem zaštite podataka koji je postavljen kao štit privatnosti građana, preko koje se brane i druga ljudska prava i slobode. Ovaj Zakon predstavlja odgovarajući pravni okvir koji će zahtevati dosta teorijskog razmatranja i praktične primene kako bi u potpunosti ispunio pomenutu ulogu zaštitnika privatnosti. Slično kao i za demokratiju, i za oblast zaštite podataka može se uzeti metafora za travnjake. Naime, za lep travnjak potrebno je dosta vremena, truda i svakodnevnog ulaganja. Takav je slučaj i sa sistemom zaštite podataka kojem će trebati puno vremena i truda da bi ostvario svoju (pravu) zaštitnu funkciju. Zbog toga, skrećemo pažnju da je način primene Zakona o zaštiti podataka o ličnosti u praksi, jednako važno pitanje kao i zakonske odredbe. Tehnički posmatrano, Zakon o zaštiti podataka o ličnosti sastoji se od 10 celina:

1. Osnovne odredbe;
2. Načela;
3. Prava lica na koje se podaci odnose;
4. Rukovalac i obrađivač;

[304] Vid. Obrazloženje Zakona o zaštiti podataka o ličnosti od 09. 07. 2018. god., str. 1.

5. Prenos podataka o ličnosti u druge države i međunarodne organizacije;
6. Poverenik;
7. Pravna sredstva, odgovornost i kazne;
8. Posebni slučajevi obrade;
9. Kaznene odredbe;
10. Prelazne i završne odredbe.[305]

5.3.1.1. Cilj, predmet i pravna priroda Zakona o zaštiti podataka o ličnosti

Poput drugih zakonskih propisa, u osnovnim odredbama ovog zakona određeni su osnovni predmet i cilj njegovih odredaba. Skrećemo pažnju da je osnovni cilj ovog zakona zaštita osnovnih prava i sloboda fizičkih lica, među kojima se posebno ističe pravo na zaštitu podataka o ličnosti. Dakle, cilj zakona nije zaštita podataka o ličnosti, kao što se može zaključiti iz njegovog naziva, već zaštita prava građana koja se nalaze u vezi sa njihovim podacima.

Dok je cilj relativno lako razumeti, predmet ovog zakona postavljen je dosta široko. Teorijski posmatrajući, ovim zakonom se ustanovljava celokupan sistem zaštite podataka o ličnosti, nezavisno od toga da li ga primenjuju lica privatnog ili javnog prava. Normativno, Zakonom o zaštiti podataka o ličnosti uređuje se pravo na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti i slobodan protok takvih podataka, načela obrade, prava lica na koje se podaci odnose, obaveze rukovalaca i obrađivača podataka o ličnosti, kodeks postupanja, prenos podataka o ličnosti u druge države i međunarodne organizacije, nadzor nad sprovođenjem ovog zakona, pravna sredstva, odgovornost i kazne u slučaju povrede prava fizičkih lica u vezi sa obradom podataka o ličnosti, kao i posebni slučajevi obrade. Pored toga, u ovom zakonu se nalaze i odredbe u vezi sa pravom na zaštitu fizičkih lica u vezi sa obradom podataka o ličnosti koju vrše organi javnog reda i mira i bezbednosti, odnosno obrada koja se vrši u cilju sprečavanja, istrage i otkrivanja krivičnih dela, gonjenja učinilaca krivičnih dela ili izvršenja

[305] Uporedno posmatrano, tehnički pristup je gotovo istovetan sa organizacijom poglavlja Opšte uredbe EU. Opšta uredba EU podeljena je na 11 poglavlja. 1. Opšta načela, 2. Načela, 3. Prava lica na koje se podaci odnose, 4. Rukovalac i obrađivač podataka, 5. Prenos podataka o ličnosti u treće države i međunarodne organizacije, 6. Nezavisni nadzorni organi, 7. Saradnja i konzistentnost, 8. Pravna sredstva, odgovornost i sankcije, 9. Odredbe u vezi sa posebnim situacijama obrade, 10. Delegirani akti i akti za sprovođenje, 11. Završne odredbe.

krivičnih sankcija, što podrazumeva i sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti, kao i slobodan protok takvih podataka.[306]

Kao što se može primetiti, Zakonom se ustanovljava opšti sistem zaštite podataka o ličnosti i osnovni pravni instituti u ovoj oblasti, ali i poseban sistem zaštite podataka o ličnosti u oblasti bezbednosti. Ovaj pristup razlikuje se od evropskog pristupa. Naime, EU je razvila odvojen pristup. Jednim propisom je regulisan opšti sistem, a posebnim propisom sistem zaštite podatka o ličnosti u oblasti bezbednosti.

Važno je pomenuti da je Zakon o zaštiti podataka o ličnosti ustanovljen kao opšti zakon u ovoj oblasti. Formalno, naš pravni sistem ne pravi razliku između propisa iste pravne snage. Ipak, praktično se pojedini zakoni primenjuju u svim posebnim oblastima u odnosu na materiju regulisanja, pa važe kao osnovni, odnosno opšti zakoni za pojedine oblasti.[307] Iz određenja ovog Zakona kao opšteg proizlazi činjenica da odredbe posebnih zakona kojima se uređuju pitanja u vezi sa zaštitom podataka, moraju da budu u skladu sa odredbama ovog zakona. Dakle, pojedina pitanja mogu se uređivati i konkretizovati, ali suštinski moraju pratiti normativna rešenja Zakona o zaštiti podataka o ličnosti. Posledica se javlja i na planu usklađivanja postojećih posebnih zakona koji se moraju uskladiti sa opštim zakonom u oblasti zaštite podataka do kraja 2020. godine.[308] To će predstavljati veliki poduhvat koji, čini se, neće biti u potpunosti završen, već će se nastaviti i u narednim godinama.

5.3.1.2. Polje primene odredaba Zakona o zaštiti podataka o ličnosti

U okviru osnovnih odredbi određuje se i polje primene Zakona o zaštiti podataka o ličnosti. Opšte je pravilo da se norme ovog zakona primenjuju kod svake *automatizovane obrade, kao i kod neautomatizovane obrade* podataka koji predstavljaju deo zbirke, odnosno skupa podataka ili su takvoj zbirci namenjeni. Automatizovana obrada podrazumeva korišćenje računara ili drugih digitalnih uređaja koji preko odgovarajućeg programa (softvera) obrađuju podatke – obrada podataka u *Microsoft Word*-u na računaru. Neautomatizovana obrada u stvari predstavlja ručnu obradu – prepisivanje podataka u svesku hemijskom olovkom.

---

[306] Čl. 1 Zakona o zaštiti podataka o ličnosti.

[307] Dobrosav Milovanović, „Odnos opšt(ij)eg i posebn(ij)ih upravno procesnih zakona“, *Polis – časopis za javnu politiku*, Stalna konferencija gradova i opština, Savez gradova i opština Srbije i Centar za javnu i lokalnu upravnu – Palgo centar, Beograd 2016, str. 42.

[308] Čl. 100 Zakona o zaštiti podataka o ličnosti.

U situaciji obrade podataka koju vrše fizička lica za sopstvene potrebe ili za potrebe svog domaćinstva, odredbe ovog zakona neće se primenjivati. *Primera radi*, reč je čuvanju iređanju fotografija u porodični album, pohranjivanje video zapisa u odgovarajuće foldere na kućnom računaru ili zapisivanje brojeva bankovnih računa bračnih drugova u zajednički kućni dnevnik.

Primena zakonskih normi je određena i prema teritorijalnom kriterijumu, kao osnovnom postulatu primene normi nacionalnih zakonodavstava. To znači da kod obrade podataka o ličnosti mora postojati određena veza sa teritorijom Republike Srbije ili njenim građana da bi se ovaj zakon mogao primeniti.

U vezi sa teritorijalnim važenjem Zakona o zaštiti podataka o ličnosti, predviđene su dve situacije. *Prva situacija* podrazumeva *teritorijalni princip*, po kome je funkcija pravosuđa države ograničena na pravne stvari u vezi sa njenom teritorijom, dok se *druga situacija* zasniva na *personalnom principu*, kod koga se nadležnost zasniva prema pravnoj stvari koja se odnosi na građane Republike Srbije u inostranstvu.[309]

U prvom slučaju, domaće zakonodavstvo primenjuje se na one obrade podataka o ličnosti koju vrše rukovalac, odnosno obrađivač koji imaju sedište ili prebivalište, odnosno boravište na teritoriji Republike Srbije, u okviru aktivnosti koje se vrše na teritoriji Republike Srbije, bez obzira da li se radnja obrade vrši na teritoriji Republike Srbije.[310]

Da bi se ispunio ovaj kriterijum, neophodno je da se ispuni nekoliko uslova. Prvi uslov je da rukovalac, odnosno obrađivač, imaju pravno relevantnu vezu sa aktivnostima na teritoriji Republike Srbije. U slučaju *pravnih lica* koje vrše obradu, to znači da imaju *sedište* (da su registrovani i da obavljaju svoje aktivnosti na teritoriji Republike Srbije), dok je *kod fizičkih lica* odgovarajuća veza *prebivalište*, kao mesto u kome se građanin nastanio sa namerom da u njemu stalno živi, odnosno mesto u kome se nalazi centar njegovih životnih, profesionalnih, ekonomskih, socijalnih i drugih aktivnosti i veza koje dokazuju njegovu trajnu povezanost sa mestom u kojem se nastanio ili *boravište*, kao mesto u kome građanin privremeno boravi van mesta svog prebivališta, duže od 90 dana.[311]

Nije neophodno da se sama radnja obrade preduzima na teritoriji Republike Srbije, već se te radnje mogu vršiti i izvan njene teritorije. *Na primer*, kod korišćenja mnogih internet sajtova, podaci se ne čuvaju na istom mestu gde

[309] Vid. Aleksandar Jakšić, *Građansko procesno pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013, str. 97.
[310] Čl. 3, st. 3 Zakona o zaštiti podataka o ličnosti.
[311] Vid. čl. 3 Zakona o prebivalištu i boravištu građana, „Sl. glasnik RS“, br. 87/2011.

se nalazi sedište rukovaoca. Dakle, iako se podaci o ličnosti preuzeti na sajtu čuvaju u bazama podataka u Sjedinjenim Američkim Državama, a sedište rukovaoca je u Srbiji, teritorijalna primena Zakona o zaštiti podataka o ličnosti Republike Srbije biće moguća i obuhvatiće i obradu takvih podataka.

Druga situacija u kojoj će doći do teritorijalne primene Zakona o zaštiti podataka o ličnosti odnosi se na slučaj obrade podataka fizičkog lica koje ima prebivalište, odnosno sedište na teritoriji Republike Srbije, a rukovalac, odnosno obrađivač imaju sedište, prebivalište ili boravište van teritorije Republike Srbije (u inostranstvu). Ipak, da bi došlo do ovakve primene, neophodno je da budu ispunjeni dodatni elementi, odnosno situacije u vezi sa radnjama obrade. Dovoljno je da rukovalac, odnosno obrađivač, vrše jednu od pomenutih aktivnosti.[312]

Prvo, zakon će se primeniti ukoliko se radnje obrade tiču ponude robe, odnosno usluga, licu na koje se podaci odnose na teritoriji Republike Srbije, bez obzira da li je takva radnja komercijalnog karaktera, odnosno da li se od lica na koga se podaci odnose, zahteva plaćanje naknade za tako ponuđenu robu, odnosno uslugu. *Primera radi*, ponuda dodatne opreme za vozila preko interneta ili ponuda usluge izrade internet stranice (*website*) od strane pakistanske firme srpskim državljanima.

Drugo, odredbe domaćeg zakona primenjuju se na rukovaoca ili obrađivača koji se nalaze u inostranstvu kada oni prate aktivnosti lica koje ima prebivalište, odnosno sedište na teritoriji Republike Srbije, uz dodatni uslov da se aktivnosti tog lica preduzimaju na teritoriji Republike Srbije. *Pojam aktivnosti* odnosi se kako na *fizičku* – kretanje ulicom ili šumom, tako i na *„digitalnu"* aktivnost – pristup pojedinim internet stranicama koji se može pratiti putem „kolačića" kao posebnog sredstva praćenja ponašanja korisnika u digitalnom svetu. „*Kolačići* (eng. *Cookies*) su mali tekstualni fajlovi (tzv. podaci mrvice) koje veb sajt skladišti na računarima korisnika, odnosno u pretraživačima, da bi se po potrebi brzo i pouzdano ponovo prepoznali."[313] *Kao primer* možemo uzeti praćenje ponašanje korisnika nakon posete određenog vebsajta koji se bavi iznajmljivanjem nepokretnosti.

Kao što možemo zaključiti, reč je o vidu *eksteritorijalne* primene Zakona o zaštiti podataka o ličnosti. Ipak, u vezi sa ovom odredbom treba imati na umu *Smernice Evropskog odbora za zaštitu podataka 3/2018 o teritorijalnoj primeni*

[312] Čl. 3, st. 4 Zakona o zaštiti podataka o ličnosti.
[313] A. Diligenski, D. Prlja, D. Cerović (2018), str. 30.

Opšte uredbe EU.[314] Naime, sledeći njihovu logiku, domaće zakonodavstvo neće se uvek primenjivati u odnosu na obradu podataka građana Srbije, od strane rukovaoca, odnosno obrađivača sa sedištem u inostranstvu. U ovom slučaju mora postojati izražena namera da se državljani Srbije „pogađaju reklamama", odnosno da im se aktivno plasira sadržaj na domaćoj teritoriji. Na takvu nameru u digitalnom okruženju mogu ukazivati, *primera radi*, jezik na kome je sačinjena internet stranica (srpski ili strani jezik), promovisanje aktivnosti rukovaoca i obrađivača (isključivo u Srbiji ili samo u inostranim državama), i drugi elementi. To znači da samo postojanje internet stranice i mogućnost pristupa takvoj stranici iz Srbije nije dovoljan element da bi se ostvarila eksteritorijalna primena našeg zakona, budući da bi to predstavljalo svojevrsnu „zloupotrebu prava".

5.3.1.3. Značenje izraza

Član. 4 Zakona o zaštiti podataka o ličnosti posvećen je određivanju pojmova koji se koriste u ovom zakonskom tekstu. Ovaj propis, za razliku od Opšte uredbe EU, nema preambulu pa je ovo jedini relevantan član za razumevanje novih instituta i pojedinih termina koje treba primeniti. U okviru ovog člana sadržane su definicije podatka o ličnosti, obrade podataka, rukovaoca, obrađivača, privrednih subjekata, nadležnih organa u sektoru bezbednosti i mnogi drugi pojmovi.[315] Njih treba koristiti i u posebnim zakonima, u slučaju postojanja pravnih praznina ili poteškoća oko razumevanja domašaja određenog instituta u vezi sa zaštitom podataka o ličnosti.

5.3.1.4. Rukovalac i obrađivač

Pored lica čiji se podaci obrađuju**,** rukovalac i obrađivač predstavljaju glavne subjekte obrade podataka o ličnosti, pa samim tim i sistema zaštite podataka.

Rukovalac je ono fizičko ili pravno lice, odnosno organ vlasti, koji samostalno ili zajedno sa drugima određuje svrhu i način obrade. Kada se posebnim zakonom propisuju svrha i način obrade, može se odrediti i rukovalac, odnosno kriterijumi prema kojima će se on odrediti. Iz ovakvog određenja proizlazi i mogućnost postojanja zajedničkih rukovalaca koji zajedničkim sporazumom određuju svrhu i način obrade podataka o ličnosti.

[314] Smernice Evropskog odbora za zaštitu podataka 3/2018 o teritorijalnoj primeni Opšte uredbe EU, https://edpb.europa.eu/sites/edpb/files/ files/file1/edpb_guidelines_ 3_2018_territorial _scope_ en.pdf.

[315] Za sve pojmove vid. čl. 4 Zakona o zaštiti podataka o ličnosti.

U određenom broju situacija, rukovaoci će biti određeni zakonom (npr. Agencija za privredne registre, banke, sportska društva, itd.), dok će u drugim situacijama u zakonu biti predviđeni kriterijumi na osnovu kojih se posredno mogu odrediti rukovaoci (lica koja obavljaju telekomunikacione delatnosti). To znači da će u velikom broju situacija rukovaoci sami morati da procene da li ispunjavaju zakonske kriterijume.

Odrediti svrhu obrade podataka o ličnosti znači odrediti razlog zbog koga se prikupljaju ili obrađuju podaci građana. Primera radi, preduzetnik koji poseduje imejlove većeg broja fizičkih lica, preko kojih komunicira sa njima i nudi im svoje kulinarske usluge, jeste rukovalac u odnosu na imejlove, koji se mogu povezati sa određenim licima.

Odrediti način obrade podataka o ličnosti znači doneti odluku o tome kako će se koristiti prikupljeni podaci. Direktor koji je uveo video nadzor u firmu, donosi odluku da će video zapisi biti sačinjavani samo u odnosu na lica koja se nalaze u konferencijskoj sali radi zaštite bezbednosti slika i druge pokretne imovine u toj sali, da će takvi video zapisi biti čuvani u računarima kompanije i da će biti čuvani u roku od 30 dana. Ovim putem, direktor je odredio način obrade, što znači da se sama kompanija nalazi u ulozi rukovaoca, a ne direktor.

Obrađivač podataka je fizičko ili pravno lice, odnosno organ vlasti, koji obrađuje podatke o ličnosti u ime rukovaoca. Praktično posmatrano, to znači da rukovalac određuje svrhu i način obrade, ali je aktivnosti u vezi sa obradom delegirao na drugo lice, koje poseduje stručna znanja ili jednostavno sarađuje sa rukovaocem. „Komunalno preduzeće angažuje preduzeće koje upravlja pozivnim centrom da u njegovo ime obavlja mnoge funkcije njegove korisničke službe. Zaposleni u pozivnom centru imaju pristup evidencijama o korisnicima usluga komunalnog preduzeća za potrebe pružanja usluga za koje su angažovani, ali te podatke mogu da koriste samo u konkretne svrhe i u skladu sa strogim ugovornim aranžmanima. Komunalno preduzeće je i dalje rukovalac podataka. Preduzeće koje upravlja pozivnim centrom je obrađivač podataka.“[316]

Rukovalac je, dakle, glavno odgovorno lice za obradu podataka o ličnosti. Ova odgovornost oslikava se i u odnosu rukovaoca i obrađivača, gde obrađivač mora da postupa u svemu prema nalozima rukovaoca, što treba da bude uređeno obaveznim ugovorom između ovih lica. Odgovornost rukovaoca podrazumeva i obavezu snošenja posledica u slučaju zloupotrebe podataka o ličnosti ili povrede odredaba Zakona o zaštiti podataka o ličnosti, putem

[316] Klemenč Mišič, Maja Lubarda, *Zaštita podataka – priručnik za rukovaoce*, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije, Beograd 2012, str. 12.

prekršaja, krivičnih dela ili instituta naknade štete. Naravno, ukoliko je za štetu kriv obrađivač, rukovalac će moći da se regresira po pravilima odštetnog prava.

5.3.1.5. Organizacione, kadrovske i tehničke mere kao element bezbednosti

Usklađenost poslovanja sa Zakonom o zaštiti podataka o ličnosti podrazumeva da rukovaoci i obrađivači predvide i primene *organizacione, kadrovske i tehničke mere* u odnosu na radnje obrade i podatke građana koji se nalaze u njihovom posedu.[317] Predviđanje i uvođenje mera znače implementaciju sistema zaštite podataka o ličnosti na mikro nivou, na nivou rukovaoca, odnosno obrađivača. Njihovim uvođenjem u procese poslovanja i obrade, podaci građana dobijaju dodatnu zaštitu po pitanju njihove privatnosti. U praksi, sve tri vrste mera su povezane i čine jedinstven bezbednosni mehanizam koji najbolje rezultate postiže njihovim uzajamnim dejstvom.

U tehničke mere mogu se uvrstiti *pesudonimizacija* podataka (mera koja pomaže da se podaci o ličnosti ne mogu pripisati određenom licu bez upotrebe dodatnih informacija, a te informacije se čuvaju odvojeno od samih podataka), *anonimizacija* (svi elementi identifikacije su uklonjeni iz zbirke podataka, pa se lice na koje se podaci odnose više ne može identifikovati), *enkripcija* (metod pretvaranja razumljivog podatka u nerazumljiv, koji se može razumeti samo pomoću šifre (ključa), pa samo onaj koji šalje informaciju i primalac mogu znati pravo značenje podatke, zato što imaju ključ za razumevanje), *čuvanje podataka* (više baza podataka od kojih je jedna u digitalnom, a druga u fizičkom obliku, pri čemu se one čuvaju na različitim mestima, itd.), *mere informacione bezbednosti*, kao što je uvođenje računarskih programa (softvera) koji štite bezbednost računara na kome su pohranjeni podaci, redovno ažuriranje sistema, itd.

Pod organizacionim merama podrazumeva se preraspodela obaveza, dužnosti, zadataka, ovlašćenja i prava u okviru organizacione strukture rukovaoca, odnosno obrađivača. Svako lice (zaposleni) u okviru rukovaoca ili obrađivača treba da ima jasno definisanu ulogu u vezi sa podacima o ličnosti i njihovim korišćenjem. Ne sme se dozvoliti da sva lica u okviru organizacije imaju pristup podacima o ličnosti, budući da to stvara veliki rizik po privatnost. To znači da pristup u okviru organizacije treba dopustiti samo konkretno određenim licima koja direktno koriste podatke. U tom smislu važna je delegacija nadležnosti, kao i odgovarajući mehanizam strukturalnog funkcionisanja u okviru

[317] Više o ovim merama vid. Stefan Andonović (2019), str. 310-328.

koga svako poznaje svoju poziciju, prava i dužnosti u odnosu na podatke o ličnosti. Na taj način organizacija služi kao metod zaštite privatnosti građana.

Organizacione mere podrazumevaju i *kontrolu kvaliteta pravnih akata* koji se tiču podataka. Kontrola kvaliteta podrazumeva analizu uspešnosti uspostavljenih mera zaštite, što može da ukaže na potrebu za usavršavanjem ili ažuriranjem pojedinih mera ili drugačiju postavku sistema zaštite. U tom smislu neophodno je prvo odrediti željene ciljeve donošenja propisa ili internog akta i potom utvrditi uspešnost njegove primene u određenom vremenskom periodu. Na taj način dobija se kompletna slika o kvalitetu donetih akata i usklađenosti unutrašnjih akata i mera sa zakonskim i drugim opštim pravnim aktima, i to sa određene vremenske distance koja omogućava objektivnu ocenu. Važna organizaciona mera jeste i mogućnost, a u određenim slučajevima i obaveza, imenovanja *lica za zaštitu podataka*.[318]

Kadrovske mere govore o tome da su lica koja obrađuju podatke o ličnosti dovoljno obučena za takav posao. Kako se rizici po podatke neprestano razvijaju, potrebno je i konstantno učenje i usavršavanje u oblasti njihove zaštite. Zbog toga, kao jedna od osnovnih mera kojima se osigurava bezbednost podataka o ličnosti jeste usavršavanje i osposobljavanje zaposlenih kod rukovaoca i obrađivača u vezi sa načinima i metodama zaštite. Sticanje novih znanja i profesionalno usavršavanje imaju dvostruku korist, kako za rukovaoca koji će smanjiti moguće rizike, tako i za građane čija se privatnost štiti i na ovaj način.

Kako postoje različite vrste rukovaoca i obrađivača (po veličini, finansijskoj moći, osnovnim delatnostima poslovanja), nerealno je da svi mogu da primene istovetne mere. Zbog toga, prilikom ustanovljavanja mera, različiti rukovaoci, odnosno obrađivači, treba da imaju u vidu *nivo tehnoloških dostignuća, troškove primene mera, kao i prirodu, obim, okolnosti, svrhu obrade, verovatnoću i nivo rizika po prava i slobode fizičkih lica*.[319] Ovi elementi govore o tome da treba primeniti najbolje i najefikasnije mere, ali u odnosu na realnu snagu, moć i delatnosti rukovaoca, odnosno obrađivača. Reč je zapravo o oceni potrebe i mogućnosti u vezi sa podacima građana. Primena mera govori o nameri rukovaoca/obrađivača da pruži zaštitu podataka o ličnosti i privatnosti građana, što smanjuje udeo njegove eventualne odgovornosti, čime se otvara mogućnost za izbegavanje sankcija u slučaju povrede ličnih podataka koja se nalazi u nekom spoljnjem uzroku ili faktoru.

[318] Stefan Andonović, „Obaveza imenovanja lica za zaštitu podataka u organima uprave“, časopis *Savremena uprava*, Beograd 2019, str. 48-53.

[319] Čl. 42, st. 1 Zakona o zaštiti podataka o ličnosti.

5.3.1.6. Vođenje evidencije o radnjama obrade

Jedan od važnijih obaveza rukovaoca i obrađivača jeste *vođenje evidencije o radnjama obrade*. Evidencije sadrže podatke koji se odnose na subjekte obrade (ko obrađuje lične podatke, kontakt podatke), na svrhe obrade, načine obrade, vrste podataka koji se obrađuju, eventualni prenos podataka, rok posle koga se brišu podaci i na opšti opis kadrovskih, organizacionih i tehničkih mera.[320] Njih vode i rukovaoci i obrađivači (njihova dužnost odnosi se na radnje obrade koje se preduzimaju u ime rukovaoca). Za razliku od prethodnog zakona,[321] više ne postoji obaveza dostavljanja evidencija Povereniku, osim ukoliko on izričito uputi zahtev za dostavljanjem evidencije.

Evidencije treba da služe kao dokaz o svim značajnijim činjenicama koje se odnose na obradu podataka o ličnosti. One se mogu koristiti kao osnov za utvrđivanje ili oslobađanje od odgovornosti rukovaoca. Dakle, evidencije suštinski svedoče o postupcima i preduzetim radnjama koje mogu biti od uticaja na privatnost građana.[322]

5.3.1.7. Davanje obaveštenja u slučaju povrede podataka o ličnosti

Obaveštenje Poverenika o povredi podataka o ličnosti, kao i obaveštavanje lica na koje se podaci odnose o povredi podataka, predstavljaju nove institute u domaćem pravu. Ovi instituti imaju za cilj brzo i efikasno delovanje u slučaju povrede podataka o ličnosti.

U prvom slučaju, dužnost je rukovaoca da obavesti Poverenika o povredi podataka o ličnosti koja može da proizvede rizik po prava i slobode fizičkih lica. Rukovalac treba Poverenika da obvesti bez nepotrebnog odlaganja ili u roku od 72 časa od saznanja za povredu (ne od nastanka povrede). Imajući na umu lanac odgovornosti, ukoliko se obrađivač susretne sa povredom podataka koja nosi rizik, on je dužan da o tome obavesti rukovaoca. Obaveštenje treba da sadrži sve informacije koje su neophodne kako bi Poverenik razumeo o kakvoj je povredi reč, ali i kakve su mere preduzete da bi se smanjio rizik i sanirale posledice povrede. Cilj ovakvog obaveštavanja jeste transparentnost, ali i eventualna pomoć ili savet Poverenika kako da se izbegnu značajni rizici. U ovom slučaju postojanja

[320] Detaljno o evidencijama radnji obrade vid. čl. 47 Zakona o zaštiti podataka o ličnosti.

[321] Na osnovu ranijeg zakona doneta je i Uredba o obrascu za vođenje evidencije i načinu vođenja evidencije o oblasti podataka o ličnosti, „Sl. glasnik RS“, br. 50/2009, koja više nije na snazi.

[322] Obrazac za vođenje evidencije o obradi podataka o ličnosti, https://www.paragraf.rs/obrasci/2052_ID.pdf.

„običnog stepena rizika“ rukovalac nije dužan da obavesti lice na koje se podaci odnose.

U situaciji kada zbog povrede podataka o ličnosti dođe do visokog stepena rizika po prava i slobode fizičkih lica, pored Poverenika, rukovalac obaveštava i lice na koje se podaci odnose. Rok za obaveštavanje nije definisan, pa rukovalac treba da pruži obaveštenje bez nepotrebnog odlaganja. Obaveštenje treba da sadrži sve elemente obrade, povrede i eventualnih posledica.

Prijemom obaveštenja, lice na koje se podaci odnose dobija mogućnost da preduzme sopstvene aktivnosti na planu smanjenja visokog stepena rizika po njegova prava i slobode. Izuzetak od pravila obaveštavanja lica na koje se podaci odnose predviđen je u slučaju da je rukovalac preduzeo odgovarajuće mere (posebno ako je pristupio kripto zaštiti i onemogućio razumljivost podataka), zatim ukoliko su preduzete mere sprečile nastanak posledice za lica na koja se ugroženi podaci odnose ili ako bi obaveštavanje dovelo do nesrazmernog utroška vremena i sredstava (što ne znači da ne postoji obaveza rukovaoca da na drugi način, npr. sredstvima javnog obaveštavanja pruži informacije o rizicima licima na koje se podaci odnose).

5.3.1.8. Procena uticaja na zaštitu podataka o ličnosti

Veliki broj rizika koji se javlja po podatke o ličnosti iznedrio je jedan institut koji ima preventivnu prirodu. Reč je o *institutu procene uticaja na zaštitu podataka o ličnosti*. Do primene ovog instituta dolazi u situacijama kada postoji verovatnoća da će određena obrada podataka stvoriti visok rizik po prava i slobode fizičkih lica. Svrha ovog instituta jeste da se preventivnim delovanjem, pre započinjanja obrade, uoče mogući faktori koji mogu dovesti do povrede podataka. Ovaj institut je posebno značajan prilikom upotrebe novih tehnologija kod obrade podataka o ličnosti (svrhe i načina obrade, vrste podataka, itd.).

Obaveznost procene uticaja javlja se u slučaju sistemske i sveobuhvatne procene stanja i osobina fizičkog lica kod automatizovane obrade (što podrazumeva i profilisanje) koja rezultira donošenjem odluke od značaja za pravni položaj pojedinca. Takođe, procena uticaja na zaštitu podataka o ličnosti obavezna je kod obrade posebnih vrsta podataka o ličnosti, kao i podataka o ličnosti u vezi sa krivičnim presudama i kažnjivim delima, kao i kod sistemskog nadzora nad javno dostupnim površinama.

Procena uticaja najmanje mora da sadrži**:**

1. sveobuhvatan opis predviđenih radnji obrade i svrhu obrade,

2. procenu neophodnosti i srazmernosti vršenja radnji obrade u odnosu na svrhu,

3. procenu rizika po prava i slobode lica čiji se podaci obrađuju,

4. opis nameravanih mera u cilju smanjivanja ili saniranja rizika, što obuhvata sve vrste organizacionih, kadrovskih i tehničkih mera.[323]

Ukoliko je procena uticaja na zaštitu podataka o ličnosti izvršena, i ukaže na činjenicu da će nameravane radnje obrade proizvesti visok rizik po prava ukoliko se ne preduzmu mere za njegovo umanjenje, rukovalac ima dužnost da, pre nego što započne obradu, zahteva mišljenje od Poverenika.[324] Uz zahtev, rukovalac dostavlja i sve važnije činjenice koje se odnose na dužnosti rukovaoca i obrađivača, svrhu obrade, način obrade, mere, procenu uticaja, itd.

5.3.1.8. Lice za zaštitu podataka o ličnosti

Radi usaglašavanja sa Zakonom o zaštiti podataka o ličnosti, rukovalac i obrađivač mogu da odrede i lice za zaštitu podataka. Lice za zaštitu podataka određuje rukovalac ili obrađivač. Institut lica za zaštitu podataka u domaćem pravu je preuzet iz evropskog zakonodavstva.[325]

Pravilo je da je imenovanje lica za zaštitu podataka samo mogućnost, ali u određenim slučajevima rukovalac ili obrađivač *imaju obavezu da imenuju ovo lice*.[326] Lice za zaštitu podataka ima savetodavnu i usmeravajuću ulogu u vezi sa procesima obrade. Ono pomaže rukovaocu ili obrađivaču da pravilno vrše aktivnosti obrade tako da osiguraju poštovanje normative u oblasti zaštite podataka. Zbog toga, prilikom određivanja ovog lica treba voditi računa o ličnim, profesionalnim i stručnim kvalifikacijama tog lica. Takvi kvaliteti jesu svojevrsni garant da će lice za zaštitu podataka pratiti dešavanja na normativnom planu, obraćati pažnju na upravnu i sudsku praksu u ovoj oblasti i da će svoje znanje na odgovarajući način implementirati u procese obrade kod rukovaoca ili obrađivača, kojima to obično nije osnovna delatnosti.

Sa licem za zaštitu podataka zaključuje se ugovor koji može biti ugovor o radu, ugovor o delu ili ugovor o obavljanju privremenih i povremenih poslova. Lice koje se određuje može biti zaposleno u okviru organizacije obrađivača ili rukovaoca ili to može biti lice koje se nalazi van njihove organizacione i poslovne

[323] Čl. 54, st. 5 Zakona o zaštiti podataka o ličnosti.
[324] Čl. 55, st. 1 Zakona o zaštiti podataka o ličnosti.
[325] Više o licu za zaštitu podataka u Evropskoj Uniji vid. P. Lambert, (2018), pp. 457-467.
[326] Lice za zaštitu podataka mora biti imenovano u organima javne vlasti (osim suda u vezi sa sudskim ovlašćenjima), kada se osnovne aktivnosti rukovaoca/obrađivača sastoje od obrade koja po svojoj prirodi, obimu i svrsi zahteva redovan i sistematski nadzor velikog broja lica i kada su osnovne aktivnosti rukovaoca/obrađivača usmerene na obradu posebnih podataka o ličnosti. Više o obavezi imenovanja lica za zaštitu podataka u organima uprave vid. S. Andonović, „Obaveza imenovanja lica za zaštitu podataka u organima uprave“, str. 48-53.

strukture. Kada se odredi, ime i prezime ovog lica, kao i njegovi kontakt podaci moraju biti dostupni na internet prezentaciji rukovaoca ili obrađivača, a ujedno se i dostavljaju Povereniku.

Prema Zakonu o zaštiti podataka o ličnosti, lice za zaštitu podataka ima najmanje obavezu da:

1. informiše i daje mišljenje rukovaocu ili obrađivaču, kao i zaposlenima koji vrše radnje obrade o njihovim zakonskim obavezama u vezi sa zaštitom podataka o ličnosti,

2. prati primenu odredbi ovog zakona, drugih zakona i internih propisa rukovaoca ili obrađivača koji se odnose na zaštitu podataka o ličnosti, uključujući i pitanja podele odgovornosti, podizanja svesti i obuke zaposlenih koji učestvuju u radnjama obrade, kao i kontrole,

3. daje mišljenje, kada se to zatraži o proceni uticaja obrade na zaštitu podataka o ličnosti i prati postupanje po toj proceni,

4. sarađuje sa Poverenikom, predstavlja kontakt tačku za saradnju sa Poverenikom i savetuje se sa njim u vezi sa pitanjima koja se odnose na obradu, uključujući i obaveštavanje i pribavljanje mišljenja o proceni uticaja.[327]

Važno je napomenuti da lice za zaštitu podataka ne snosi odgovornost za obradu podataka. Takva odgovornost ostaje na rukovaocu. Lice za zaštitu podataka predstavlja svojevrsnu pomoć u pronalaženju najboljih rešenja u vezi sa procesima obrade, kojima se izbegavaju kazne za nepoštovanje prava građana u ovoj oblasti. Jednostavno, usmerenost na osnovne delatnosti često će imati za posledicu nepoznavanje ili zaboravljanje pojedinih dužnosti u komplikovanoj oblasti zaštite podataka o ličnosti. Zbog toga se i imenuje lice za zaštitu podataka kako bi pomoglo, olakšalo i ukazalo na eventualne propuste, mogućnost poboljšanja rada i akata u vezi sa pojedinim elementima obrade, itd. Određenjem ovog lica kao kontakt tačke sa Poverenikom i drugim licima (klijentima), izbegavaju se nesporazumi i neefikasni razgovori u vezi sa podacima građana koji mogu uticati na smetnje u vezi sa radom i osnovnim delatnostima rukovaoca ili obrađivača. Zbog svega toga, imenovanje lica za zaštitu podataka predstavlja značajan institut u ovoj oblasti zaštite podataka koja je u nastajanju.

5.3.1.9. Prenos podataka o ličnosti u druge države i međunarodne organizacije

Opšte je pravilo da nacionalni propisi važe samo na teritoriji države na kojoj su doneti. Tako je i u oblasti zaštite podataka o ličnosti. Međutim, internet i

[327] Čl. 58 Zakona o zaštiti podataka o ličnosti.

informaciono-komunikacione tehnologije omogućile su da se podaci, posebno u digitalnom obliku, efikasno i lako prenose u velikim količinama u strane države i međunarodne organizacije. Na taj način izbegava se primena domaćeg zakonodavstva i „domaća" zaštita podataka, budući da oni postaju predmet interesovanja druge države u koju su podaci preneti.

Zbog toga, domaći zakonodavac predviđa pravila vezane za mogućnost prenosa podataka o ličnosti u strane države ili međunarodne organizacije, kako bi se, u najvećem mogućem obimu, zaštitila privatnost građana i van granica domaće države. To znači da se legalno može izvršiti samo onaj prenos koji je u skladu sa odredbama Zakona o zaštiti podataka o ličnosti.

Kao osnovno pravilo, za koje se ne zahteva prethodno odobrenje Poverenika, postavljen je *prenos podataka na osnovu primerenog nivoa zaštite*. Primereni nivo zaštite znači da država, međunarodna organizacija ili neki sektor u okviru ovih entiteta, gde se prenose podaci, garantuje primereni stepen nivoa zaštite podataka o ličnosti. Strana država ispunjava ovaj uslov ukoliko je pristupila Konvenciji Saveta Evrope 108 o zaštiti lica u odnosu na automatsku obradu ličnih podataka.[328] Ova pretpostavka je oboriva, po posebnoj odluci Vlade da pojedina država ne ispunjava odgovarajući stepen zaštite. Takođe, kada nadležni organi EU utvrde da država ili međunarodna organizacija garantuje primereni nivo zaštite, moguć je prenos bez odobrenja, ali tek pošto se takva lista potvrdi u *Službenom glasniku* Republike Srbije.[329] Na ovaj način se olakšava kretanje podataka, isto kao i kretanje podataka građana EU, čime se usaglašavaju pravila dva sistema, ali donekle i smanjuje nivo zaštite domaćih državljana. Na kraju, primereni nivo zaštite podataka postoji i kada Srbija zaključi ugovor (sporazum) o prenosu podataka o ličnosti sa drugom državom ili međunarodnom organizacijom.

Kada nije ustanovljen primereni nivo zaštite podataka o ličnosti u stranoj državi ili međunarodnoj organizaciji, *prenos podataka mora se vršiti uz primenu odgovarajućih mera zaštite*. Postoje dve vrste odgovarajućih mera zaštite, u zavisnosti od toga da li se zahteva posebno odobrenje Poverenika ili ne. Kada je reč o pravno obavezujućim aktima organa vlasti, standardnim ugovornim klauzulama, obavezujućim poslovnima pravilima, kodeksima postupanja i izdatim

[328] Lista potpisnica Konvencije 108, https:// www.coe.int / en / web / conventions / full - list /-/ conventions/treaty/108/signatures?p_auth=Vq1GCrUz.

[329] U trenutku izrade rada, Evropska komisija je utvrdila da Okvir štita privatnosti primenjuju i ispunjavaju sledeće zemlje: Andora, Argentina, Kanada, Farska ostrva, Gernsej, Izrael, Ostrvo Men, Japan, Džersi, Novi Zeland, Švajcarska, Urugvaj, Sjedinjene Američke države, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents.

sertifikatima kao mehanizmima na osnovu kojih se vrši prenos, nije potrebno odobrenje Poverenika.

Posebno odobrenje Poverenika neophodno je kada se prenos vrši na osnovu ugovornih odredbi rukovalaca/obrađivača, kao ugovornih strana u različitim državama ili kada je reč o odredbama koje se unose u sporazum između organa vlasti, u vezi sa zaštitom prava privatnosti i podataka građana.[330]

U cilju poboljšanja zaštite privatnost u odnosu na delatnosti prenosa podataka, predviđena je i mogućnost donošenja *obavezujućih poslovnih pravila*, koje odobrava Poverenik. Obavezujuća poslovna pravila predstavljaju unutrašnja, interna pravila domaćeg rukovaoca ili obrađivača, kojima se regulišu pravila prenosa podataka o ličnosti unutar multinacionalne kompanije ili grupe privrednih subjekata. Na taj način olakšava se prenos unutar velikih kompanija koji posluju na teritoriji više država, ali se ujedno poboljšava kvalitet zaštite, budući da jedan državni organ proverava ispunjenost uslova za ova pravila i prenos podataka.

Postoji još jedan način prenosa podataka. On se primenjuje kada nije moguće primeniti pravila u vezi sa prenosom na osnovu primerenog nivoa zaštite ili uz odgovarajuće mere zaštite. U tom slučaju, podaci se mogu preneti, ali samo u *posebnim situacijama*, predviđenim zakonom, koje se odnose na:

1. pristanak lica čiji se podaci prenose, pri čemu se ovo lice mora obavestiti da nije moguć prenos na osnovu primerenog nivoa zaštite ili uz odgovarajuće mere,

2. neophodnost izvršenja ugovora između lica na koje se podaci odnose i rukovaoca ili za izvršenje predugovornih radnji po nalogu tog lica,

3. neophodnost zaključenja ili izvršenja ugovora u interesu lica na koje se podaci odnose,

4. prenos koji je neophodan za ostvarivanje važnog javnog interesa, pod uslovom da je takav interes propisan zakonom,

5. podnošenje, ostvarivanje i odbranu od pravnog zahteva,

6. neophodnost zaštite životno važnih interesa lica na koje se podaci odnose ili drugog lica, samo ako nisu u mogućnosti da daju pristanak,

7. potrebe prenosa podataka iz javnog registra, pri čemu su podaci dostupni bilo kom licu ili licu koje dokaže interes, u meri u kojoj su ti podaci dostupni.[331] *Čak i u slučaju da se prenos podataka ne može izvršiti u skladu sa pomenutim pravilima, prenos se može izvršiti ako su kumulativno ispunjene činjenice da se prenos podataka ne ponavlja, da se odnosi na ograničen broj lica, da je neophodan u cilju ostvarivanja legitimnog interesa rukovaoca koji preteže*

[330] Čl. 65 Zakona o zaštiti podataka o ličnosti.
[331] Čl. 69, st. 1 Zakona o zaštiti podataka o ličnosti.

nad interesima lica čiji se podaci obrađuju i ako su obezbeđene odgovarajuće mere zaštite.

5.3.1.10. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti

U oblasti zaštite podataka o ličnosti prelama se veliki broj privatnih i javnih interesa. Poput lica privatnog prava i državni organi prikupljaju i koriste podatke građana. Imajući u vidu da kontrolor teško može da kontroliše samog sebe, javlja se potreba za nezavisnim autoritetom u ovoj oblasti, koji će imati javna ovlašćenja u cilju zaštite različitih interesa i prava, ali istovremeno biti nezavisan od državne strukture. U tom cilju se osnivaju nadzorna tela u ovoj oblasti, koja predstavljaju državne organe koji su samostalni i nezavisni[332] od ostalih organa u vršenju svojih delatnosti.[333]

U Srbiji nezavisni nadzorni organ je Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (u daljem tekstu: Poverenik) koji obavlja svoje delatnosti u cilju zaštite osnovnih prava i sloboda fizičkih lica u vezi sa obradom njihovih podataka. Poverenik ne predstavlja ustavnu kategoriju, već je osnovan *Zakonom o slobodnom pristupu informacijama od javnog značaja 2004. god*,[334] kao Poverenik za informacije od javnog značaja. Tek kasnije, usvajanjem Zakona o zaštiti podataka o ličnosti iz 2008. godine, Poverenik u svoju nadležnost dobija i oblast zaštite podataka, kao srodnu oblast, pa i menja svoj naziv u današnji.

Što se tiče uslova za imenovanje, za Poverenika može biti izabrano lice s priznatim ugledom i stručnošću u oblasti zaštite i unapređenja ljudskih prava, koje ispunjava uslove za rad u državnim organima, koje je završilo pravni fakultet i ima najmanje deset godina radnog iskustva. Lice koje ispunjava uslove na funkciju Poverenika bira Narodna skupština većinom glasova narodnih poslanika, na predlog odbora Narodne skupštine nadležnog za informisanje, na period od sedam godina, uz mogućnost još jednog izbora.[335]

Poverenik je posebno nezavisno telo čija je nadležnost usmerena na obavljanje stručnih i kontrolnih poslova u vezi sa zaštitom prava i sloboda

[332] Više o nezavisnim telima vid. Ratko Marković, *Ustavno pravo i političke institucije*, Pravni fakultet Univerziteta u Beogradu, Beograd 2008, str. 518-524.

[333] Stefan Andonović, „Pravna priroda Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti“, *Arhiv za pravne i društvene nauke*, Savez udruženja pravnika Srbije i Republike Srpske, Institut za političke studije, Beograd 2019, str. 205.

[334] Zakon o slobodnom pristupu informacijama od javnog značaja, „Sl. glasnik RS“, br. 120/2004.

[335] Čl. 30 Zakona o slobodnom pristupu informacijama od javnog značaja.

građana u oblasti informacija od javnog značaja i zaštite podataka o ličnosti, što govori o kompleksnoj pravnoj prirodi i složenoj funkciji koje ovo telo ima u pravu Srbije.[336] Na osnovu takvih karakteristika, Poverenika možemo odrediti kao nezavisno nadzorno i kontrolno telo.[337]

Nezavisnost Poverenika je dvostruka, *funkcionalna i finansijska*. *Funkcionalna nezavisnost* se odnosi na slobodno obavljanje poslova iz njegove nadležnosti, bez prava bilo kog drugog organa ili lica da se meša u vršenje njegovih poslova i ovlašćenja. Naravno, ova vrsta nezavisnosti nije apsolutna, posebno u pogledu Narodne skupštine koja ga bira, može da ga razreši i kojoj odgovara za svoj rad podnošenjem redovnog i vanrednih izveštaja. Takođe, sudovi i tužilaštva, po prirodi stvari, mogu da vrše kontrolu zakonitosti nad radom Poverenika. Pod funkcionalnom nezavisnošću podrazumeva se i nespojivost obavljanja drugih poslova sa funkcijom Poverenika. *Finansijska nezavisnost* znači da se za rad Poverenika obezbeđuju sredstva iz posebnih budžeta države. Poverenik ima platu u rangu sa platama sudija najvišeg suda u Srbiji, što govori o važnosti njegove uloge. Osim toga, finansijska sredstva Poverenik koristi za zapošljavanje stručnog i profesionalnog kadra koji čine kancelariju Poverenika, kao i za naknadu troškova koje ima prilikom vršenja ovlašćenja.

Poverenik u svojoj nadležnosti ima veliki broj poslova. Osnovni zadatak Poverenika u oblasti zaštite podataka tiče se vršenja nadzora nad primenom i obezbeđivanja pravilne primene Zakona o zaštiti podataka o ličnosti. Jedan od važnijih poslova odnosi se na postupanje po pritužbama lica na koje se podaci odnose, tako što utvrđuje da li postoji povreda i, ukoliko postoji, stara se o sankcionisanju lica koja su povredu učinila, kao i o saniranju posledica.

Pomenuli smo da su građanima garantovana određena prava u vezi sa podacima o ličnosti. Inicijalni akt za njihovo ostvarenje, odnosno zahtev za pristup podacima, za ispravku i dopunu, brisanje, ograničenje obrade, prenos podataka, prekid obrade ili neprimenjivanje odluke zasnovane na automatizovanoj obradi podnosi se rukovaocu.[338] Na taj način ostvaruje se pravo građana na pravno sredstvo, odnosno zaštita njihovih prava pred državnim organom ili licem privatnog prava koje se nalazi u ulozi rukovaoca. Podnošenje pritužbe Povereniku ne utiče na mogućnost pokretanja drugih upravnih ili sudskih postupaka radi zaštite privatnosti. U izvršenju ove vrste posla, značajnu pomoć pružaju

[336] Marko Davinić, *Nezavisna kontrolna tela u Republici Srbiji*, Dosije, Beograd 2018, str. 23.

[337] Više o pravnoj prirodi Poverenika u pravu Srbije vid. S. Andonović, „Pravna priroda Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti“, str. 205-220.

[338] Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, *Ovlašćenja Poverenika*, https://www. poverenik.rs/sr-yu/za%C5%A1tita-podataka/ovlascenja-poverenika-zp.html.

inspekcijska ovlašćenja Poverenika.[339] Važno je pomenuti da su i odluke Poverenika podložne sudskoj kontroli u upravnom sporu pred Upravnim sudom, što je jedno od pravnih sredstava predviđenih Zakonom o zaštiti podataka o ličnosti.

Podizanje svesti rukovaoca i obrađivača je još jedan posao putem koga se postiže kvalitetniji sistem zaštite podataka. Prevencija je jedan od najvažnijih principa Poverenikovog rada, pa tako on podstiče izradu kodeksa postupanja i sačinjava brojne druge akte koji doprinose adekvatnijoj primeni normi iz oblasti zaštite podataka o ličnosti. Poslovi Poverenika su usmereni i prema državnim organima, pa tako on daje mišljenje Narodnoj skupštini, Vladi, drugim organima vlasti i organizacijama o zakonskim i drugim merama koje se odnose na zaštitu prava i sloboda fizičkih lica u vezi sa obradom. Osim na unutrašnjem planu, Poverenik deluje i na „spoljnom", tako što sarađuje sa nadzornim organima stranih država, posebno u pogledu izvršavanja domaćih odluka i načina primene prava.

Na osnovu svega navedenog možemo zaključiti da Poverenik predstavlja „vrhunski autoritet" u oblasti zaštite podataka o ličnosti u Srbiji, odnosno, najznačajniji je organ javne vlasti u ovoj oblasti. Njegova pravna priroda, ovlašćenja i poslovi usmereni su na širok spektar delatnosti prema svim licima koja su, na direktan i indirektan način, uključeni u proces obrade podataka.

5.3.1.11. Pravna sredstva, odgovornost i kazne

Pored Poverenika, značajnu ulogu u poštovanju ljudskih prava, posebno prava na privatnost i kontroli zakonitosti obrade podataka o ličnosti imaju i sudovi. Sudska vlast je nezavisna od drugih grana vlasti, što omogućava nepristrasnost u odlučivanju i nadzoru nad nezavisnim kontrolnim telom – Poverenikom. Osnovni cilj sudske zaštite jeste da pruži zaštitu pravima, slobodama i interesima građana. Pravo građana na sudsku zaštitu ličnih podataka garantovano je Ustavom,[340] a detaljnije je uređeno Zakonom o zaštiti podataka o ličnosti.

Sudsku zaštitu podataka o ličnosti u Srbiji možemo podeliti na četiri oblika. *Prvi* se odnosi na sudsku zaštitu u odnosu na odluke Poverenika, *drugi* se odnosi na pružanje sudske zaštite u slučaju povrede podataka od strane rukovaoca i obrađivača, *treći oblik* se odnosi na naknadu štete zbog povrede podataka i odredaba Zakona o zaštiti podataka o ličnosti, dok se *četvrti oblik* odnosi na

[339] Više o inspekcijskim ovlašćenjima Poverenika vid. čl. 79 Zakona o zaštiti podataka o ličnosti.
[340] Čl. 42, Ustava Republike Srbije.

sudske postupke koji se vode zbog učinjenih prekršaja u vezi sa podacima o ličnosti.[341]

5.3.1.12. Sudska zaštita u odnosu na odluke Poverenika

Lice koje je nezadovoljno odlukom Poverenika koja se na njega odnosi, ima pravo da protiv te odluke pokrene upravni spor. Upravni spor se pokreće tužbom pred Upravnim sudom. U ulozi tužioca može se naći lice čiji se podaci obrađuju, rukovalac, obrađivač i ostala fizička lica na koje se odnosi odluka Poverenika. Spor se pokreće u roku od 30 dana od prijema odluke Poverenika.

Pored toga, upravni spor se može pokrenuti i zbog nepostupanja Poverenika. U slučaju da Poverenik ne postupi po pritužbi, odnosno ne donese odluku u roku od 60 dana od dana izjavljivanja pritužbe, lice koje je izjavilo pritužbu ima pravo da pokrene upravni spor sa zahtevom da sud obaveže Poverenika na donošenje odluke. Mogućnost vođenja ove vrste upravnog spora istovetna je upravnom sporu zbog „ćutanja uprave".[342]

Upravni sud ispituje samo zakonitost odluke, odnosno nepostupanja Poverenika i ne upušta se u celishodnost i pravilnost njegovog odlučivanja. To znači da sud ispituje samo pravilnost postupanja Poverenika po zakonskim odredbama, a ne zalazi u stručnost odlučivanja Poverenika u vezi sa samom materijom – zaštitom podataka o ličnosti, budući da je Poverenik stručan i nezavisan organ u ovoj posebnoj oblasti. Pokretanje ovog postupaka ne predstavlja smetnju za vođenje drugih upravnih i sudskih postupaka u vezi sa predmetom spora, odnosno povredom podataka o ličnosti ili zakonskih normi u vezi sa tim podacima. Dakle, moguće je istovremeno voditi više različitih sporova u vezi sa zloupotrebom ili povredom podataka o ličnosti.

5.3.1.13. Sudska zaštita u odnosu na povrede rukovaoca i obrađivača

Lice na koje se podaci odnose ima pravo da pred sudom traži zaštitu ukoliko smatra da su rukovalac ili obrađivač izvršenjem neke od radnji obrada postupili suprotno odredbama Zakona o zaštiti podataka o ličnosti i time povredili neko od posebnih prava u vezi sa podacima (pravo na pristup podacima, pravo na obaveštenost o obradi, pravo na zaborav, pravo na ispravku i dopunu podataka o

[341] Stefan Andonović (2019), str. 267.

[342] O upravnom sporu zbog ćutanja uprave vid. Ratko Radošević, „Upravni spor zbog ćutanja uprave", *Zbornik radova Pravnog fakulteta u Novom Sadu* br. 4/2015, Novi Sad 2015, str. 1971-1985.

ličnosti, pravo na ograničenje obrade, pravo na prenosivost podataka, prava u vezi sa automatskom obradom podataka i pravo na pravno sredstvo u vezi sa obradom).

U zavisnosti od toga koje je pravo povređeno, glasiće i tužbeni zahtev. Ukoliko je povređeno pravo na obaveštenost, tužba će biti usmerena na davanje informacije. U slučaju prava na ispravku i dopunu, tužbeni zahtev biće usmeren na ispravku odnosno brisanje podataka o ličnosti koji se nalaze kod rukovaoca. Takođe, tužbom za zaštitu prava može se zahtevati ograničenje obrade, davanje podataka u strukturisanom, uobičajeno korišćenom i elektronski čitljivom obliku, prenošenje podataka drugom rukovaocu i prekid obrade podataka.[343] Pored toga, tužbeni zahtev može da bude usmeren na donošenje utvrđujuće presude da se na njega ne odnosi odluka rukovaoca ili obrađivača koja je doneta na osnovu automatizovane obrade podataka.

Za ovaj sudski postupak predviđena je alternativna mesna nadležnost suda. Tužba se može podneti višem sudu u mestu prebivališta, boravišta ili sedišta rukovaoca ili obrađivača podataka ili prebivališta, odnosno boravišta lica na koje se podaci odnose. Na ovaj način povećava se stepen zaštite lica na koga se odnose podaci, budući da može da bira kom sudu će podneti tužbu radi zaštite svojih prava. Međutim, propisano je da se ova nadležnost ne odnosi na rukovaoce, odnosno obrađivače podataka koji pripadaju organima javne vlasti. Treba pomenuti i pravilo da je u sporovima zaštite prava u vezi sa podacima o ličnosti revizija uvek dozvoljena protiv pravosnažne sudske presude. Naravno, u ovim postupcima važe pravila parničnog postupka. Uvođenje sudske zaštite predstavlja logičan korak u poboljšanju pozicije građana u vezi sa podacima građana.[344]

5.3.1.14. Naknada štete zbog povrede podataka o ličnosti

Ukoliko su rukovalac/obrađivač radnjama obrade prouzrokovali štetu licu čiji su se podaci obrađivali, ono ima pravo da zahteva novčanu naknadu. Novčana naknada se može tražiti zbog pretrpljene materijalne ili nematerijalne štete[345] koja je nastala povredom odredaba Zakona o zaštiti podataka o ličnosti.[346] Uobičajeno, zahtev za naknadu štete će biti usmeren prema rukovaocu koji je odgovoran za

[343] Čl. 84, st. 2 Zakona o zaštiti podataka o ličnosti.

[344] O pitanjima nadležnosti kada je organ uprave u ulozi rukovaoca ili obrađivača obrade vid. S. Andonović, (2019), str. 271.

[345] Više o mogućnosti naknade nematerijalne štete kod povrede podataka o ličnosti vid. Dragan Prlja, Stefan Andonović, „Naknada štete kod povrede ličnih podataka“, *Odgovornost za štetu, naknada štete i osiguranje* (ur. V. Čolović, Z. Petrović), Valjevo – Beograd 2019.

[346] Čl. 86, st. 1 Zakona o zaštiti podataka o ličnosti.

radnje obrade. Ipak, za štetu može odgovarati i obrađivač, ali samo u slučaju da je propustio da preduzme neku od zakonskih obaveza koje se odnose na njega ili, ako postupa suprotno uputstvima koje je dobio od rukovaoca. Sva ostala pravila odštetnog prava primenjuju se i u slučaju potraživanja naknade štete nastale u vezi sa povredom podataka.

Oslobođenje od odgovornosti moguće je samo u slučaju da rukovalac/obrađivač dokažu da ni na koji način nisu odgovorni za nastanak štete, što znači da moraju da dokažu da je šteta nastala iz nekog drugog uzroka, a ne zbog njihovih radnji obrade. Kada postoji više rukovalaca ili obrađivača, oni za štetu odgovaraju solidarno, prema udelu u odgovornosti, s tim što zahtev tužioca za punom naknadom može da bude usmeren i samo prema jednom od njih.

5.3.1.15. Prekršajni postupak zbog povrede pravila u vezi sa podacima o ličnosti

Dok su prethodni oblici sudske zaštite usmereni prevashodno na zaštitu ličnih interesa, prekršajni postupak se vodi i radi zaštite javnih interesa. Prema Zakonu o prekršajima,[347] prekršaj je protivpravno delo koje je zakonom ili drugim propisom nadležnog organa određeno kao prekršaj i za koje je propisana prekršajna sankcija. Cilj novčanih kazni koje se izriču za prekršaje u vezi sa pravilima zaštite podataka o ličnosti jeste da na preventivan i delotvoran način kazne učinioca prekršaja i na taj način utiču na njega, ali i na ostala lica u sličnim situacijama da više ne čine takve radnje ili propuste.

Raspon novčanih kazni kreće se od 50.000 do 2.000.000 dinara za rukovaoce ili obrađivače koji imaju svojstvo pravnog lica, s tim što preduzetnici odgovaraju u blažem iznosu od 20.000 do 500.000 dinara, odnosno od 5.000 do 150.000 dinara za fizička lica i odgovorna lica u pravnom licu ili državnog organa. Kao što se može primetiti, zaprećene kazne su daleko blaže nego što je to predviđeno Opštom uredbom EU. Takva situacija se može posmatrati kroz dva aspekta. Blaže zaprećene kazne ostavljaju više prostora rukovaocima i obrađivačima da „prave greške“ koje mogu dovesti do zloupotrebe ili povrede ličnog podatka, pa bi strože zaprećene sankcije imale jače preventivno dejstvo. Sa druge strane, blaže kazne mogu delovati i afirmativno za strana ulaganja i dolazak inostranih kompanija u državu, upravo zbog blažih kazni, pa samim tim i povoljnijih uslova poslovanja.

[347] Zakon o prekršajima, „Sl. glasnik RS“, br. 65/2013, 13/2016 i 98/2016.

Zakon o zaštiti podataka o ličnosti predviđa brojne radnje kao prekršaje zbog kojih se mogu izreći pomenute novčane sankcije. Rukovalac, odnosno obrađivač biće kažnjen ukoliko:

1) *obrađuje podatke o ličnosti suprotno načelima obrade,*
2) *obrađuje podatke o ličnosti u druge svrhe, suprotno zakonu,*
3) *jasno ne izdvoji podatke o ličnosti koji su zasnovani na činjeničnom stanju od podataka o ličnosti koji su zasnovani na ličnoj oceni,*
4) *ako korišćenjem razumnih mera ne obezbedi da se netačni, nepotpuni i neažurni podaci o ličnosti ne prenose, odnosno da ne budu dostupni,*
5) *obrađuje podatke o ličnosti bez saglasnosti lica na koje se podaci odnose, a nije u mogućnosti da predoči da je lice na koje se podaci odnose dalo pristanak za obradu svojih podataka,*
6) *obrađuje posebne vrste podataka o ličnosti suprotno zakonu,*
7) *obrađuje podatke o ličnosti u vezi sa krivičnim presudama, kažnjivim delima i merama bezbednosti suprotno zakonu,*
8) *licu na koje se podaci odnose ne pruži odgovarajuće informacije o podacima koje se na to lice odnose,*
9) *licu na koje se podaci odnose ne stavi na raspolaganje ili ne pruži informacije kada obradu vrše nadležni organi u posebne svrhe,*
10) *ne pruži tražene informacije, ne omogući pristup podacima, odnosno ako ne dostavi kopiju podataka koje obrađuje,*
11) *ograniči delimično ili u celini pravo na pristup podacima licu na koje se podaci odnose,*
12) *ne ispravi netačne podatke ili ne dopuni nepotpune podatke,*
13) *ne izbriše podatke lica na koje se podaci odnose bez odlaganja u zakonom predviđenim slučajevima,*
14) *ne ograniči obradu podataka o ličnosti u slučajevima predviđenim zakonom,*
15) *ne izbriše podatke kada zakon to nalaže,*
16) *ne obavesti primaoca u vezi sa ispravkom, brisanjem i ograničenjem obrade,*
17) *ne informiše lice na koje se podaci odnose o odluci o odbijanju ispravljanja, brisanja, odnosno ograničavanja obrade, kao i o razlogu za odbijanje,*
18) *ne prekine sa obradom podataka nakon što je lice podnelo prigovor,*
19) *se donese odluka koja proizvodi pravne posledice po lice na koje se podaci odnose isključivo na osnovu automatizovane obrade,*

20) prilikom određivanja načina obrade, kao i u toku obrade ne preduzme odgovarajuće tehničke, organizacione i kadrovske mere,
21) se odnos između zajedničkih rukovaoca ne uredi na odgovarajući zakonom predviđen način,
22) poveri obradu podataka o ličnosti obrađivaču suprotno odredbama ovog zakona,
23) se podaci obrađuju bez naloga ili suprotno nalogu rukovaoca
24) ne obavesti Poverenika o povredi bezbednosti podataka,
25) ne obavesti lice na koje se podaci odnose o povredi bezbednosti podataka,
26) ne izvrši procenu uticaja na zaštitu bezbednosti podataka,
27) ne obavesti Poverenika, odnosno ne zatraži mišljenje Poverenika pre započinjanja radnje obrade u zakonom predviđenim situacijama,
28) ne odredi lice za zaštitu podataka o ličnosti kada je to obavezno,
29) ne izvrši svoje obaveze prema licu za zaštitu podataka o ličnosti,
30) se prenos podataka o ličnosti u druge zemlje i međunarodne organizacije vrši suprotno odredbama zakona o prenosu podataka,
31) ne obezbedi primenu efektivnih mehanizama poverljivog prijavljivanja slučajeva povrede ovog zakona, obrađuje podatke o ličnosti u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili istorijskog istraživanja ili u statističke svrhe suprotno zakonu.[348]

U odnosu na ove prekršaje primenjuje se postupak koji je predviđen Zakonom o prekršajima, što znači da postupak vodi i kazne izriče prekršajni sud. Ipak, u određenim situacijama Poverenik može da izrekne novčanu kaznu zbog prekršaja. Poverenik će izreći novčanu kaznu na osnovu prekršajnog naloga, ako je prilikom inspekcijskog nadzora utvrđeno da je došlo do prekršaja za koji je Zakonom o zaštiti podataka o ličnosti propisana novčana kazna u fiksnom iznosu.[349]

Na osnovu prekršajnog naloga Poverenika, rukovalac i obrađivač mogu biti kažnjeni ako ne upoznaju primaoca podataka sa posebnim uslovima obrade, ako ne dostave licu na koje se podaci odnose obrazloženu odluku u vezi sa njegovim podacima, odnosno ne obaveste ga o rokovima obrade, nastave sa obradom u cilju direktnog oglašavanja i posle izjavljivanja prigovora, ne odrede predstavnika u Srbiji, ne vode propisane evidencije o obradi ili ne objave kontakt podatke lica za zaštitu podataka o ličnosti.[350]

[348] Čl. 95 Zakona o zaštiti podataka o ličnosti.
[349] Čl. 79, st. 2, tač. 9 Zakona o zaštiti podataka o ličnosti.
[350] Čl. 95, st. 2 Zakona o zaštiti podataka o ličnosti.

5.3.1.16. Posebni slučajevi obrade podataka o ličnosti

U određenim situacijama moguće je da dođe do svojevrsnog „sukoba" dva ili više prava ili interesa. U tim situacijama važno je pronaći kompromisno rešenje kako bi svi interesi bili zadovoljeni, u meri u kojoj je to moguće. Pravo na zaštitu podataka o ličnosti jednog lica može da se suprotstavi nečijim interesima ili pravima i slobodama drugog lica. Zbog toga, Zakon o zaštiti podataka o ličnosti, po ugledu na Opštu uredbu EU, predviđa nekoliko posebnih slučajeva obrade koji predstavljaju načine rešavanja sukobljavanja više prava.

Sloboda izražavanja i informisanja ima veliku značaj za funkcionisanje društva i poslovnih tokova. Zahvaljujući njima, građani i privredni subjekti na osnovu dobijenih informacija mogu da usklade ili izmene svoje ponašanje, odnosno poslovanje. Međutim, prilikom informisanja građana neretko se koriste i različiti podaci o ličnosti. Ukoliko bi se u potpunosti primenjivale norme Zakona o zaštiti podataka o ličnosti, sloboda informisanja bi u velikoj meri bila uskraćena. Zbog toga, na obradu koja se vrši u svrhe novinarskog istraživanja i objavljivanja informacija u medijima, kao i u svrhe naučnog, umetničkog ili književnog izražavanja ne primenjuje se najveći deo sistem zaštite podataka u ličnosti.[351]

Uslov za neprimenjivanje takvih normi jeste neophodnost istraživanja i time ostvarivanje slobode izražavanja u konkretnom slučaju. Kako se navodi: „Izuzetak od primene određenih odredbi Zakona (o zaštiti podataka o ličnosti) važi tokom konkretne aktivnosti koja za svrhu ima novinarsko istraživanje i objavljivanje informacija, umetničko ili književno izražavanje. Nakon što je konkretna aktivnost gotova, sve podatke koji nisu potrebni trebalo bi obrisati ili anonimizovati".[352]

U vezi sa slobodom izražavanje jeste i *sloboda pristupa informacijama* kojima raspolažu organi javne vlasti. To su informacije koje su nastale u radu ili u vezi sa radom tih organa, pri čemu se odnose na sve ono o čemu javnost ima opravdan interes da zna.[353] Svako lice ima pravo da zahteva pristup ovakvim informacijama, pod određenim uslovima, i da ostvari uvid u njih. Međutim, ukoliko takva informacija sadrži podatke o ličnosti dolazi do suprotstavljenih

[351] Ne primenjuju se glave od II do VI, kao i članovi 89 do 94 Zakona o zaštiti podataka o ličnosti.

[352] Jelena Adamović, Milica Jovanović, Petar Kalezić, Nevena Krivokapić, Bojan Perkov, Andrej Petrovski, *Vodič za medije: Zaštita ličnih podataka i novinarski izuzetak*, SHARE fondacija, Beograd 2018, str. 42.

[353] Čl. 2, st. 1 Zakona o slobodnom pristupu informacijama od javnog značaja, „Sl. glasnik RS", br. 120/2004, 54/2007, 104/2009, 36/2010.

interesa slobode informisanja i zaštite privatnosti. Zbog toga ove interese treba istovremeno ostvariti, tako da oba prava budu zadovoljena.

Način zajedničkog ostvarivanja ovih prava predviđa Zakon o slobodnom pristupu informacijama od javnog značaja koji navodi da organ vlasti neće tražiocu omogućiti ostvarivanje prava na pristup informacijama od javnog značaja ako bi na taj način povredio pravo na privatnost, pravo na ugled ili koje drugo pravo lica na koje se tražena informacija lično odnosi, osim:

1. ako je lice (na koje se podaci odnose) na to pristalo,
2. ako se radi o ličnosti, pojavi ili događaju od interesa za javnost, a naročito ako se radi o nosiocu državne i političke funkcije i ako je informacija važna s obzirom na funkciju koju to lice vrši,
3. ako se radi o licu koje je svojim ponašanjem, naročito u vezi sa privatnim životom, dalo povoda za traženje informacije.[354]

U praksi, informacija od javnog značaja će biti data (data na uvid), ali će se ujedno zaštititi (obojiti crnom bojom ili precrtati tako da se ne mogu razumeti) svi podaci o ličnosti u dokumentu koji se izdaje. Na taj način dolazi do uspešne koegzistencije prava na zaštitu podataka o ličnosti i prava na slobodan pristup informacijama od javnog značaja.

Jedinstveni matični broj građana (JMBG) predstavlja važan podatak koji se koristi za identifikaciju lica u mnogim životnim situacijama i za ostvarivanje prava, interesa i sloboda građana. Iako se može definisati kao posebna kategorija podataka o ličnosti, na obradu JMBG-a primenjuju se odredbe posebnog zakona – *Zakona o jedinstvenom matičnom broju građana*.[355] Matični broj se određuje kao individualna i neponovljiva oznaka identifikacionih podataka o građaninu koji je državljanin Republike Srbije.[356] Poseban zakon, međutim, uređuje njegovu pravnu prirodu, način dodeljivanja i vođenja od strane organa uprave, ali ne pruža više informacija o njegovom korišćenju u pravnom prometu. Zbog toga, na zaštitu matičnog broja, kao podatka o ličnosti, treba primeniti Zakona o zaštiti podataka o ličnosti.

Dalje, na obradu podataka o ličnosti koji se koriste u vezi sa radom i zapošljavanjem fizičkih lica, primenjuju se odredbe posebne radno-pravne oblasti. U ovom slučaju treba primeniti *Zakon o radu*,[357] kao osnovni zakon u oblasti rada

[354] Čl. 14 Zakona o slobodnom pristupu informacijama od javnog značaja.
[355] Zakon o jedinstvenom matičnom broju građana, „Sl. glasnik RS“, br. 24/2018.
[356] Čl. 1 i 2 Zakona o jedinstvenom matičnom broju građana.
[357] Zakon o radu, „Sl. glasnik RS“, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017, 95/2018.

i zapošljavanja, *Zakon o državnim službenicima*,[358] kao i *kolektivne ugovore* (*primera radi*: Poseban kolektivni ugovor za zaposlene u osnovnim i srednjim školama i domovima učenika,[359] Poseban kolektivni ugovor za javna preduzeća u komunalnoj delatnosti na teritoriji Republike Srbije,[360] itd.).

Budući da ovi propisi ne uređuju detaljno sva pitanja u vezi sa zaštitom podataka, primeniće se sva opšta načela, prava i posebni instituti predviđeni Zakonom o zaštiti podataka o ličnosti. Ukoliko se ipak predviđaju odredbe u vezi sa zaštitom podataka, njima se moraju urediti i mere zaštite dostojanstva ličnosti, legitimnih interesa i osnovnih prava lica na koja se odnose, naročito u vezi sa prenosom podataka u okvirima multinacionalnih kompanija i grupa privrednih subjekata.[361]

Posebni slučajevi obrade jesu oni čija je svrha arhiviranje u javnom interesu, naučnom interesu, interesu istorijskog ili statističkog istraživanja. Kod obrada koje imaju neku od pomenutih svrha, potrebno je primeniti odgovarajuće mere zaštite koje su predviđene Zakonom o zaštiti podataka o ličnosti, tako da se ne ugrožava osnovna svrha ovih delatnosti. To znači da kada se preduzima neka radnja obrade u cilju ostvarivanja naučnog cilja, istorijskog istraživanja ili statistička obrada podataka, treba preduzeti mere koje onemogućavaju identifikaciju lica ili dalju identifikaciju, kada je to moguće i ako se svrha istraživanja može ispuniti i bez navođenja takvih podataka. Kako obrada u pomenute svrhe nema samo pojedinačan, već i širi društveni značaj, u ovim slučajevima ne mogu se ostvarivati posebna prava građana. Međutim, kada se osim u pomenute svrhe, podaci o ličnosti prilikom istih radnji obrade koriste i za neke druge svrhe, moraju se primeniti sve odredbe Zakona o zaštiti podataka o ličnosti.

Crkve i verske zajednice uživaju poseban status u društvu, pa je zbog toga obrada podataka o ličnosti koje one vrše za svoje potrebe označena kao posebna vrsta obrade.[362] Zakon o zaštiti podataka o ličnosti prihvata posebne načine

[358] Zakon o državnim službenicima, „Sl. glasnik RS“, br. 79/2005, 81/2005, 83/2005, 64/2007, 67/2007, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018.

[359] Poseban kolektivni ugovor za zaposlene u osnovnim i srednjim školama i domovima učenika, „Sl. glasnik RS“, br. 21/2015.

[360] Poseban kolektivni ugovor za javna preduzeća u komunalnoj delatnosti na teritoriji Republike Srbije, „Sl. glasnik RS“, br. 27/2015.

[361] Čl. 91, st. 2 Zakona o zaštiti podataka o ličnosti.

[362] Više o obradi podataka o ličnosti koje vrše crkve i verske organizacije vid. Stefan Andonović, „Zaštita podataka o ličnosti koje obrađuju crkve i verske zajednice u Republici Srbiji“, *Zbornik radova sa međunarodnog naučnog skupa „Državno-crkveno pravo kroz vekove“*, Institut za uporedno pravo, Pravoslavna Mitropolija Crnogorsko-primorska, urednici: Vladimir Čolović, Velibor Džomić, Vladimir Đurić, Miloš Stanić, Beograd – Budva 2019, str. 457-470.

obrade podataka vernika koji pripadaju crkvama i verskim zajednicama, pod uslovom da su takve obrade u skladu sa ovim zakonom. Pri tome, važno je imati na umu da se verska sloboda ne sme koristiti tako da ugrožava pravo na život, pravo na zdravlje, prava dece, pravo na lični i porodični integritet i pravo na imovinu,[363] što obuhvata i posebnu pažnju prema podacima o ličnosti kao važnom delu prava na lični integritet.

Obrada u humanitarne svrhe od strane organa vlasti predstavlja poslednji poseban slučaj obrade. Podaci o ličnosti koje obrađuju organi vlasti mogu se obrađivati i u cilju prikupljanja sredstava za humanitarne svrhe, uz primenu odgovarajućih mera zaštite prava i sloboda lica na koje se odnose.[364] Humanitarnim radom zadovoljavaju se širi društveni interesi i podstiče se društvena solidarnost, posebno prema ugroženim delovima društva, pa ovu vrstu rada treba pojednostaviti tako da se efikasno obavlja. Naravno, podatke o ličnosti koji se koriste u ovu svrhu, organi vlasti ne smeju dalje upotrebljavati za druge svrhe.

5.3.2. Zaštita podataka o ličnosti u posebnim propisima

Možemo reći da Zakon o zaštiti podataka o ličnosti ustanovljava temelje i osnovne institute u oblasti sistema zaštite podataka o ličnosti u Srbiji. Ipak, određene segmente i institute zaštite podataka možemo pronaći i u drugim propisima, odnosno zakonima koji uređuju posebne oblasti društvenog života. Na taj način dobija se zaokruženi sistem zaštite podataka koji se neprestano širi, otvaranjem novih društvenih oblasti i razvojem upotrebe podataka i rizika. Kako bi se uspešno zaštitila privatnost i podaci građana potrebno je uskladiti sve delove sistema i upodobiti ih osnovama koje su ustanovljene Zakonom o zaštiti podataka o ličnosti, što je i zakonska dužnost, pa u narednom periodu treba pristupiti usklađivanju posebnih zakona u ovoj materiji. Imajući u vidu rečeno, u ovom poglavlju pažnju ćemo posvetiti posebnim zakonima koji pažnju posvećuju i pitanjima u vezi sa zaštitom podataka o ličnosti.

[363] Čl. 3, st. 2 Zakona o crkvama i verskim zajednicama, „Sl .glasnik RS“, br. 36/2006.
[364] Čl. 93, st. 1 Zakona o zaštiti podataka o ličnosti.

5.3.3. Zakon o opštem upravnom postupku

Javna uprava predstavlja pojam koji obuhvata državne organe, organizacije, organe i organizacije pokrajinske autonomije, organe i organizacije jedinica lokalne samouprave, ustanove javna preduzeća, posebne organe preko kojih se ostvaruje regulatorna funkcija i pravna i fizička lica kojima su poverena javna ovlašćenja. Ovi organi obavljaju poslove iz svoje nadležnosti u javnom interesu, pa tako donose upravne akte, garantne akte, zaključuju upravne ugovore, preduzimaju upravne radnje i pružaju javne usluge.[365]

Kada postupaju u upravnim stvarima i obavljaju poslove iz svoje nadležnosti, organi uprave dužni su da postupaju po pravilima Zakona o opštem upravnom postupku. Ova pravila garantuju ostvarivanje prava i interesa građana u upravnom postupku i odgovarajuće ophođenje države prema njima.

U svom radu, prilikom postupanja u upravnim stvarima, organi uprave se u značajnoj meri oslanjaju na podatke građana. Zbog toga, kao jedno od osnovnih načela opšteg upravnog postupka postavljeno je načelo pristupa informacijama i zaštite podataka. Osim što ima dužnost omogućavanja pristupa informacijama od javnog značaja, upravni organ je dužan da pruži zaštitu tajnim i podacima o ličnosti u skladu sa posebnim zakonima.[366] Ovo načelo govori o velikom značaju podataka o ličnosti u upravnom postupku i skreće pažnju organima da vode računa o njihovoj zaštiti, što predstavlja jedan od osnovnih principa upravnog postupka. Naravno, način primene Zakona o zaštiti podataka o ličnosti i drugih propisa iz oblasti zaštite podataka o ličnosti poseduje određene specifičnosti u odnosu na organe uprave, posebno po pitanju mogućnosti pristupa podacima, prikupljanja i brisanja podataka (neretko ih ustanovljavaju organi države, pa se ne mogu brisati, osim ukoliko to nije posebno propisano), načina ostvarivanja pravnih sredstava, itd.[367]

5.3.4. Krivični zakonik

Podaci o ličnosti ne uživaju isključivo upravno i građansko pravnu zaštitu, već se štite i normama krivičnog prava, čime se ukazuje na značaj privatnosti u savremenom društvu. Pojedine radnje kojima se prekoračuju granice

[365] Čl. 2, st. 1 Zakona o opštem upravnom postupku.
[366] Čl. 15 Zakona o opštem upravnom postupku.
[367] Više o zaštiti podataka u javnoj upravi vid. S. Andonović (2019).

obrade podataka o ličnosti predstavljaju strogo zabranjeno ponašanje koje se Krivičnim zakonikom sankcioniše kao krivično delo.

U 14. glavi Krivičnog zakonika, koja uređuje krivična dela protiv slobode i prava čoveka i građanina, predviđeno je *krivično delo neovlašćenog prikupljanja ličnih podataka*.[368] Ko podatke o ličnosti koji se prikupljaju, obrađuju i koriste na osnovu zakona neovlašćeno pribavi, saopšti drugom ili upotrebi u svrhu za koju nisu namenjeni kazniće se novčanom kaznom ili zatvorom do jedne godine. Istom sankcijom će se kazniti lice koje protivno zakonu prikuplja podatke o ličnosti građana ili tako prikupljene podatke koristi. Kvalifikovani oblik ovog dela predviđen je za službeno lice koje izvrši neku od pomenutih radnji u vršenju službe, za šta je zaprećena kazna zatvora do tri godine.

Dakle, podaci o ličnosti se moraju koristiti u svrhu radi koje su prikupljeni i na način kako je to predviđeno Zakonom o zaštiti podataka o ličnosti. Svako neopravdano izlaženje van zakonskih granica predstavlja povredu koja može prouzrokovati krivičnu odgovornost rukovaoca, odnosno obrađivača, ali i drugih lica koji nemaju te uloge, ali su na neki način upoznata sa podacima o ličnosti. Kao što se može primetiti, ne zahteva se nikakva posledica, već je dovoljno da se učini nedozvoljena radnja pribavljanja, saopštavanja ili upotrebljavanja u druge svrhe.

Pored ovog krivičnog dela, u neposrednoj vezi sa podacima o ličnosti jeste i krivično delo neovlašćenog objavljivanja i prikazivanja tuđeg spisa, portreta i snimka, što znači da su zaštitni objekt podaci o ličnosti. Kada neko lice objavi ili prikaže lične podatke poput spisa, portreta, fotografije, filma ili fonograma, pri čemu ne postoji pristanak lica koje je spis sačinilo ili lica čiji se podaci nalaze na takvom spisu, fotografiji, filmu ili fonogramu, kazniće se novčanom kaznom ili kaznom zatvora do dve godine.[369] Uslov za izricanje sankcije jeste da je na taj način došlo do osetnog zadiranja u lični život lica koji se nalazi na spisu, fotografiji, filmu ili fonogramu. Osetno zadiranje u lični život može se odrediti kao neopravdano i nepotrebno otkrivanje sadržaja iz lične sfere koje to lice nije želelo, tako da se veći broj nepozvanih lica upoznaje sa određenim aspektom privatnog života pojedinca. Kvalifikovani oblik ovog dela vrši službeno lice koje radnju izvršenja učini u vršenju službe, za šta je zaprećena kazna zatvora do tri godine.

U ovim situacijama treba voditi računa i o *Zakonu o javnom informisanju i medijima*,[370] koji dozvoljava objavljivanje pojedinih podataka iz ličnog života

[368] Čl. 146 Zakonika o krivičnom postupku.
[369] Čl. 145, st. 1 Zakona o krivičnom postupku.
[370] Zakon o javnom informisanju i medijima, „Sl. glasnik RS“, br. 83/2014, 58/2015, 12/2016.

građana, kada postoji interes javnosti da se upozna sa pojedinom informacijom, što je osetljivo pitanje koje treba ocenjivati u svakom konkretnom slučaju.

*Primer za neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka nalazimo u praksi Vrhovnog kasacionog suda***.** U jedom predmetu, sud je pronašao sva subjektivna i objektivna obeležja bića ovog krivičnog dela kada su „okrivljena A. A. i okrivljeni B. B. kritičnom prilikom, po prethodnom dogovoru, neovlašćeno načinili više fotografskih snimaka privatne tužilje, bez njenog prethodnog ovlašćenja, dok je ista bila naga na plaži na kojoj je postavljenim znakom – tablama, fotografisanje zabranjeno, na način bliže opisan u izreci, pri čemu su bili uračunljivi i svesni svog dela i njegove zabranjenosti, čije izvršenje su hteli, čime su osetno zadrli u njen privatni život... kritičnom prilikom, okrivljena V. V. i okrivljeni G. G, po prethodnom dogovoru, neovlašćeno su objavili fotografije privatne tužilje Đ. Đ, sačinjene na način opisan u prvom stavu izreke navedene presude, tako što su bez pristanka privatne tužilje objavili fotografije u pisanom i elektronskom mediju "EE" i time osetno zadrli u njen lični život, pri čemu su bili svesni svog dela i hteli njegovo izvršenje i znali da je ono zabranjeno članom 80 Zakona o javnom informisanju i medijima.“[371]

Treba pomenuti da otkrivanje podataka o ličnosti neće predstavljati krivično delo kada je učinjeno radi odbrane od pravnog zahteva i zaštite ličnog interesa pred organima javne vlasti. „Kako se u konkretnom slučaju okrivljenom stavlja na teret da je predao sudu 15 fotografija i jedan DVD snimak, pravilno je prvostepeni sud primenom čl. 503 u vezi čl. 338 st. 1 t. 1 ZKP odbio privatnu tužbu privatnog tužioca iz razloga što predmetno delo nije krivično delo odnosno radnje „predaje i pokazivanja“ ne mogu se izjednačiti sa radnjom „objavljivanja ili prikazivanja“ u smislu kvalifikacije krivičnog dela iz čl. 145 KZ.“[372]

5.3.5. Zakon o radu

Jedan od posebnih slučajeva obrade prema Zakonu o zaštiti podataka o ličnosti odnosi se na oblast rada i zapošljavanja. Ovo ne čudi, s obzirom na pravnu prirodu odnosa poslodavca i zaposlenog, gde se poslodavac mora upoznati i sa pojedinim ličnim karakteristikama, odnosno podacima zaposlenog, kako bi se omogućilo zakonito i pravilno ispunjenje radnih zadataka. „Najviše se zlonamerno koriste podaci o zdravstvenom stanju, seksualnom opredeljenju,

[371] Iz obrazloženja presude Vrhovnog kasacionog suda, KZZ. 184/19 od 26.02.2019. god.
[372] Rešenje Osnovnog suda u Čačku K 398/16 od 16.11.2016. god, i rešenje Višeg suda u Čačku KŽ 119/16 od 09.01.2017. god.

privatnom ponašanju, kažnjavanju, stavovima i opredeljenima zaposlenih."[373] Zbog toga, pored osnovnog Zakona o zaštiti podataka o ličnosti, treba uvažiti i potrebe poslodavaca i pružiti mu mogućnost upoznavanja sa podacima o ličnosti, ali tako da se zaštiti privatnost zaposlenog ili kandidata.

Zakon o radu, kao osnovni zakon koji uređuje prava, obaveze i odgovornosti iz radnog odnosa, odnosno po osnovu rada,[374] posvećuje jedan član zaštiti podataka o ličnosti, kao meri zaštite zaposlenih. Zakon predviđa da zaposleni ima prava uvida u dokumente koji sadrže podatke o ličnosti koji se čuvaju kod poslodavca i pravo da zahteva brisanje podataka koji nisu od neposrednog značaja za poslove koje obavlja, kao i ispravljanje netačnih podataka. Na ovaj način konkretizuju se prava garantovana u Zakonu o zaštiti podataka o ličnosti, čiju primenu treba i ovde dozvoliti, posebno po pitanju pravnih sredstava u slučaju neostvarivanja pomenutih prava. Dalje, predviđena je i zabrana otkrivanja podataka o ličnosti zaposlenih trećim licima, osim u situacijama koje dozvoljavaju propisi. *Na ovom mestu treba pomenuti mišljenje ranijeg Ministarstva prosvete i sporta* da „se podaci o plati zaposlenog mogu smatrati ličnim, pa ne bi bilo poželjno da se s njima upoznaju treća lica. U tom smislu smatramo da odluka Školskog odbora da se pojedinačne plate istaknu na oglasnoj tabli škole i time podaci o plati postanu javni, ne bi bila ispravna."[375]

Imajući u vidu veliki broj ljudi koji može da se upozna sa podacima zaposlenih, predviđeno je da u okviru poslodavca, lične podatke zaposlenih može da prikuplja, obrađuje, koristi i dostavlja trećim licima samo zaposleni ovlašćen od strane direktora, čime se ograničava odgovornost direktora i ovlašćenog lice u okviru poslodavca.[376] U slučaju da tokom radnog odnosa dođe do promene podataka o ličnosti zaposlenog ili poslodavca, takva promena ne zahteva novi ugovor, već se može konstatovati i u aneksu ugovora.[377]

Pored Zakona o radu, važan radno pravni propis, kojim se uređuju prava i dužnosti značajnog broja državnih službenika i nameštenika predstavlja *Zakon o državnim službenicima***.** U okviru dostupnosti informacija o radu državnih službenika, predviđa se da je državni službenik dužan da u svom radu i prilikom obaveštavanja javnosti, obezbedi primenu mere zaštite podataka o ličnosti.[378] Dalje, prilikom objavljivanja odluka žalbene komisije o pitanjima koja su najčešći

[373] Senad Jašarević, „Zaštita ličnih podataka zaposlenih u srpskom i evropskom pravu", *Zbornik radova Pravnog fakultet u Novom Sadu*, br. 2/2009, Novi Sad 2009, str. 294.
[374] Čl. 1, st. 1 Zakona o radu.
[375] Mišljenje Ministarstva prosvete i sporta, br. 120-01-230/2007-02 od 20.03.2007. god.
[376] Čl. 83 Zakona o radu.
[377] Vid. čl. 172a, st. 3 Zakona o radu.
[378] Čl. 8, st. 2 Zakona o državnim službenicima.

predmet odlučivanja i o kome treba da bude obaveštena šira javnost, treba voditi računa o bezbednosti podataka o ličnosti. Takođe, ovim zakonom data je mogućnost Službi za upravljanje kadrovima da vrši obradu podataka upisanih u Centralnu kadrovski evidenciju u svrhu izvršavanja poslova iz svoje nadležnosti,[379] što znači da je zakonom predviđena svrha obrade i ti podaci se ne mogu obrađivati iz drugog razloga.

5.3.6. Zakon o poreskom postupku i poreskoj administraciji

Prilikom utvrđivanja, naplate i kontrole javnih prihoda upravni organi postupaju prema *Zakonu o poreskom postupku i poreskoj administraciji*.[380] Kao organ uprave u sastavu ministarstva nadležnog za poslove finansija, Poreska uprava je dužna da prema podacima o ličnosti do kojih dođe u svom radu, postupa na isti način kao i organ koji joj je te podatke dostavio. Obveznici dostavljanja podataka Poreskoj upravi jesu Agencija za privredne registre, sudovi, organi unutrašnjih poslova, banke i mnogi drugi. Naravno, u odnosu na podatke koje sama prikupi i obrađuje, Poreska uprava treba u svemu da primeni Zakon o zaštiti podataka o ličnosti.[381]

5.3.7. Zakon o javnim nabavkama

Zakon o javnim nabavkama[382] uređuje pitanja planiranja, nabavke, uslova, načina i postupka javne nabavke i druga pitanja od značaja za nabavku dobara, usluga ili radova od strane naručioca (organi javne vlasti i pravna lica u čijoj upravljačkoj ili nadzornoj strukturi učestvuje država).

Jasno je da se i u ovim postupcima koristi veliki broj podataka o ličnosti kojima treba pružiti zaštitu. Iako ne uređuje zaštitu podataka o ličnosti, ovaj zakon predviđa dužnosti naručioca u vezi sa zaštitom podataka. Te dužnosti se odnose na čuvanje kao poverljivih podataka o ponuđačima, odbijanje davanja informacije kojom bi se učinila povreda poverljivosti podataka iz ponude i čuvanje kao poslovne tajne svih podataka o imenima, zainteresovanim licima,

[379] Čl. 161, st. 6 Zakona o državnim službenicima.
[380] Zakon o poreskom postupku i poreskoj administraciji, „Sl. glasnik RS“, br. 80/2002, 86/2019.
[381] Čl. 29, st. 11 Zakona o poreskom postupku i poreskoj administraciji.
[382] Zakon o javnim nabavkama, „Sl. glasnik RS“, br. 124/2012, 14/2015, 68/2015.

ponuđačima, podnosiocima ponuda, itd.[383] Na primeru ove odredbe vidimo da podaci građana nekada prevazilaze lični interes i „ugrađuju se“ u poslovne i javne interese koji se štite i drugim institutima, pored onih koji su ustanovljeni sistemom zaštite podataka o ličnosti.

5.3.8. Porodični zakon

Porodični zakon,[384] kao zakon koji uređuje brak, odnose u braku i vanbračnoj zajednici, odnose deteta i roditelja, hraniteljstvo, starateljstvo, izdržavanje, imovinske odnose u porodici, zaštitu od nasilja u porodici i postupke u vezi sa porodičnim odnosima, ne sadrži detaljnije odredbe o zaštiti podataka maloletnih lica, odnosno dece. Deca predstavljaju kategoriju kojoj treba pružiti posebnu zaštitu, što se posebno odnosi na njihovu privatnost i podatke o ličnosti, budući da ona to sama ne mogu da učine. Predviđeno je da podaci iz sudskih spisa predstavljaju službenu tajnu koju su dužni da čuvaju svi učesnici u postupku, što se implicitno odnosi i na lične podatke.

Zakon o zaštiti podataka o ličnosti u vezi sa maloletnim licima predviđa samo granicu od 15 godina života za samostalno davanje pristanka na obradu podataka o ličnosti u vezi sa uslugama informacionog društva, ali ne uređuje posebne mere zaštite maloletnih lica. Smatramo da bi trebalo posebnu pažnju posvetiti regulativi u vezi sa maloletnim licima koji, u najvećoj meri, nisu svesni opasnosti koje vrebaju po njihovu privatnost i lične podatke, a o zaštiti ne bi trebalo da se staraju isključivo roditelji, već i država.

5.3.9. Zakon o zdravstvenoj zaštiti, Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva i Zakon o pravima pacijenata

Zakon o zdravstvenoj zaštiti[385] uređuje osnovne principe i elemente sistema zdravstvene zaštite u Srbiji. Kako podaci o ličnosti u vezi sa zdravljem predstavljaju posebno osetljivu kategoriju podataka, njima treba posvetiti dodatnu

[383] Čl. 14 Zakona o javnim nabavkama.
[384] Porodični zakon, „Sl. glasnik RS“, br. 18/2005, 72/2011, 6/2015.
[385] Zakon o zdravstvenoj zaštiti, „Sl. glasnik RS“, br. 25/2019.

pažnju.[386] Zbog toga, ovaj zakon predviđa da će vrsta i obim podataka, svrha obrade podataka, sadržaj podataka o zdravstvenom stanju, dostupnost podataka, mere njihove zaštite i druga pitanja od značaja za zaštitu podataka o ličnosti, biti uređena zakonom kojim se uređuje zdravstvena dokumentacija i evidencije u oblasti zdravstva i zakonom kojim se uređuju prava pacijenata.

Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva[387] kao jedno od osnovnih načela predviđa načelo zaštite podataka o ličnosti. U okviru ovog načela predviđa se da će se podaci o ličnosti, sadržani u medicinskoj i zdravstvenoj dokumentaciji, obrađivati u skladu sa načelima zaštite podataka o ličnosti, što pretpostavlja zakonitu, primerenu i srazmernu obradu podataka o ličnosti, koji moraju biti tačni, ažurni i na odgovarajući način zaštićeni od gubitka, uništenja, nedopuštenog pristupa, promene, objavljivanja i svake druge zloupotrebe.[388] Reč je, dakle, o principima koje predstavljaju temelje sistema zaštite podataka. Podaci iz medicinske dokumentacije, prema ovom zakonu, predstavljaju naročito osetljive podatke o ličnosti. Kategorija naročito osetljivih podataka o ličnosti bila je prisutna u ranijem zakonodavstvu (Zakonu o zaštiti podataka o ličnosti iz 2008. god.), ali je preimenovana u posebne kategorije podataka, pa takve izmene treba implementirati i u ovom posebnom zakonu.

Zdravstvene ustanove, privatne prakse i druga pravna lica imaju dužnost da prikupljaju i obrađuju podatke o ličnosti pacijenata na način na koji se obezbeđuje ostvarivanje njihovih prava, posebno prava na privatnost i prava na zaštitu podataka o ličnosti.[389] Važnu ulogu u čuvanju zdravstvenih podataka o ličnosti imaju zdravstveni radnici. U skladu sa tim, za njih je predviđena stroga dužnost očuvanja poverljivosti podataka za koje su saznali u obavljanju svoje delatnosti. Ipak, ova lica mogu biti oslobođena dužnosti čuvanja poverljivosti podataka isključivo na osnovu pisanog pristanka pacijenta, njegovog zakonskog zastupnika ili na osnovu odluke nadležnog suda.

Zanimljivo je pomenuti i jednu obavezu Zavoda za javno zdravlje u vezi sa povredama podataka, koja je ustanovljena kao posebno pravilo u odnosu na opšti sistem zaštite podataka. Naime, Zavod za javno zdravlje ima dužnost da o svakoj povredi bezbednosti podataka o ličnosti obavesti lice na koje se podaci

[386] Radoje Brković, Zoran Jovanović, Mirza Totić, „Pravo na privatnost i zaštitu ličnih podataka zaposlenog kao pacijenta u pravu Republike Srbije“, *Anali Pravnog fakulteta Univerziteta u Zenici*, vol. 13, br. 24, Zenica 2019, str. 205.

[387] Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva, „Sl. glasnik RS“, br. 123/2014, 106/2015, 105/2017, 25/2019.

[388] Čl. 7 Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva.

[389] Čl. 40, st. 2 Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva.

odnose, ministarstvo nadležno za poslove zdravlja i Poverenika.[390] Obaveštavanje ovih ustanova i lica ima za cilj da se deluje efikasno i sa različitih strana na povredu i spreče negativni efekti povrede, budući da se radi o podacima pojedinca koji mogu otkriti osetljive informacije iz života pojedinca i uticati na njegovu ličnu, profesionalnu i društvenu poziciju i status. Ukoliko Zavod za javno zdravlje propusti da obavesti ova lica o povredi kazniće se novčanom kaznom u iznosu od 50.000 do 2.000.000 dinara.

Pacijenti imaju pravo da ostvare uvid u svoje podatke o ličnosti koji se čuvaju u medicinskoj dokumentaciji. Mogućnost uvida treba da bude omogućena i preko interneta, ali samo u slučaju da se osiguraju mere zaštite podataka koje predviđa Zakon o zaštiti podataka o ličnosti. Mere bezbednosti i sigurnosti treba da primene sve zdravstvene ustanove, privatne prakse i druga pravna lica koja su deo medicinskog sektora.

Ovaj zakon predviđa i posebne kaznene odredbe u vezi sa eventualnom povredom podataka o ličnosti. To znači da, ukoliko u postupku prikupljanja i obrade podataka o ličnosti pacijenata zdravstvena ustanova i drugo pravno lice postupe tako da se naruši pravo na privatnost i pravo na poverljivost podataka o ličnosti pacijenata, biće kažnjeni novčanom kaznom u iznosu od 50.000 do 2.000.000 dinara.[391] Za isti prekršaj kazniće se i osnivač privatne prakse, samo što je zaprećen niži najviši iznos, od 500.000 dinara.

Zakon o pravima pacijenata[392] takođe koristi terminologiju starog zakona i određuje podatke o zdravstvenom stanju, kao i podatke iz medicinske dokumentacije kao naročito osetljive podatke o ličnosti. Takvim podacima smatraju se i podaci o ljudskim supstancama, kada se na osnovu njih može odrediti identitet lica na koje se odnose. Dužnost čuvanja tih podataka leži na svim zdravstvenim radnicima i saradnicima, ali i drugim licima koja su zaposlena u zdravstvenim ustanovama, privatnoj praksi, organizacionim jedinicama visokoškolskih ustanova, ustanovama zdravstvene struke, drugim pravnim licima koja obavljaju određene poslove iz oblasti zdravstvene delatnosti i pravnim licima koja su deo dobrovoljnog zdravstvenog osiguranja.[393]

Značajno pravo u vezi sa podacima o ličnosti u oblasti zdravstva jeste pravo uvida u medicinsku dokumentaciju. Osim samih pacijenata i članovi njihove uže porodice imaju pravo uvida u takvu dokumentaciju, ukoliko su ti podaci značajni za njihovo lečenje. Ovo je specifičan izuzetak od poverljivosti

[390] Čl. 44, st. 5 Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva.
[391] Čl. 53, st. 1, tač. 6 Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva.
[392] Zakon o pravima pacijenata, „Sl. glasnik RS“, br. 45/2013, 25/2019.
[393] Čl. 21, st. 2 Zakona o pravima pacijenata.

podataka, gde se, iz razloga zaštite zdravlja drugih lica, omogućava pristup i njima, iako se podaci ne odnose direktno na njih. Ukoliko se prekrši obaveza čuvanja ovih podataka ili se sa ovim podacima rukuje suprotno načinu postupanja sa njima, moguće je kažnjavanje lica koje je prekršilo te odredbe u iznosu od 300.0000 do 1.000.000 dinara.[394]

5.3.10. Zakon o sportu

Imajući u vidu da sport predstavlja društvenu delatnost u kojoj učestvuje veliki broj fizičkih lica, potrebno je osvrnuti se i na zaštitu podataka o ličnosti koja se koristi u sportskom sektoru za različite svrhe. Oblast organizacije sporta i fizičke aktivnosti, kao i prava i obaveza učesnika u ovim oblastima, uređena su Zakonom o sportu.[395]

Kod vođenja evidencija i drugih zbirki podataka, kao i prilikom izdavanja ili podnošenja dokumenta od strane svih učesnika u sistemu sporta, postoji dužnost poštovanja zaštite podataka o ličnosti i privatnosti. Posebnu pažnju na podatke o ličnosti treba da obrate nadležni nacionalni sportski savezi. Evidencije koje oni vode su predviđene Zakonom o sportu, a podaci iz tih evidencija čuvaju se 10 godina.[396]

Kako sektor sporta ne čine isključivo sportisti već je uključen i značajan broj lica koja imaju drugu osnovnu delatnost, predviđeno je da – za potrebe naučnoistraživačkog rada i prilikom izrade sportsko-političkih i statističkih analiza – treba primeniti sve mere zaštite podataka o ličnosti svih učesnika u sistemu sporta.[397]

5.3.11. Zakon o slobodnom pristupu informacijama od javnog značaja

Kao što smo pomenuli, obrade podataka o ličnosti koji se nalaze u okvirima informacija od javnog značaja uživaju poseban status. Zakon o slobodnom pristupu informacijama od javnog značaja, pored Zakona o zaštiti podataka o ličnosti, predviđa još jednu odredbu u vezi sa ovakvom obradom.

[394] Čl. 44, st. 1, tač. 6 Zakona o pravima pacijenata.
[395] Zakon o sportu, „Sl. glasnik RS“, br. 10/2016.
[396] Za više o sadržaju ovih evidencija vid. čl. 5, st. 2 Zakona o sportu.
[397] Čl. 5, st. 11 Zakona o sportu.

Naime, organ vlasti neće omogućiti tražiocu informacije ostvarivanje prava na pristup informacijama od javnog značaja, ukoliko bi na taj način povredio privatnost, pravo na ugled ili koje drugo pravo lica na koje se tražena informacija odnosi.[398] Ipak, od ovog pravila postoje izuzeci, u slučaju da je lice na koje se podaci odnose dalo pristanak, ukoliko je reč o ličnosti, pojavi ili događaju za koji je javnost zainteresovana i ako je lice svojim ponašanjem, posebno u vezi sa svojim privatnim životom, dalo povoda za tražene informacije. Na ovaj način učinjeno je normativno vaganje važnih interesa koji se neretko suprotstavljaju u svakodnevnom životu, pa je potrebno u svakom konkretnom slučaju obratiti pažnju na pretežnost interesa.

5.3.12. Propisi koji uređuju zaštitu podataka o ličnosti u sektoru bezbednosti

Kao što smo pomenuli, ovaj rad neće posvetiti pažnju pitanjima zaštite podataka o ličnosti u sektoru bezbednosti,[399] zbog brojnih specifičnosti i nešto drugačijeg režima i instituta zaštite podataka u odnosu na opšti. Osnovna pravila u vezi sa pitanjima iz ove oblasti mogu se naći u Zakonu o zaštiti podataka o ličnosti, gde su predviđeni brojni izuzeci. Takođe, pojedine odredbe se mogu pronaći i u Zakonu o policiji,[400] Zakonu o evidencijama i obradama podataka u oblasti unutrašnjih poslova,[401] Zakonu o bezbednosti saobraćaja na putevima,[402] Zakonu o privatnom obezbeđenju,[403] itd.

5.3.13. Zaključak

Regulativa u oblasti zaštite podataka nalazi se u većem broju zakona na kojima se dalje baziraju podzakonski opšti akti, kao i brojni pojedinačni pravni akti. Svi ti akti moraju se uskladiti sa Zakonom o zaštiti podataka o ličnosti, koji

[398] Čl. 14, st. 1, Zakona o slobodnom pristupu informacijama od javnog značaja.
[399] Više o zaštiti podataka u sektoru bezbednosti vid. OEBS*, Zaštita podataka u sektoru bezbednosti – Vodič kroz zakonsku regulativu*, (ur. Saša Gajin), Centar za unapređenje pravnih studija, Beograd 2019.
[400] Zakon o policiji, „Sl. glasnik RS“, br. 6/2016, 24/2018, 87/2018.
[401] Zakon o evidencijama i obradama podataka u oblasti unutrašnjih poslova, „Sl. glasnik RS“, br. 2018.
[402] Zakon o bezebednosti saobraćaja na putevima, „Sl. glasnik RS“, br. 41/2009, 53/2010, 101/2011, 55/2014, 96/2015, 9/2016, 24/2018, 41/2018, 87/2018, 23/2019.
[403] Zakon o privatnom obezbeđenju, „Sl. glasnik RS“, br. 104/2013, 42/2015, 87/2018.

uspostavlja osnove sistema zaštite podataka o ličnosti. Imajući u vidu brojnost posebnih propisa, posebnu pažnju treba usmeriti na edukaciju i informisanje onih lica koja primenjuju posebne zakone da moraju voditi računa o zaštiti podataka o ličnosti, u svakom konkretnom slučaju. Na taj način osiguraće se zakonito i pravilno obavljanje poslova, odnosno poštovanje zakonskih pravila, a ujedno će to biti put ka adekvatnoj zaštiti privatnosti građana čiji se podaci svakodnevno koriste u značajnom obimu. Osim propisa, za funkcionisanje sistema zaštite podataka neizmeran značaj imaju odluke upravnih i sudskih organa u ovoj oblasti.

6. PRAKSA ZAŠTITE POJEDINACA OD ZLOUPOTREBE PODATAKA O LIČNOSTI

6.1. Praksa zaštite pojedinaca od zloupotreba podataka o ličnosti u Evropi

Poštovanje fundamentalnih ljudskih prava, među kojima i prava na zaštitu podataka o ličnosti, garantovano je svim ljudskim bićima međunarodno-pravnim i nacionalnim propisima. Same garancije u međunarodnim i nacionalnim propisima samo su osnov za stvaranje efikasnih mehanizama za zaštitu pojedinaca od zloupotrebe podataka o ličnosti. Potrebno je da sve države obezbede stvarno uživanje zagarantovanih ljudskih prava stvaranjem efikasnih mehanizama zaštite, koji će odvratiti one koji žele da zloupotrebe podatke o ličnosti i ujedno ih efikasno kazniti.

Kvalitetna primena prava u velikoj meri zavisi od posledica kojima su izloženi oni koji su dužni da propise primenjuju, kako državne tako i nedržavne organizacije i pojedinci. Garantovanje prava utemeljenih najvišim pravnim aktima "mrtvo je slovo na papiru" ako nema njihove efikasne primene, koja podrazumeva i efikasno sankcionisanje onih koji krše propise koje su dužni da primenjuju.

Potpuno svesni ove činjenice o potrebi delotvorne primene propisa, poslanici Evropskog parlamenta i članovi Saveta EU prilikom pripreme i usvajanja Opšte uredbe EU, pored toga što su ustanovili najviše moguće standarde zaštite ličnih podataka, predvideli su i drakonski sistem sankcija. Kršenje ovog propisa donosi takve finansijske posledice koje mogu da otežaju, ili čak u potpunosti onemoguće poslovanje i najvećih kompanija, državnih institucija i ustanova. Sankcije mogu dostići milione, a u nekim ekstremnim slučajevima i milijarde evra. Opšta uredba EU u čl. 83 predviđa izricanje adminstrativnih novčanih kazni: za manja kršenja propisa u iznosu do 10 miliona evra, odnosno 2% ukupnog godišnjeg prometa u svetu za prethodnu finansijsku godinu, u zavisnosti od toga koji iznos je veći, a za veća kršenja propisa o zaštiti podataka do 20 miliona evra, odnosno 4% ukupnog godišnjeg prometa u svetu za prethodnu finansijsku godinu, u zavisnosti od toga koji iznos je veći.

Nacionalna zakonodavstva predviđaju tri vrste odgovornosti za kršenje odredaba koje se tiču zaštite ličnih podataka. To su prekršajna odgovornost

pravnih i fizičkih lica i organa vlasti, građanska odgovornost pravnih i fizičkih lica i organa vlasti, kada dođe do materijalne ili nematerijalne štete, i krivična odgovornost fizičkih lica za počinjena krivična dela predviđena nacionalnim zakonodavstvima.

Dosadašnje sankcionisanje zloupotrebe podataka o ličnosti od strane Evropskog suda za ljudska prava (ESLJP), Suda pravde EU i nacionalnih regulatornih tela za zaštitu podataka koji primenjuju Opštu uredbu EU, ukazuju na to da će zaštita pojedinaca od zloupotrebe podataka o ličnosti postajati sve delotvornija i da će pojedinci svoja zagarantovana prava zaista moći da ostvare.

6.1.1. Praksa zaštita pojedinaca od zloupotreba podataka o ličnosti Evropskog suda za ljudska prava

Evropski sud za ljudska prava (ESLjP), osnovan 1959. godine od strane Saveta Evrope, sa sedištem u Strazburu, ima zadatak da obezbedi da države članice poštuju prava i garancije koje su date *Evropskom konvencijom za zaštitu ljudskih prava* (EKLjP). Obezbeđivanje garantovanih prava pojedinaca, pa tako i prava na zaštitu podataka, ESLjP sprovodi kroz razmatranje predstavki podnetih od strane pojedinaca koji svoje pravo nisu mogli da ostvare pred nacionalnim pravosudnim i upravnim organima. Kada se ustanovi da je država prekršila jedno ili više prava, ESLjP donosi presudu. Presude su obavezujuće, a država na koju se presuda odnosi je u obavezi da deluje u skladu sa odlukom.

ESLjP je do sada doneo niz presuda koje se odnose i na zaštitu pojedinaca od zloupotrebe podataka o ličnosti. Izdvojili smo nekoliko najznačajnijih presuda koje se odnose baš na zaštitu podatka o ličnosti u okviru kršenja čl. 8 EKLjP. Član 8 EKLjP ima znatno širu primenu nego što je zaštita podatka o ličnosti, pa je ESLjP doneo i niz drugih presuda u vezi sa kršenjem prava na poštovanje privatnog i porodičnog života koje se odnose na zaštitu psihološkog i moralnog integriteta pojedinaca, kao i zaštitu identiteta i autonomije pojedinca.

Engleski državljanin Džefri Denis Pek podneo je tužbu protiv UK 1998. godine zbog ugrožavanja prava na privatnost.[404] On je avgusta 1995. godine bolovao od depresije i na ulici je kuhinjskim nožem pokušao da iseče vene i izvrši samoubistvo. Nije znao da ga snimaju kamere za video nadzor instalirane na administrativnoj ustanovi u toj ulici. Na osnovu tog snimka objavljene su dve

[404] Peck v. The United Kingdom (Application no. 44647/98), ECHR, https:// hudoc.echr.coe.int/ eng-press?i= 003-687182- 694690#{%22itemid%22: [%22003 -687182 -694690%22]}.

fotografije, u članku i na naslovnoj strani u lokalnim novinama, a kasnije i u drugim novinama, a lice podnosioca tužbe nije bilo sakriveno na fotografijama. Kasnije je deo video snimka objavljen na više televizija. Pošto je iscrpeo pravna sredstva unutar UK obratio se ESLjP, koji je konstatovao kršenje čl. 8 EKLjP. Sud nije našao da su postojali opravdani razlozi koji bi dozvolili otkrivanje identiteta, a objavljivanje je izvršeno *bez saglasnosti* podnosioca tužbe. Sud je smatrao da je objavljivanje snimka predstavljalo *nesrazmerno i neopravdano mešanje u privatni život*.

Državljanin UK podneo je 2000. godine tužbu protiv UK ESLjP zbog kršenja prava privatnosti *zbog nadzora korespondencije od strane poslodavca*.[405] Podnosilac tužbe je bio zaposlen na državnom koledžu, a tokom trajanja radnog odnosa njegovo korišćenje telefona, e-maila, i interneta bilo je podvrgnuto nadzoru u cilju da se utvrdi da li preterano upotrebljava sredstva u svojini koledža u privatne svrhe. ESLjP je u ovom slučaju došao do zaključka da je došlo do kršenja čl. 8 EKLjP. Podnosilac tužbe nije bio upozoren da će komunikacija koju ima biti praćena i osnovano je očekivao da će njegova privatnost biti zaštićena. Prema stavu ESLjP za postojanje kršenja čl. 8 EKLjP nebitna je činjenica da podaci do kojih je kolež došao nisu javno objavljeni i nisu upotrebljeni u disciplinskom ili drugom postupku. Sud je zaključio da *samo prikupljanje i čuvanje podataka* o ličnosti koji se odnose na telefonske pozive, korišćenje elektronske pošte i interneta, bez znanja podnosioca tužbe predstavlja povredu njegovog prava na poštovanje privatnog života u smislu čl. 8 EKLjP.

Jedna britanska i dve irske nevladine organizacije podnele su tužbu ESLjP protiv UK 2000. godine[406] zbog presretanja javnih komunikacija, telefona, faksa i elektronske pošte. Nakon što su iscrpli sva pravna sredstva unutar UK, podnosioci su se obratili ESLjP pozivajući se na kršenje čl. 8 EKLjP. ESLjP je zaključio da je došlo do povrede čl. 8 i *samim postojanjem propisa koji dozvoljava trajno praćenje komunikacija* koje ulaze u sferu privatnosti, a da javnosti nije bila dostupna nikakva jasna procedura oko prikupljanja podataka o ličnosti, pristupa tim podacima, korigovanju tih podataka, itd.

Tužbu protiv Finske podneo je njen državljanin 2002. godine[407] zbog kršenja čl. 8 EKLjP, povrede prava na poštovanje privatnog i porodičnog života. U martu 1999. na internet stranici za sklapanje poznanstva postavljen je oglas u

[405] Copland v. The United Kingdom (Application no. 62617/00), ECHR, https://hudoc. echr.coe. int/ eng#{%22itemid%22:[%22001-79996%22]}.

[406] Liberty and Others v. The United Kingdom (Application no. 58243/00), ECHR, https://hudoc. echr.coe.int/eng#{%22itemid%22:[%22001-87207%22]}.

[407] K. U. v. Finland (Application no. 2872/02), ECHR, https://hudoc.echr.coe.int/eng# {%22itemid %22:[%22001-89964%22]}.

kome su bili navedeni podaci o godini rođenja, njegov detaljan opis, broj telefona, i link ka internet stranici koju je posedovao. U oglasu je stajalo da podnosilac tužbe traži intimno poznanstvo. Za oglas je saznao nakon što je primio e-mail od osobe koja je odgovorila na oglas. U to vreme on je imao 12 godina. Njegov otac je kontaktirao policiju i tražio pokretanje odgovarajućeg postupka, ali je internet provajder odbio da obelodani identitet vlasnika IP adrese sa koje je postavljen oglas pozivajući se na zakon o tajnosti elektronskih komunikacija. Nakon što su iscrpljena sva pravna sredstva na nacionalnom planu, podneta je tužba ESLjP. Sud je prihvatio tužbu imajući u vidu *ugrožavanje prava na privatan i porodični život i štetu i opasnost po psihičko i mentalno zdravlje maloletnika* i došao je do zaključka da je u konkretnom slučaju došlo do kršenja čl. 8 EKLjP, jer nije obezbeđena odgovarajuća pravna zaštita i nije otkriven identitet počinioca.

Grčki državljani Dimitros Reklas i Vasiliki Davurlis, 2005. godine podneli su tužbu ESLjP[408] zbog kršenja prava na privatnost i porodični život na osnovu čl. 8 EKLjP. Podnosioci zahteva su roditelji sina, bebe koja je odmah po rođenju smeštena u sterilnu jedinicu privatne klinike da bi bila pod stalnim lekarskim nadzorom. Majci su uskoro bile predočene dve fotografije bebe koje je napravio profesionalni fotograf, jer je klinika nudila usluge profesionalnih fotografa. Podnosioci su se žalili zbog fotografija, smatrajući da je fotografisanje uznemirilo bebu, a oni nisu dali svoju saglasnost za fotografisanje. Pošto su iscrpli sva pravna sredstva unutar države, podnosioci su se obratili ESLjP. Sud je zaključio da su fotografije snimljene na mestu koje je bilo dostupno samo medicinskom osoblju, i da, iako nije došlo do javnog objavljivanja, postoji povreda prava na privatnost. Fotografija lika neke osobe predstavlja jednu od glavnih osobina njegove ili njene ličnosti, jer otkriva jedinstvene karakteristike po kojima se ta osoba razlikuje od drugih. *Pravo na zaštitu nečije fotografije je jedno od bitnih komponenata prava na lični razvoj* i pretpostavlja pravo na regulisanje uslova pod kojima se fotografija može koristiti. Podnosioci tužbe *nisu dali svoju saglasnost* za fotografisanje bebe, a ne radi se o "javnoj ličnosti" gde bi se javnim interesom moglo pravdati objavljivanje fotografije bez dozvole. Utvrđena je povreda prava na privatnost i dosuđena je naknada štete u iznosu od 8.000 evra.

Jedna osoba u Nemačkoj podnela je tužbu ESLjP[409] protiv Nemačke 2005. godine, zbog kršenja člana 8 EKLjP, odnosno zbog zakonske odredbe na osnovu koje je dozvoljen nadzor putem geolokalizacije, fotografije, video nadzora

[408] Reklos and Davourlis v. Greece (Application no. 1234/05), ECHR, https://hudoc.echr.coe.int/ eng#{%22itemid%22:[%22001-90617%22]}.

[409] Uzun v. Germany (Application no. 35623/05), ECHR, https://hudoc.echr.coe.int/ eng#{%22 itemid%22:[%22001-100293%22]}.

i drugih posebnih tehničkih sredstava u slučajevima "naročito teških" krivičnih dela. ESLjP je odbacio tužbu ocenjujući *da je prikupljanje podataka o ličnosti i drugih informacija o podnosiocu bilo opravdano sa stanovišta interesa nacionalne bezbednosti i radi sprečavanja vršenja krivičnih dela*, te je mešanje vlasti u privatni život podnosioca bilo *srazmerno cilju i neophodno u demokratskom društvu*.

Mihail Soro, državljanin Estonije, podneo je tužbu protiv Estonije 2008. godine,[410] Evropskom savetu za ljudska prava (ESLjP) smatrajući da mu je ugroženo pravo na privatnost, odnosno pravo na privatan i porodični život i pravo na zaštitu podataka jer su javno objavljene informacije o njegovom radu u službi za državnu bezbednost. Pošto je iscrpeo domaća pravna sredstava za zaštitu svojih interesa, podnosilac tužbe se obratio ESLjP pozivajući se na kršenja čl. 8 EKLjP. Sud je zauzeo stav da je objavljivanje informacije o njegovom radu u službi državne bezbednosti uticalo na njegovu reputaciju i da predstavlja mešanje u njegovu privatnost. Podnosilac tužbe je bio vozač i njegov posao na bilo koji način nije bio "opasan" pa je na taj način *mešanje u njegov privatni život bilo u disproporciji sa zaštitom javnog interesa*, a on je nakon objavljivanja morao da dâ otkaz i bio je šikaniran. Dosuđena mu je i naknada štete od 6.000 evra. Odluka Suda je postala konačna 3. septembra 2015. godine.

6.1.2. Praksa zaštita pojedinaca od zloupotreba podataka o ličnosti Suda pravde EU

Sud pravde EU, što je novi naziv ovog suda od Ugovora iz Lisabona 2009. godine, od svog osnivanja 1952, imao je suštinski isti zadatak jednake primene i tumačenja komunitarnog prava.[411] Ovaj sud EU, sa sedištem u Luksemburgu, za razliku od nacionalnih sudova, kod kojih postoji podela na opšte i posebne, u određenoj meri je i ustavni sud, upravni sud i građanski sud.[412] U funkciji ustavnog suda ovaj sud rešava sporove između komunitarnih organa i između tih organa i država članica, u funkciji upravnog suda on vrši kontrolu zakonitosti akata komunitarnih organa, a u funkciji građanskog suda on rešava građanske sporove kao što je naknada štete. Sud pravde EU danas čini 28 sudija koje sporazumno imenuju vlade država članica na period od 6 godina. Njegove

[410] Soro v. Estonia (Application no. 22588/08), ECHR, https://hudoc.echr.coe.int/ eng#{%22 itemid% 22:[%22001-156518%22]}.

[411] G. Gasmi, *Quo Vadis EU?: Relevantni pravni i institucionalni faktori*, Institut za uporedno pravo, Beograd, 2016, str. 194-195.

[412] Budimir Košutić, *Uvod u Evropsko pravo*, Zavod za udžbenike, Beograd, 2006, str. 141.

odluke obavezne su za države članice, pa on čak može naložiti državi članici plaćanje kazne ako utvrdi da se ona nije pridržavala odluke Suda pravde EU. Može se reći da je Sud pravde EU jedinstveni sudski organ, istovremeno međunarodnog i unutrašnjeg karaktera, sa značajnim nadnacionalnim karakteristikama koje se ogledaju i u tome da može svojim odlukama ustanovljavati prava i obaveze kako za države članice, tako i za fizička i pravna lica država članica.[413] Ovaj sud svojim tumačenjima deluje i kao stvaralac komunitarnog prava, pružajući svojim presudama putokaz za buduću primenu tog prava i pravni osnov za rešavanje budućih sporova.[414]

Povelja Evropske unije o osnovnim pravima iz 2000. godine, prvobitno samo politički dokument strateškog značaja, postala je pravno obavezujuća u momentu kad je Lisabonski ugovor stupio na snagu 1. decembra 2009.[415] Do donošenja Povelje EU o osnovnim pravima, pravo na zaštitu podataka nije eksplicitno bilo izdvajano kao posebno fundamentalno ljudsko pravo na istom nivou kao i druga fundamentalna ljudska prava, već se podrazumevalo da ono proističe iz prava na privatnost. Članom 8 Povelje garantuje se pravo na zaštitu podataka o ličnosti. U članu 8 se navodi da obrada podataka o ličnosti mora biti poštena, da se može vršiti samo u tačno određene svrhe, da mora biti zasnovana na pristanku određene osobe ili na legitimnom interesu utvrđenom zakonom. Pojedinci moraju imati pravo pristupa svojim ličnim podacima, pravo ispravke i da poštovanje prava na zaštitu podataka o ličnosti mora biti pod nadzorom nezavisnog organa.[416] Pošto Sud pravde EU ima zadatak da primenjuje i tumači pravo EU on je to činio i kada je u pitanju, Poveljom EU i članom 8, garantovano pravo na zaštitu podataka, a činio je to i pre donošenja Povelje na osnovu primene i tumačenja Direktive o zaštiti podataka iz 1995. godine i drugih propisa EU koji su garantovali zaštitu privatnosti i, u okviru nje, zaštitu podataka.

U slučaju C-275/06 *Promusicae* iz 2006. godine,[417] Sud pravde EU je razmotrio da li zakonodavstvo EU zahteva od država članica da usvoje nacionalno zakonodavstvo kojim se internet provajderi obvezuju da dostavljaju podatke o ličnosti navodnih prekršitelja autorskog prava vlasnicima autorskih prava radi olakšavanja parničnog postupka. Konkretno, španski sud pitao je Sud pravde EU da li pozitivna obaveza davanja takvih podataka o ličnosti vlasnicima autorskih prava proizlazi iz tri direktive EU. Sud pravde je prvo preformulisao pitanja koja

[413] G. Gasmi (2016), str. 195-198.
[414] *Ibid.*, str. 206.
[415] *Ibid.*, str. 82.
[416] Charter of fundamental rights of the European Union, Official Journal of the European Communities, C 364/5, 18.12.2000.
[417] C-275/06 Promusicae, CJEU.

je postavio nacionalni sud uzimajući u obzir da li evropsko pravo o zaštiti podataka, posebno Direktiva o zaštiti podataka i Direktiva o privatnosti, onemogućava državi članici da postavlja takvu obavezu. Zatim se bavio pitanjem koje je postavio španski sud; da li direktive zahtevaju da država članica usvoji zakonodavstvo kojim se određuje takva obaveza. Konačno, Sud je razmotrio kakav bi uticaj Povelja EU, koja još nije bila obavezujuća za države članice, trebalo da ima na zaključke do kojih je došla u prva dva pitanja. Napomenuo je da činjenično stanje uključuje, s jedne strane, pravo na vlasništvo i efikasnu sudsku zaštitu, a s druge strane, pravo koje garantuje zaštitu podataka o ličnosti, a time i privatnost života. Sud pravde je u preliminarnoj presudi ukazao na potrebu usklađivanja zaštite različitih fundamentalnih prava, odnosno prava na poštovanje privatnog života s jedne strane, i prava na zaštitu imovine i delotvorni pravni leka, s druge strane.[418]

U slučaju *Bavarian Lager* iz 2007. godine,[419] Sud pravde EU je trebalo da odluči o odnosu između prava na zaštitu podataka i prava na slobodan pristup informacijama. Kompanija Bavarian Lager uputila je zahtev Evropskoj komisiji, u skladu s EU zakonodavstvom o pristupu dokumentima, kako bi dobila zapisnik sa određenog sastanka i imena učesnika sastanka. Komisija je podatke dostavila samo u anonimiziranom obliku na temelju toga da traženi podaci sadrže podatke o ličnosti i da otkrivanje podataka ne bi bilo u skladu s pravilima zaštite podataka koja važe za institucije EU. Od Opšteg suda EU zatraženo je da utvrdi je li odluka Komisije da odbije relevantne podatke pokazala ispravnu ravnotežu između slobode informiranja i zaštite podataka u pravnom poretku EU. Na presudu Opšteg suda EU, kompanija Bavarske Lager podnela je žalbu Sudu pravde EU, a on je zaključio da u svim situacijama u kojima se traži pristup dokumentu koji sadrži podatke o ličnosti EU pravila zaštite podataka postaju primenjiva u celosti. Praktična posledica ovog tumačenja Suda pravde EU je da pravila EU o zaštiti podataka moraju prevladati nad pravilima EU o slobodi informacija.[420]

U slučaju *Google v. Costeja* (*Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (*poznatija kao *Google v. Costeja)*[421] iz 2014.

---

[418] O. Lynskey, "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, 3/2014, p. 569-597, http://eprints.lse.ac.uk/57713.

[419] T-194/04 *Bavarian Lager v Commission* [2007] ECR II-3201, CJEU.

[420] O. Lynskey (2014), p. 579.

[421] Odluka Suda pravde Evropske unije u slučaju *Google v. Costeja* – Court of Justice of the European Union, *Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (Google v. Costeja), Case C-131/12, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131*.

godine, Sud pravde EU je odlučivao o pravu na zaborav. Iako je doneta od strane suda na teritoriji EU, značaj ove presude je mnogo širi i odnosi se na korisnike interneta širom sveta, a tekovina ove odluke našla je mesto u mnogim uporedno-pravnim sistemima.

Činjenično stanje u ovom slučaju se zasniva na tome da su španske novine *La Vanguardia* objavile 1998. godine dva obaveštenja o prinudnoj prodaji nepokretnosti advokata Marija Kostehe (*Maria Costeje*). Prinudna prodaja trebalo je da se izvrši radi namirenja duga iz socijalnog osiguranja. U međuvremenu, Kosteha je izmirio svoja dugovanja, ali informacije o prinudnoj naplati zbog duga ostale su na internetu. Kad god bi neko pretraživao njegovo ime na najpopularnijem internet pretraživaču (*Google*), pojavljivala bi se informacija o izvršenju na nepokretnostima radi namirenja duga.

Kako bi sačuvao svoj lični i poslovni ugled, Kosteha se obratio španskoj agenciji za zaštitu podataka sa prigovorom u kome je tražio da *Google Spain* ukloni sve sporne članke na internetu u vezi sa slučajem i da se naloži pomenutom pretraživaču da izbriše sve njegove lične podatke koji se pojavljuju prilikom pretraživanja njegovog ličnog imena. Takođe, Kosteha je zahtevao da novinarska agencija *La Vanguarida* povuče sve članke iz novina u vezi sa njim i njegovim sudskim postupkom. On je ukazao na to da je njegov slučaj okončan pre nekoliko godina, da više nije aktuelan, pa samim tim ne postoji potreba niti interes javnosti da bude upoznata sa detaljima slučaja.

Španska agencija za zaštitu podataka samo je delimično usvojila njegov prigovor. Prigovor je usvojen u delu koji se odnosi na *Google Spain* i zahtev da se povuku (obrišu) podaci Kostehe iz baza podataka pretraživača, kako bi se sprečio dalji pristup ovim podacima. Međutim, agencija je odbila njegov zahtev u delu koji se odnosi na članke novina *La Vanguaride*. Agencija je stala na stanovište da javnost ima interesa da bude upoznata sa takvim informacijama, pa samim tim je postojao i zakonski osnov za objavljivanje. Zbog ovakve odluke, *Google Spain* i *La Vanguaria* podneli su odvojene tužbe španskom sudu, zahtevajući poništaj navedene odluke agencije.

Španski sud je zatražio pomoć od Suda pravde EU u tumačenju određenih pitanja u vezi sa slučajem. Da li davalac usluge internet pretraživanja prilikom pružanja usluge pretraživanja interneta obrađuje lične podatke, ako su ti podaci dobijeni iz drugog izvora, a ne neposredno od lica čiji se podaci objavljuju? Da li je davalac usluge internet pretraživanja ujedno i rukovalac obrade podataka koji se objavljuju? I osnovno pitanje, da li imalac može zahtevati brisanje podataka iz rezultata pretrage određenog internet pretraživača?

Sud pravde EU dao je odgovore na sporna pitanja, uz osvrt na pojedina pitanja koja su stvarala dileme u praksi korišćenja podataka. Stanovište Suda pravde EU zasnivalo se na tome da se tadašnje evropsko zakonodavstvo u oblasti zaštite podataka (Direktiva 95/46/EZ) odnosi na organizacije u državama EU, ali i na organizacije izvan EU, ukoliko one pružaju usluge na tržištu EU. To je za konkretan slučaj bilo od velike važnosti, budući da se predmet odnosio na davaoca usluge internet pretraživanja (*Google*) koji deluje u brojnim državama, a ne samo u Španiji. Zbog sveopšte povezanosti putem interneta omogućena je konzistentnost objavljenih informacija svuda u svetu, pa odluka nema značaj samo za teritoriju EU. Dalje, Sud pravde EU je stao na stanovište da se *Google* može smatrati rukovaocem podataka koji se objavljuju na sajtu ovog internet pretraživača, budući da on utvrđuje načine i svrhu obrade. Internet pretraživač „prikuplja", „snima" i „organizuje" lične podatke prilikom pretraživanja ključnih reči korisnika.

Na kraju, utvrđeno je da Kosteha ima pravo da zahteva uklanjanje informacija sa internet pretraživača. Naime, obrada njegovih podataka imala je zakonit cilj koji je vremenom ispunjen, pa više ne postoji. Zbog toga je dalja obrada neprikladna, irelevantna i preterana u odnosu na svrhu radi koje su podaci prikupljeni i obrađeni, imajući u vidu da je od konkretnog slučaja prošlo dosta vremena.

Na ovaj način, *sud je formulisao pravo na zaborav podataka* u okviru prava EU, kao jedno od najvažnijih sredstava za zaštitu podataka, iako ga nije eksplicitno odredio pod takvim terminom. Kroz ovo pravo ostvaruje se načelo istine i tačnosti podataka koji se objavljuju. Ipak, sud je zaključio da ovo ovlašćenje (pravo) „nije apsolutne naravi, već u svakom konkretnom slučaju treba proceniti njegovu funkcionalnost u odnosu na druga prava i interese, kao što su sloboda izražavanja i sloboda medija".[422] Ova odluka uticala je na to da pravo na zaborav nađe svoje mesto u uporedno-pravnim propisima koji uređuju zaštitu podataka, kako u pravnom sistemu EU, tako i u pravnom sistemu Srbije.

[422] Maja Čolaković, Lana Bubalo, „Pravo na zaborav kao instrument zaštite prava ličnosti u Evropskoj Uniji", *Zbornik radova Pravnog fakulteta u Tuzli*, br. 2/2017 (ur. Vedad Gurda), Pravni fakultet u Tuzli, Tuzla 2017, str. 26.

6.1.3. Praksa zaštite pojedinaca od zloupotreba podataka o ličnosti na osnovu odluka nezavisnih organa zemalja EU

Primena Opšte uredbe EU u Evropi u protekle dve godine pokazala je da su posledice neusaglašenosti sa propisima o zaštiti podataka bile visoke novčane kazne i visok reputacioni rizik. Od početka primene Opšte uredbe EU do danas, regulatorna tela za zaštitu podataka u evropskim zemljama izrekla su preko 270 kazni sa različitim novčanim iznosima i po različitim pravnim osnovama.[423] Od svih tih slučajeva izdvajamo nekoliko onih koji su imali najteže posledice po kompanije, koje se nisu u potpunosti usaglasile sa zahtevima evropskih propisa u pogledu zaštite podatak ao ličnosti, a pre svega sa odredbama Opšte uredbe EU.

Francuski nezavisni organ za zaštitu podataka kaznio je 21. januara 2019. godine *Google* sa 50 miliona evra za kršenje čl. 12 Opšte uredbe EU zbog *nedostatka transparentnosti*, čl. 5 tj. *nedozvoljenog pravnog osnova za obradu podataka,* čl. 6, i *nedostatka pristanka* kod personalizovanih oglasa po čl. 7. Žalbe su bile podnete odmah po otpočinjanju primene Opšte uredbe EU, 25. i 28. maja 2018. godine, a bilo je potrebno šest meseci da bi se okončao postupak.

Poverenik za informacije UK je u julu 2019. godine predložio kaznu od 204,6 miliona evra za British Airways zbog kršenja čl. 32 Opšte uredbe EU, zbog toga što *nije primenio dovoljne tehničke i organizacione mere da osigura bezbednost podataka*. Taj propust je omogućio hakerima da ukradu lične podatke više od 500.000 klijenata avionske kompanije.

U julu 2019. Poverenik za informacije UK najavio je nameru kažnjavanja kompanije Marriott International sa 110,4 miliona evra zbog gubitka podataka o evidenciji 339 miliona hotelskih gostiju, od čega je 31 milion iz Evrope. Razlog kažnjavanja su *nedovoljne tehničke i organizacione mere za osiguranje informacione bezbednosti* po čl. 32 Opšte uredbe EU.

Poverenik za informacije UK je 20. decembra 2019. godine kaznio sa 320.000 evra farmaceutsku kompaniju Doorstep Dispensaree iz Londona jer *nije primenila dovoljne tehničke i organizacione mere da osigura bezbednost posebnih kategorija podataka pacijenata*. To su bili podaci o imenima, adresama, datumima rođenja, podaci o receptima i drugi podaci iz medicinskih kartona. Pored plaćanja kazni, Poverenik je zahtevao da se u roku od tri meseca poboljšaju svi postupci zaštite podataka.

Italijanski Poverenik za zaštitu podataka je 15. januara 2020. godine kaznio sa 27,8 miliona evra Italijanski telekom TIM zbog kršenja Opšte uredbe

[423] GDPR Enforcement Tracker, https://www.enforcementtracker.com/.

EU (čl. 6, čl. 17, čl. 21, i čl. 32). Nekoliko miliona pojedinaca je bilo pogođeno agresivnom marketinškom kampanjom korišćenjem bez pristanka ličnih podataka: imena i prezimena, adresa, telefona, poreskih brojeva, itd. Kažnjavanje je izvršeno po osnovu *nepostojanja adekvatnog pravnog osnova za obradu podataka*.

Austrijska agencija za zaštitu podataka je 23. oktobra 2019. godine kaznila austrijsku Poštu sa 18 miliona evra plus 1,8 miliona evra za troškove postupka. Razlog kažnjavanja bio je profilisanje 3 miliona austrijskih građana, prikupljanjem podataka o političkim interesima i sklonostima, koji su predati trećim licima. Osnov kažnjavanja bio je *nedovoljan pravni osnov za obradu podataka*, odnosno kršenje čl. 5 i čl. 6 Opšte uredbe EU.

Poverenik za zaštitu podataka i slobodu informacija u Berlinu je 30. oktobra 2019. godine kaznio kompaniju za prodaju nekretnina Deutsche Wohnen SE sa 14,5 miliona evra iz razloga što nisu omogućili brisanje podataka. Kompanija nije brisala podatke o stanarima koji su ranije prikupljeni, a nije postojala svrha zbog koje bi se ti podaci i dalje čuvali. Pravni osnov kažnjavanja bio je *nepoštovanje opštih principa obrade podataka* po čl. 25 Opšte uredbe EU.

Nemački Savezni poverenik za zaštitu podataka i slobodu informacija je 9. decembra 2019. godine kaznio sa 9,5 miliona evra kompaniju 1&Telecom zbog nepreduzimanja odgovarajućih radnji kako bi se sprečilo neovlašćeno pristupanje podacima kupaca. *Nisu preduzete odgovarajuće tehničke i organizacione mere radi zaštite ličnih podataka* u skladu sa čl. 32 Opšte uredbe EU.

Italijanska agencija za zaštitu podataka je, zbog kršenja čl. 5, čl. 6, čl. 17 i čl. 21 Opšte uredbe EU, izrekla kaznu od 8,5 miliona evra kompaniji "Eni Gas e Luce" zbog nezakonite obrade ličnih podataka u kontekstu reklamnih aktivnosti u vezi sa telemarketingom i prodajnim aktivnostima bez pristanka osoba koje su kontaktirane; nedostajale su i tehničke i organizacione mere, a podaci su čuvani duže od dozvoljenog vremena za čuvanje tih podataka. Kompanija nije imala adekvatan pravni osnov za obradu podataka. Ista kompanija je kažnjena i još jednom novčanom kaznom od 3 miliona evra po osnovu kršenja čl. 5 Opšte uredbe EU zbog *neadekvatnog pravnog osnova za obradu podataka*.

Nezavisni organi za zaštitu podataka u svim evropskim zemljama svakodnevno pokreću postupke u vezi sa propustima u oblasti zaštite podataka. Do sada su izrečene novčane kazne u Austriji, Belgiji, Bugarskoj, Kipru, Češkoj, Danskoj, Francuskoj, Nemačkoj, Grčkoj, Mađarskoj, Italiji, Letoniji, Litvaniji, Poljskoj, Portugalu, Rumuniji, Sloveniji, Slovačkoj, Švedskoj, Španiji, itd.

Visoke novčane kazne i efikasni postupci primer su delotvornosti pravnih lekova i najbolji su način za prevenciju budućih zloupotreba podataka o ličnosti.

6.1.4. Zaključak

Zloupotreba podataka o ličnosti pojedinaca konstantno je u porastu. Razlog tome je što se o svakom pojedincu danas prikuplja veliki broj podataka: gde se nalazi, kuda se kreće, od čega se leči, šta čita, šta gleda na televiziji, kakve sajtove pretražuje, kakva su mu politička i druga opredeljenja, šta kupuje, gde radi, u kojoj banci štedi, da li ima imovinu ili dugovanja, i slično. Takvi podaci su sve češće dostupni velikom broju institucija i pojedinaca, pa su i zloupotrebe ličnih podataka sve češće. Nastankom velikog broja podataka o svakom pojedincu, zapravo, dolazi do sukoba interesa pojedinca da kontroliše podatke koji se o njemu prikupljaju i sačuva svoju privatnost, sa jedne strane, i interesa institucija i drugih pojedinaca da zloupotrebom tih podataka stiču novac ili moć, sa druge strane. Očigledno sukobljeni interesi stvaraju rizik od povrede prava na zaštitu podataka o ličnosti – jednog u nizu univerzalnih prava i sloboda pojedinaca. Pošto je pravo na zaštitu podataka o ličnosti fundamentalno ljudsko pravo, njega garantuju, pre svega, EKLjP, Povelja EU o osnovnim pravima i Opšta uredba EU. To su propisi na bazi kojih ESLjP, Sud pravde EU, i regulatorna tela za zaštitu podataka na nacionalnom nivou obezbeđuju delotvornost pravnih normi, odnosno visoki nivo efikasne primene.

Da bi se prava pojedinaca na zaštitu ličnih podataka ostvarila, neophodno je da svi oni koji prikupljaju i obrađuju podatke u različite svrhe, kao rukovaoci i obrađivači, preduzmu sve neophodne mere kako bi uskladili svoje poslovanje sa najvišim standardima u oblasti zaštite podataka o ličnosti. Razlozi za ovakvo postupanje rukovalaca i obrađivača nisu samo ozbiljne posledice koje nastupaju zbog neusaglašenosti sa propisima o zaštiti podataka, već i potreba podizanja nivoa društvene odgovornosti. Delotvornost pravnih lekova meri se efikasnom primenom istih. ESLjP i regulatorna tela za zaštitu podataka o ličnosti u velikom broju evropskih zemalja, svojom praksom dokazuju da pravo na zaštitu podataka o ličnosti nije "mrtvo slovo na papiru", već je pravo koje pojedinci mogu ostvariti i na taj način se zaštititi od zloupotrebe podataka o ličnosti.

6.2. Praksa zaštite pojedinaca od zloupotreba podataka o ličnosti u Republici Srbiji

6.2.1. Praksa Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti

Od svog osnivanja, u okviru svoje nadležnosti, Poverenik je stvarao praksu u oblasti zaštite podataka donošenjem mišljenja, upozorenja, rešenja u postupku inspekcijskog nadzora. Pored toga, Poverenik je podnosio krivične prijave, kao i zahteve za pokretanje prekršajnog postupka u slučajevima kada je postojala sumnja da je došlo do povrede prava privatnosti ili određene odredbe zakonskih normi u oblasti zaštite podataka.

Značajna uloga i delatnost Poverenika uticala je na razvoj svesti građana o značaju i ulozi podataka o ličnosti u svakodnevnom životu, na način ophođenja kompanija prema podacima o ličnosti, ali i na pristup države ovoj delikatnoj materiji. Poverenik je tokom svog rada uspeo da kreira značajan broj odluka koje su uticale ne samo na stranke na koje se odnosi odluka, već i na izmenu zakonske regulative.

6.2.1.1. Mišljenja Poverenika

Poverenik se svojim mišljenjem izjasnio po pitanju starosne dobi maloletnika i mogućnosti davanja saglasnosti za obradu podataka o ličnosti. Naime, ranijim zakonodavstvom nije precizno definisana starosna granica koja određuje kada maloletna lica mogu da daju saglasnost na obradu svojih podataka o ličnosti. U okviru svog mišljenja Poverenik je stao na stanovište da je neophodno utvrditi konkretnu svrhu obrade podataka o ličnosti maloletnika, kao prethodno pitanja, a posle toga identifikovati relevantne propise u posebnim društvenim oblastima i utvrditi koju starosnu granicu treba primeniti, imajući u vidu da su predviđene različite starosne dobi u oblasti rada, zdravstva, sporta, itd.[424] Ovo pitanje rešeno je u novom Zakonu o zaštiti podataka o ličnosti, tako što dete koje je navršilo 15 godina života može dati pristanak na obradu svojih podataka o ličnosti. Tako je Poverenik posredno uticao na razvoj normative u oblasti zaštite podataka.

Na sličan način Poverenik je uticao na normativnu praksu davanjem mišljenja o statusu predstavništva i ogranka stranog pravnog lica u kontekstu

[424] Mišljenje Poverenika br. 011-00-00607/2013-05, od 16.10.2013. god.

iznošenja podataka i obaveze upisa u Centralni registar Poverenika.[425] Poverenik je tada naveo da „obavezu uspostavljanja i vođenja evidencija o podacima o ličnosti koje obrađuje predstavništvo stranog privrednog društva, odnosno ogranak privrednog društva i dostavljanja evidencije o zbirci podataka, odnosno promena u evidenciji podataka Povereniku radi upisa u Centralni registar ima strano privredno društvo, tj. strano pravno lice koje je osnovalo predstavništvo, odnosno privredno društvo koje je obrazovalo ogranak u Republici Srbiji, bez obzira da li obradu podataka o ličnosti vrši neposredno ili preko svog predstavništva, odnosno ogranka.“[426] Na taj način ukazano je na značaj podataka o ličnosti u oblasti kompanijskog prava i na potrebu uspostavljanja evidencije (po starom zakonodavstvu) čak i kada podatke obrađuju predstavnici stranih kompanija.

Jedno od najznačajnijih mišljenja Poverenika bilo je upućeno Ministarstvu pravde, a ticalo se Nacrta zakona o zaštiti podataka o ličnosti.[427] Naime, Poverenik je iskoristio svoje zakonsko ovlašćenje i pokušao svojim mišljenjem da utiče na izmenu normative u oblasti zaštite podataka. On je u svom mišljenju uputio kritike na pojedine odredbe nacrta novog zakona, od kojih su neke našle mesto u zakonskim odredbama, dok druge nisu prihvaćene. Među odredbama koje nisu prihvaćene, skrećemo pažnju na ukazivanje Poverenika na potrebu regulisanja video nadzora, kao izuzetno značajne oblasti zaštite podataka. Poverenik je predlagao da se usvoje novi članovi, čak 6, koji bi se odnosili na opšte obaveze u vezi sa video nadzorom, video nadzor u poslovnom prostoru, evidencijama o video nadzoru, video nadzor u stambenim zgradama, video nadzor privatnih stanova i kuća, kao i video nadzor javnih površina.[428] Smatramo da je potrebno urediti pitanje video nadzora, budući da može imati značajne implikacije na privatnost građana i njihove podatke o ličnosti, pa o ovom pitanju mišljenje Poverenika može da služi kao putokaz u razvoju zakonske regulative u budućnosti.

6.2.1.2. Upozorenja Poverenika

Jedno od upozorenja Poverenika odnosilo se na Ministarstvo unutrašnjih poslova koje je bilo rukovalac podataka u pogledu sistema za video nadzor kojim su se nadzirale i snimale saobraćajnice u Beogradu.[429] Poverenik je upozorio

[425] Mišljenje Poverenika br. 011-00-00272/2014-02 od 14.04.2014. god.
[426] Vid. Mišljenje Poverenika br. 011-00-00272/2014-02, str. 2.
[427] Mišljenje Poverenika br. 073-12-1090/2018-02.
[428] Vid. Mišljenje Poverenika br. 073-12-1090/2018-02, str. 22-25.
[429] Upozorenje Poverenika br. 164-00-00030/2011-07 od 31.03.2011. god.

MUP da je neophodno preduzeti dodatne mere tehničke, kadrovske i organizacione zaštite, kako bi se sistem video nadzora i prikupljanje podataka zaštitio od nedopuštenog pristupa, promene, objavljivanja i drugih vrsta zloupotrebe. U tom smislu, Poverenik je istakao da je neophodno da MUP propiše procedure kojima se reguliše prikupljanje ovih podataka i odrede lica koja bi rukovodila takvim sistemom, da je potrebno da nalozi za snimanje operatorski i supervizorski glase na individualno određena lica, a ne na radno mesto u okviru kojih se primenjuje video nadzor, budući da računarima tih radnih mesta može pristupiti veći broj lica. Takođe, Poverenik je upozorio na skladištenja podataka prikupljenih video nadzorom, kojima mogu pristupiti i određeni broj načelnika MUP, što povećava prostor za moguće zloupotrebe, pa je neophodno regulisati i ovo pitanje. MUP-u je ostavljen rok od 15 dana da obavesti Poverenika o preduzetim merama i planiranim aktivnostima za otklanjanje nepravilnosti.

Dalje, Poverenik je kontrolisao postupanje zdravstvenih ustanova privatnog sektora, pa je tako izdao upozorenje Domu zdravlja „Dr Ristić“, u cilju ustanovaljavanja odgovarajućih tehničkih, kadrovskih i organizacionih mera zaštite u vezi sa zbirkama podataka koji se čuvaju u drvenom ormanu, koji ne omogućava odgovarajuću zaštitu, pa je neophodno obezbediti stabilnije načine fizičke zaštite podataka, poput metalnih kutija sa sigurnosnom bravom i elektronskom evidencijom pristupa podacima.[430] Upozorenje Poverenika upućeno je i Republičkom zavodu za zdravstveno osiguranje zbog toga što nisu preduzete raspoložive tehničke mere koje se tiču podataka u vezi sa povredama na radu i profesionalnih bolesti, a koji se nisu vodile u automatizovanom obliku, što bi pružilo dodatnu meru zaštite.[431] Takođe, Republički fond je nepotrebno obrađivao podatke koji se tiču pripadnosti osiguranika MUP-u, BIA-i i naziva mesta privremenog rada van prebivališta, što nije bilo opravdano svrhom obrade. Osim toga, upozorenje se odnosilo i na potrebu ustanovljavanja tehničkih mera u pogledu video nadzora filijala koje nisu imali obezbeđene kopije, pa ne pružaju sigurnost od neovlašćenog pristupa podacima.

6.2.1.3. Rešenja Poverenika

Pored brojnih rešenja u pogledu uloženih žalbi, Poverenik je donosio i rešenja kojima je zabranjivao obradu podataka o ličnosti u situacijama koje su predstavljale nezakonito vršenje ovlašćenja. Tako je jednim rešenjem[432] privremeno zabranio obradu podataka o ličnosti rukovaocu Gradskoj opštini Novi

[430] Upozorenje Poverenika br. 164/01-00003/2010/06 od 11.05.2010. god.
[431] Upozorenje Poverenika br. 164-01-00015/2010-07 od 31.03.2011. god.
[432] Rešenje Poverenika br. 07-00-01090/2010-05 od 27.07.2010. god.

Beograd – Upravi gradske opštine u jednom predmetu u kome je nezakonito vršena obrada podataka o ličnosti učesnika u predmetu. Istim rešenjem, naređeno je rukovaocu da nakon okončanja krivičnog postupka obriše podatke koji su prikupljeni bez pravnog osnova u istom predmetu, a što će se izvršiti uništavanjem Zahteva za upis u birački spisak i svih drugih nosača na kojima se podaci nalaze (fotokopije, fajlovi na USB stiku, računarima, elektronskim bazama podataka itd.).

Zanimljivo je pomenuti da u okviru svojih ovlašćenja Poverenik može da poništi i rešenje sudova. Tako je 2010. godine Poverenik rešenjem poništio rešenje Višeg suda u Vranju i istim naložio sudu da bez odlaganja, a najkasnije u roku od tri dana od prijema rešenja stavi na uvid Naredbu istražnog sudije Okružnog suda u Vranju.[433] Naime, rešenjem Višeg suda u Vranju odbijen je zahtev za ostvarivanje prava u vezi sa obradom podataka o ličnosti kojim je traženo da se ostvari uvid u Naredbu istražnog sudije Okružnog suda u Vranju. Poverenik je pronašao da je rukovalac, odnosno sud, pogrešno postupio kada je odbio zahtev za ostvarivanje prava na uvid, budući da svako ima pravo uvida u dokumenta u kojima se nalaze njegovi podaci. Stoga, izdavanje kopije rešenja ne sprečava pravo uvida u takav dokument. Ovo rešenje Poverenika značajno je za buduće slične slučajeve.

Svojim rešenjima Poverenik je rešavao i o mogućnosti iznošenja podataka o ličnosti iz zemlje. Jednim od rešenja dozvolio je rukovaocu podataka Lexmark International da iznese konkretno određene podatke u Sjedinjene Američke Države, za vreme trajanja Ugovora o obradi i prenosu podataka koji je zaključen sa kompanijom iz SAD.[434] Takođe, ovim rešenjem je naloženo rukovaocu da pre iznošenja podataka opredeli način postupanja sa podacima nakon prestanka ugovorne obrade, odnosno njihovo brisanje ili vraćanje rukovaocu, uz sprovođenje odgovarajućih mera zaštite podataka. Uz to, zabranjen je dalji prenos ili činjenje dostupnim podataka iz dispozitiva ovog rešenja, van kompanije Lexmark International.

Za razliku od dozvole za iznošenje, obustavljanje postupka po zahtevu za iznošenje podataka iz Republike Srbije uređuje se zaključkom. Tako je zaključkom obustavljen postupak po zahtevu Predstavništva 3M AG iz Beograda za davanje dozvole za iznošenje podataka o ličnosti iz Republike Srbije, budući da je podnosilac odustao od podnetog zahteva.[435]

[433] Rešenje Poverenika br. 07-00-02308/2010-06 od 21.12.2010. god.
[434] Rešenje Poverenika br. 011-00-00102/2009-05 od 08.03.2011. god.
[435] Zaključak Poverenika br. 011-00-00156/2009-05 od 16.09.2010. god.

6.2.1.4. Krivične prijave Poverenika

Praksu Poverenika odlikuje i podnošenje krivičnih prijava zbog nepoštovanja propisa u oblasti podataka o ličnosti. Tako je Poverenik podneo krivičnu prijavu protiv nepoznatih izvršilaca zbog toga što su neovlašćeno pribavili i upotrebili u svrhu za koju nisu namenjeni, podatke o ličnosti građana sa teritoriji opštine Bor, koji su prikupljani, obrađivani i korišćeni na osnovu Zakona o lokalnim izborima i Zakona o izboru narodnih poslanika u postupku sprovođenja lokalnih izbora za odbornike.[436] Nepoznati počinioci su iz spiska građana upotrebili imena, prezimena i adrese većeg broja građana za adresiranje neutvrđenog broja pisama istovetnog propagandnog sadržaja, sa priloženim nalogom za uplatu iznosa od „skromnih 1860.00 dinara" u kojima se mole sigurni glasači da uplate novčani iznos. Napomenuto je da su sva pisma predata preko pošte. Poverenik je predložio tužilaštvu da rasvetli navedeno krivično delo i utvrdi identitet nepoznatih izvršilaca i da postupi u skladu sa Zakonikom o krivičnom postupku.

Poverenik je protiv nepoznatih izvršilaca podneo krivičnu prijavu i zbog postojanja sumnje da su kao saizvršioci izvršili krivično delo neovlašćenog prikupljanja ličnih podataka i falsifikovanja isprave.[437] Prema krivičnoj prijavi, nepoznati izvršioci su 13.04.2010. godine u Beogradu neovlašćeno pribavili, saopštili drugom i upotrebili u svrhu za koju nisu namenjeni podatke oštećenog (ime i prezime, ime njegovog oca, oznaku pola, rođenja, JMBG, broj lične karte, mesto prebivališta i adresu) i iskoristili ih tako što su ih uneli u Obrazac 1 – Zahtev za upis u poseban birački spisak bošnjačke nacionalne manjine, kao i falsifikovali potpis na istom obrascu, nakon čega su lažnu ispravu predali aktivisti Nacionalnog saveta bošnjačke nacionalne manjine, koja je predata Odeljenju za opštu upravu Gradske opštine Novi Beograd. Na taj način su, prema mišljenju Poverenika, izvršili krivično delo neovlašćenog prikupljanja ličnih podataka.

6.2.2. Sudska praksa u oblasti zaštite podataka o ličnosti u Republici Srbiji

Do trenutka pisanja ovog rada, autori nisu uspeli da dođu do bilo koje sudske odluke po novom Zakonu o zaštiti podataka o ličnosti. Zbog toga, sva sudska praksa koja se iznosi u ovom radu zasniva se na odredbama prethodnog Zakona o zaštiti podataka o ličnosti.

[436] Krivična prijava Poverenika br. 164-00-00010/2010-07 od 30.06.2010. god.
[437] Krivična prijava Poverenika br. 07-00-01090/2010-05 od 12-07-2010. god.

Ukoliko se osvrnemo na praksu Upravnog suda, konstatujemo da se najveći broj tužbi u vezi sa zaštitom podataka o ličnosti koje su podnete ovom sudu, završio odbijajućim presudama[438] ili rešenjima o odbacivanju.[439] Smatramo da je osnovni razlog ovakvih negativnih ishoda slabije razvijena svest o načinima i metodama zaštite podataka o ličnosti, kao i nedovoljno precizna terminologija koja se koristila u prethodnom zakonodavstvu. Čini se da je usvajanjem novog Zakona o zaštiti podataka o ličnosti rešen veći broj spornih pravila i odredaba, a takođe je i povećan obim zaštite koju zakon pruža, pa je realno očekivati u budućnosti više presuda u korist tužilaca. Ipak, do takve prakse moraće da prođe određeno vreme, koje je neophodno da građani shvate značaj zaštite, da pokrenu mehanizme zaštite pred upravnim organima, barem što se tiče upravnih sporova, i nakon toga da zaštitu zahtevaju pred Upravnim sudom.

Pored Upravnog suda u materiji zaštite podataka delovali su i drugi sudovi opšte i posebne nadležnosti, samo u značajno manjem obimu. Tako, u praksi nalazimo Presudu Višeg suda u Beogradu kojom se prihvata sporazum o priznanju krivičnog dela.[440] Okrivljeni je priznao da je u periodu od dve godine, u svojstvu službenog lica – šefa tehničke službe Fakulteta za specijalnu edukaciju i rehabilitaciju, u više navrata neovlašćeno saopštio australijskoj agenciji iz Melburna, za potrebe vođenja postupak pred australijskim sudom, podatke o ličnosti koji se obrađuju i koriste na osnovu Zakona o visokom obrazovanju, čime je izvršio krivično delo neovlašćeno prikupljanje ličnih podataka iz čl. 146 st. 3 Krivičnog zakonika. Zbog toga, okrivljenom je izrečena uslovna osuda, tako što mu je utvrđena kazna zatvora u trajanju od 6 (šest) meseci i istovremeno određeno da se utvrđena kazna zatvora neće izvršiti ukoliko okrivljeni u roku od jedne godine od dana pravosnažnosti ne učini novo krivično delo.

Prekršajni sud u Beogradu je izrekao osuđujuće presude trojici okrivljenih zato što su 2012. godine – i to GSP kao rukovalac podataka, jedno lice kao generalni direktor GSP-a i treće neposredno odgovorno lice u organizacionoj jedinici GSP – vršili obradu podataka suprotno odredbama čl. 12 Zakona o zaštiti podataka o ličnosti, tako što su dozvolili i omogućili direktoru jednog pravnog lica da dobije snimak iz tramvaja na kome se vidi petoro mladih ljudi koji su se prevozili tramvajem, od kojih je jedan iščupao validator, pri čemu je na snimku vidljiv lik mladića u roze košulji koji je sedeo iza navedenog društva, iako nije

[438] Vid. Presuda Upravnog suda Odeljenje u Novom Sadu br. III-8 U.17892/17, od 10.01.2018. god., Presuda Upravnog suda u Beogradu 17 U 12679/17 od 15.12.2017. god.

[439] Npr. Rešenje Upravnog suda u Beogradu br. 10 U 4205/19 od 22.03.2019. god. ili Rešenje Upravnog suda u Beogradu br. 14 U 13873/18 od 09.11.2018. god.

[440] Presuda Višeg suda u Beogradu br. K. Po3-10/13-SPK – 15/15 od 25.05.2015. god.

postojao pravni osnov da GSP ustupi sporni snimak drugom licu, niti su lica koja se vide na snimku dala svoju saglasnost za obradu njihovih podataka.[441] Zbog ovog prekršaja, GSP je osuđen na novčanu kaznu od 50.000.00 dinara, generalni direktor na novčanu kaznu od 5.000,00 dinara, a izvršni direktor, neposredno odgovorni na novčanu kaznu u istom iznosu kao i generalni direktor.

Takođe, u drugom posebnom postupku, osuđeno je pravno lice koje je dobilo podatke od GSP-a (u iznosu od 100.000,00 dinara) kao i odgovorno lice na kaznu u iznosu od 10.000,00 dinara, budući da su nezakonito prikupljali podatke od drugog lica, a ne od lica na koje se ti podaci odnose, niti od organa uprave koji su ovlašćeni za njihovo prikupljanje, niti je takav način prikupljanja propisan zakonom, čime je učinjen prekršaj iz čl. 57, st. 1, tač. 3 Zakona o prekršajima.[442]

Iz novije prakse izdvajamo osuđujuću presudu Prekršajnog suda u Šapcu, odeljenje u Bogatiću, kojom je odgovorna osoba osuđena na novčanu kaznu od 5.000,00 dinara.[443] Okrivljena je odgovorna zato što je kao sanitarni inspektor, pri podnošenju zahteva za pokretanje prekršajnog postupka bez zakonskog ovlašćenja, a suprotno uslovima za obradu od strane organa vlasti, dostavila dva dokumenta, izdata od strane Službe za zdravstvenu zaštitu dece i omladine Doma zdravlja koji su sadržali podatke o ličnosti ukupno 29-oro maloletne dece i njihovih 16 roditelja, koji tu decu nisu vakcinisali, čime je izvršena nedozvoljena obrada u smislu Zakona o zaštiti podataka o ličnosti (povređen je čl. 8, st. 1, kao i čl. 13 ovog zakona).

U nekoliko navrata i Ustavni sud se izjašnjavao o saglasnosti pojedinih odredaba posebnih zakona sa Ustavom. Ustavni sud je pronašao da odredbe Zakona o elektronskim komunikacijama nisu u saglasnosti sa Ustavom.[444] Naime, sud je utvrdio da odredbe člana 128, st. 1 Zakona o elektronskim komunikacijama, nisu u saglasnosti sa odredbom čl. 41, st. 2 Ustava, budući da dozvoljavaju primenu posebnih mera kojima se odstupa od tajnosti pisama i drugih sredstava komunikacije, ne samo sudskom odlukom, već i bez naloga suda – kada je takva mogućnost propisana zakonom, odnosno na zahtev nadležnog državnog organa. Na taj način povređena su zajamčena prava tajnosti pisama i drugih sredstava javnog obaveštavanja.

Pored Zakona o elektronskim komunikacijama, Ustavni sud se izjašnjavao i o ustavnosti pojedinih odredbi Zakona o Vojnobezbednosnoj

[441] Presuda Prekršajnog suda u Beogradu 89 pr. Br. 120316/12 od 29.01.2014. god.
[442] Presuda Prekršajnog suda u Beogradu 56. Pr.br. 118324/12 od 11.12.2013. god.
[443] Presuda Prekršajnog suda u Šapcu, odeljenje u Bogatiću, br. I. 13 pr. 9690/17 od 10.05.2018. god.
[444] Odluka Ustavnog suda br. Iuz – 1245/2010 od 08.07.2013. god.

agenciji i Vojnoobaveštanoj agenciji.[445] Ova odluka doneta je na osnovu predloga Zaštitnika građana i Poverenika, koji su tvrdili da su odredbe pomenutog zakona koje se odnose na nalog direktora VBA ili lica koje on ovlasti, da se putem tajnog elektronskog nadzora prikupljaju podaci o telekomunikacionom saobraćaju i lokaciji korisnika, bez uvida u njihov sadržaj nesaglasne sa Ustavom. Takođe, predlagači su ukazali na neustavnost odredbi po kojima je VBA imala pravo da od telekomunikacionih operatora traži i dobije informacije o korisnicima njihovih usluga, samostalno i bez ikakve uloge suda. Ustavni sud je pronašao da su pomenute odredbe neustavne, odnosno da nisu u saglasnosti sa odredbom čl. 41, st. 2 Ustava, budući da se time odstupa od prava na nepovredivost pisama i drugih sredstava komunikacije, koje se može ograničiti samo na osnovu odluke suda. Iako je utvrdio neustavnost ovih odredbi, Ustavni sud je odbacio zahtev za obustavu izvršenja pojedinačnih akata donetih, odnosno radnji preduzetih na osnovu osporenih neustavnih odredbi.

6.2.3. Zaključak

Imajući u vidu da je „novi" Zakon o zaštiti podataka o ličnosti u Srbiji na snazi oko godinu dana, teško je govoriti o ustanovljenoj upravnoj i sudskoj praksi koja se zasniva na njegovim odredbama. Ipak, duh i intencija zakonskih normi u oblasti zaštite podataka ostala je istovetna i nakon donošenja novog zakona pa je bilo važno predstaviti neke od već donetih sudskih odluka, kao i odluka Poverenika. Ove odluke, donete na osnovu prethodnog zakona, sigurno će predstavljati putokaz za dalji razvoj prakse u oblasti zaštite podataka o ličnosti.

Imajući u vidu značaj prakse za funkcionisanje celog sistema zaštite podataka o ličnosti, očekujemo da će tek u narednom periodu odluke Poverenika i sudova obezbediti pojedincima adekvatnu zaštitu od zloupotrebe podataka o ličnosti.

[445] Odluka Ustavnog suda br. Iuz-1218/2010 od 24.05.2012. god.

7. ZAKLJUČAK

Kada razmišljamo o budućnosti, nema nikakve sumnje da razmišljamo o razvoju tehnologije i njenoj ulozi u svakodnevnom životu. Tehnološke inovacije agresivno prodiru sve više u naš svakodnevni život, često presudno utičući na naš posao, navike i privatni život. Već danas, a svakako i u budućnosti, ljudi će se sve više oslanjati na pametne telefone, pametne televizore, pametne računare, pametne automobile, pametne zgrade, pa čak i pametne frižidere. Svaki od ovih predmeta namenjenih da unaprede i olakšaju život, bez kojih teško da možemo da zamislimo život u budućnosti, prikuplja ogroman broj podataka o ličnosti pa prema tome možemo da zaključimo bez ikakve dileme da budućnost pripada podacima.

U budućnosti svi podaci će sadržati podatke o ličnosti, a i sam pojam podataka o ličnosti će biti sigurno drastično proširen. Pošto je jedna od uloga prava da zaštiti osnovne ljudske vrednosti, možemo očekivati da će se u budućnosti pravo zaštite podataka o ličnosti primenjivati na sve podatke, odnosno tražiće se mehanizmi za što efikasniju primenu prava u ovoj oblasti. Sofisticiranije i složenije tehnologije proizvodiće savršeno precizne informacije o svakom pojedincu. Analiza informacija i automatsko odlučivanje na bazi informacija stalno će se podizati na sve viši nivo preciznosti i upotrebljivosti, a svaka od tako obrađenih informacija u pametnom okruženju odnosiće se na konkretnu osobu. Ne samo da će tehnologija koja nas okružuje prikupljati informacije o nama, već je izvesno da će pametna tehnologija biti ugrađivana i u ljudsko telo, s ciljem što efikasnijeg prikupljanja podataka. Eksperimentisanje sa ovakvom tehnologijom pruža rezultate i sve je veći broj ljudi koji su spremni, iz različitih razloga, da u svoje telo ugrade pametnu tehnologiju koja prikuplja podatke o ličnosti.

Upravljanje podacima u hiperpovezanom svetu budućnosti – zasnovanom na veštačkoj inteligenciji, biotehnologiji i algoritmima za obradu velike količine podataka – predstavljaće osnovu industrije i upravljanja društvom, a time i osnovu upravljanja pojedincem. U takvoj budućnosti, koja je potpuno izvesna, uloga prava zaštite podataka o ličnosti biće sve veća. Ovo pravo i njegova efikasna primena predstavljaće nezamenljivo sredstvo za odbranu od zloupotreba podataka. Kako je danas broj zloupotreba podataka o ličnosti veliki, a očekujemo da će u budućnosti zbog povećanja podataka taj broj biti još veći, nužno je

izgraditi što kvalitetniji sistem zaštite podataka o ličnosti. Taj sistem primenjivaće se na svakog ko obrađuje bilo koju vrstu podataka o ličnosti i na svakoga čiji se podaci obrađuju.

Naše se okruženje ubrzano približava nečemu što se naziva *"onlife"* svet. To je svet u kome dnevnom egzistencijom upravlja pametna tehnologija, a odluke se donose u hiperpovezanom okruženju na bazi obrade podataka o ličnosti pametnom tehnologijom. Sigurno je da će u takvom okruženju biti ogroman izazov stvoriti pravne mehanizme koji će moći pojedinca efikasno da zaštite od zloupotrebe podataka o ličnosti od drugih pojedinaca, institucija i samog sistema.

Sistem zaštite podataka o ličnosti mora da obuhvati, s jedne strane, tehničke aspekte zaštite informacionih sistema i njihovu bezbednost, a s druge strane mora da obuhvati usaglašenu normativu regulativu i praksu primene zaštite podataka o ličnosti na međunarodnom i nacionalnom planu. Veliki korak unapred ka stvaranju sistema zaštite podataka o ličnosti predstavlja usvajanje Opšte uredbe EU. Ovaj propis ne samo da je usaglasio normativu i praksu na nivou EU, nego je od početka primene 2018. godine izvršio veliki uticaj na razvoj sistema zaštite podataka u velikom broju zemalja širom sveta. Možemo zaključiti da se radi o propisu sa globalnim uticajem na razvoj sistema zaštite podataka u čitavom svetu, pa shodno tome i u Srbiji. Posebno značajna je delotvornost primene Opšte uredbe EU i veliki broj okončanih postupaka za zaštitu podataka o ličnosti u različitim zemljama sa izrečenim sankcijama u vrednosti od više stotina miliona evra. U okviru efikasne primene ovog propisa posebno mesto imaju nezavisni organi za zaštitu podataka o ličnosti i novoustanovljeno zanimanje lica za zaštitu podataka. Njihova uloga je da primenjuju načela zaštite podataka o ličnosti, podižu svest o društvenoj odgovornosti u ovoj oblasti, pokreću postupke i ostvaruju prava i obaveze u cilju zaštite pojedinaca i institucija u vezi sa zaštitom podataka o ličnosti. Pod uticajem Opšte uredbe EU nastao je i novi Zakon o zaštiti podataka o ličnosti u Srbiji. Imajući u vidu da je ovaj propis tek na samom početku svog razvoja, ostaje da se vidi kako će evropska praksa uticati na domaću.

Razvoj pravnih normi u oblasti zaštite podataka, s jedne strane, delotvorna primena prava, s druge strane, i, s treće strane, podizanje nivoa znanja pravnika i svih pojedinaca o nužnosti unapređenje sistema zaštite podataka o ličnosti preduslov su, ne samo zaštiti fundamentalnih ljudskih prava, nego i dostizanju višeg nivoa društvene odgovornosti u ovoj oblasti.

8. LITERATURA

8.1. Knjige i članci

Abramson Jeffrey, „Searching for Reputation: Reconciling Free Speech and the „Right to be Forgotten“, *North Carolina Journal of Law & Technology*, vol. 17, issue 1, North Carolina 2015.

Adamović Anđelija, „Postupak u parnicama za objavljivanje ispravke neistinite, nepotpune ili netačno prenete informacije“, *Zbornik radova Pravnog fakulteta u Nišu LXI* (ur. Milan Petrović), Pravni fakultet u Nišu, Niš 2012.

Adamović Jelena, Jovanović Milica, Kalezić Petar, Krivokapić Nevena, Perkov Bojan, Petrovski Andrej, *Vodič za medije: Zaštita ličnih podataka i novinarski izuzetak*, Share fondacija, Beograd 2018.

Ambrose Meg Leta, Ausloos Jef, „The Right to Be Forgotten Across the Pond“, *Journal of Information Policy,* vol. 3, Pennsylvania State University Press, Penssylvania 2013.

Andonović Stefan, *Zaštita podataka u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti*, doktorska disertacija, Pravni fakultet Univerziteta u Beogradu, Beograd 2019.

Andonović Stefan, „Obaveza imenovanja lica za zaštitu podataka u organima uprave“, časopis *Savremena uprava*, Beograd 2019.

Andonović Stefan, „Pravna priroda Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti“, Arhiv za pravne i društvene nauke, Savez udruženja pravnika Srbije i Republike Srpske, Institut za političke studije, Beograd 2019.

Andonović Stefan, „Zaštita podataka o ličnosti koje obrađuju crkve i verske zajednice u Republici Srbiji“, *Zbornik radova sa međunarodnog naučnog skupa „Državno-crkveno pravo kroz vekove“*, Institut za uporedno pravo, Pravoslavna Mitropolija Crnogorsko-primorska, urednici: Vladimir Čolović, Velibor Džomić, Vladimir Đurić, Miloš Stanić, Beograd-Budva 2019.

Antić Oliver, „Moral (etika) u građanskom pravu“, Zbornik radova *Harmonizacija građanskog prava u regionu* (ur. Dijana Marković-Bajalović), Pravni fakultet Univerziteta u Istočnom Sarajevu, Istočno Sarajevo 2013.

Aplin Tanya, *Copyright Law in the Digital Society: The Chalenges of Multimedia*, 2005.

Bainbridge David, *Introduction to Computer Law*, Longman, 2000.

Banović Božidar, *Elektronski dokazi*, Revija za kriminologiju i krivično pravo, br. 3/2006.

Boranijašević Vladimir, „Postupak u parnicama za objavljivanje ispravke", *Zbornik radova „Vladavina prava i pravna država u regionu"* (ur. Goran Marković), Pravni fakultet u Istočnom Sarajevu, Istočno Sarajevo 2014.

Brandeis Warren, „The Right to Privacy", Harvard Law Review, vol. IV, no. 5, 1890.

Brković Radoje, Jovanović Zoran, Totić Mirza, "Pravo na privatnost i zaštitu ličnih podataka zaposlenog kao pacijenta u pravu Republike Srbije", *Anali Pravnog fakulteta Univerziteta u Zenici*, vol 13, br. 24, Zenica 2019.

Burkert Herbert, „Privacy - Data Protection a German/European Perspective", *in Governance of Global Networks in the Light of Differing Local Values, (eds. E. Christoph, K. Keeneth),* Nomos Baden-Baden 2000.

Culik Nicolai, Döpke Christian, „About Forgetting and Being Forgotten", u *Big Data in Context- Legal, Social and Technological Insights,* (eds. Thomas Hoeren, Barbara Kolany-Raiser), Springer, online 2018.

Čolaković Maja, Bubalo Lana, „Pravo na zaborav kao instrument zaštite prava ličnosti u Evropskoj Uniji", *Zbornik radova Pravnog fakulteta u Tuzli*, br. 2/2017 (ur. Vedad Gurda), Pravni fakultet u Tuzli, Tuzla 2017.

Davinić Marko, *Nezavisna kontrolna tela u Republici Srbiji*, Dosije studio, Beograd 2018.

Diligenski Andrej, Prlja Dragan, Cerović Dražen, *Pravo zaštite podataka- GDPR*, Institut za uporedno pravo, Beograd 2018.

Diligenski Andrej, "Obaveza navođenja pravog imena na Fejsbuku", portal Zaštita podataka o ličnosti, http://partners-serbia.org/privatnost/blog/obaveza-navodenja-pravog-imena-na-fejsbuku/.

Dimitrijević Predrag, „Pravna regulacija elektronske komunikacije i pravo na privatnost, *Zbornik radova Pravnog fakulteta Univerziteta u Istočnom Sarajevu* (ur. Goran Marković), Pravni fakultet u Istočnom Sarajevu, Istočno Sarajevo 2011.

Dimitrijević Predrag, *Pravo informacione tehnologije*, SVEN, Niš, 2010.

De Baets Antoon, „A historian's view on the right to be forgotten", *International Review of Law, Computers & Technology*, Vol. 30, Nos. 1-2, Routledge-Taylor & Francis group, online 2016.

De Terwangne Cécile, „Internet Privacy and the Right to Be Forgotten/Right to Oblivion", Monograph "VII International Conference on Internet, Law & Politics- Net Neutrality and other challenges for the future of the Internet", *Revista de internet, derecho y politica,* Universitat Oberta de Catalunya, Barcelona 2012.

De Hert Paul*, et al*, „The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer law & security review* (ed. Steve Saxby), Amsterdam – Boston - London 2018.

Debeljački Milorad, "Zakon o zaštiti podataka o ličnosti: radna grupa za izradu nacrta", PravoIkt, online 2016., https://pravoikt.org/zakon-o-zastiti-podataka-o-licnosti-radna-grupa-za-izradu-nacrta/.

Drakulić Mirjana i Drakulić Ratimir, *Pravna regulacija e-poslovanja*, Internet adresa: http://www.e-trgovina.co.yu/pravo/regulacija1.html, 17.08.2009.

Drozdova Ekatarina A, *Civil Liberties and Security in Cyberspace*, u: Abraham D.Sofaer, Seymour E.Goodman (ed.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, 2001.

Dworkin Gerald, *Judical Control of Copyright on Public Policy Grounds,* in: Inellectual Property and Information Law, Kluwer, 1998.

Evropska komisija, "Šta se podrazumeva pod pravom zaštite podataka "po dizajnu" i "po pravilu" – European Commission, What does data protection „by design" and „by default" mean?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en.

Efroni Zohar, *Access – Right : The Future Of Copyright Law*, Oxford University Press, 2011.

Fejsbuk, *Opšti uslovi poslovanja Fejsbuka*, http:// www. facebook. com/legal/terms, 2013.

Fink Simon, *Datenschutz zwischen Staat und Markt (Die „Safe Harbor"-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie)*, UNIVERSITÄT KONSTANZ, 2002, Magisterarbeit.

Forgó Nikolaus, Hänold Stefanie, Schütze Benjamin, „The Principle of Purpose Limitation and Big Data", u: *New techonolgy, Big Data and the Law* (ed.

Marcelo Corrales, Mark Fenwick, Nikolaus Forgó), Springer, Singapore 2017.

Gajin Saša, „Zaštita podataka o ličnosti, perspektive harmonizacije domaćeg prava sa pravom Evropske Unije“, u: *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005.

GDPR Informer, *Službene smjernice o prenosivosti podataka*, online 2018, *https://gdprinformer.com/hr/gdpr-clanci/sluzbene-smjernice-o-prenosivosti-podataka*, 12. 09. 2018.

Hećimović Željko, *Metapodaci*, Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije, Katedra za geodeziju i geoinformatiku, Split 2016.

Hoeren Thomas, *Facebook und Co: Es ist nicht alles Gold, was glänzt, Risiken für Unternehmen und Privatnutzer*, Wissen+Karriere časopis, broj Ausgabe 06/2011 September/Oktober.

Ilić Petković Aleksandra, Ilić Mile, „Odgovornost državnih službenika i zaštita njihovih prava“, *Godišnjak Pedagoškog fakulteta u Vranju*, 1/2017, (ur. Sunčica Denić), Pedagoški fakultet u Vranju, Vranje 2017.

Jakšić Aleksandar, *Građansko procesno pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013.

Jašarević Senad, Zaštita ličnih podataka zaposlenih u srpskom i evropskom pravu, *Zbornik radova Pravnog fakultet u Novom Sadu*, br. 2/2009, Novi Sad 2009.

Jehoram Tobias Cohen, *Copyright in Non-Orginal Wrutings Past – Present – Future?*, in: Inellectual Property and Information Law, Kluwer, 1998.

Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf.

Jovičić Jelena, „Ustavno regulisanje prava na javno informisanje“, *Zbornik radova pravnog fakulteta u Nišu* (ur. Predrag Dimitrijević), Pravni fakultet Univerziteta u Nišu, Niš 2012.

Kabel Jan, *Inellectual Property and Information Law,* Kluwer, 1998.

Krivokapić Danilo, Adamović Jelena, Tasić Dunja, Petrovski Andrej, Kalezić Petar, Krivokapić Đorđe, *Vodič kroz Zakon o zaštiti podataka o ličnosti i GDPR – tumačenje novog pravnog okvira*, SHARE fondacija, Beograd 2019.

Krivokapić Danilo, Krivokapić Đorđe, Jovanović Milica, Perkov Bojan, Petrovski Andrej, *Moji podaci, moja prava*, SHARE fondacija, Beograd 2018.

Kanzlei Bahr, *Kein Recht auf Einschränkung der Datenverarbeitung nach Art. 18*, DSGVO, online 2018, *https://www.datenschutz.eu/urteile/Kein-Recht-*

auf-Einschraenkung-der-Datenverarbeitung-nach-Art-18-DSGVO-Verwaltungsgericht-Stade-20181009/#.

Kovačević-Lepojević Marina, Žunić-Pavlović Vesna, „Rizici socijalnog umrežavanja dece na internetu“, *Zbornik Instituta za kriminološka i sociološka istraživanja* (ur. Leposava Kon), br. 1-2, Institut za sociološka i kriminološka istraživanja, Beograd 2011.

Koumantas Georges, *Reflections on the Concept of Intellectual Property*, in: Inellectual Property and Information Law, Kluwer, 1998.

Krebs Brian, *Year of Computing Dangerously*, Washington Post, 22.12.2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html.

Lambert Paul, *Understanding the New European Protection Rules*, Taylor & Francis group, 2018.

Lilić Stevan, Prlja Dragan, *Pravna informatika veština*, Pravni fakultet Univerziteta u Beogradu, Beograd 2010.

Lilić Stevan, „Pravo, informatička tehnologija i zaštita podataka“, *Anali Pravnog fakulteta u Beogradu*, br. 2-3/1989, Beograd 1989.

Lilić Stevan, „Zaštita ličnih podataka u pravu Srbije i evropski standardi, u Harmonizacija zakonodavstva Republike Srbije sa pravom Evropske unije (ur. Duško Dimitrijević, Brano Miljuš), Institut za međunarodnu politiku i privredu, Beograd 2010.

Lilić Stevan, „Pravni aspekti zaštite podataka u automatizovanim službenim evidencijama“, *Naša zakonitost*, br. 5, Zagreb 1989.

Litman Jessica, *Digital copyright: protecting intellectual property on the Internet*, Prometheus Books, 2001.

Maisl Herbert, *Etat de la Legislation Française et Tendences de la Jurisprudence Relatives à la Protection des donnees Personnalles*, Revue Internationale de Droit Comparé, No. 3, 1987.

Marković Ratko, *Ustavno pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2018.

Marković Ratko, *Ustavno pravo i političke institucije*, Pravni fakultet Univerziteta u Beogradu, Beograd 2008.

Mezrih Ben, *Slučajni milijarderi: nastajanje Fejsbuka*, Beograd: Evro-Giunti, 2010.

Milenković Dejan, *Pristup informacijama, zaštita podataka o ličnosti i tajnost informacija – Aktuelna pitanja zakonodavstva u Srbiji*, Komitet pravnika za ljudska prava, Beograd 2009.

Milovanović Dobrosav, "Odnos opšt(ij)eg i posebn(ij)ih upravno procesnih zakona", *Polis – časopis za javnu politiku*, Stalna konferencija gradova i opština, Savez gradova i opština Srbije i Centar za javnu i lokalnu upravnu – Palgo centar, Beograd 2016.

Mitrović Dragan, *Uvod u pravo*, Pravni fakultet Univerziteta u Beogradu, Beograd 2010.

Mišič Klemenč, Lubarda Maja, *Zaštita podataka – priručnik za rukovaoce*, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti Republike Srbije, Beograd 2012.

National Research Council (US), *The digital dilemma: intellectual property in the information age*, National Academic, 2000.

OEBS, *Zaštita podataka u sektoru bezbednosti – Vodič kroz zakonsku regulativu*, (ur. Saša Gajin), Centar za unapređenje pravnih studija, Beograd 2019.

Overbeck Wayne, Genelle Belmas, *Major principles of media law*, Stamford: Cengage Learning, 2011.

Pavlović Dušan, Uredba Evropske unije o zaštiti podataka o ličnosti, http://pravoikt.org/uredba-evropske-unije-o-zastiti-podataka-o-licnosti/.

Paunović Milan, Krivokapić Boris, Krstić Ivana, *Međunarodna ljudska prava*, Pravni fakultet Univerziteta u Beogradu, Beograd 2013.

PC Press, *Odobreno korišćenje špijunskih sofrvera*, https://pcpress.rs/izrael-odobrio-koriscenje-spijunskih-softvera/.

Pejić Jelena, *Šta je „Policijska direktiva Evropske unije"? – Kako organi sprovođenja zakona (treba da) štite lične podatke*, Beogradski centar za bezbednosnu politiku, 2019.

Peran Branko, Goreta Mirko, Vukošić Kristina, „Pojam i vrste tajni", *Zbornik radova Veleučilišta u Šibeniku,* br. 3-4/2015, Šibenik 2015.

Protrka Nikola, "Normativna uređenost zaštite osnovnih podataka u Republici Hrvatskoj", *Policijska sigurnost*, god. 22, br. 4, Zagreb 2002.

Prlja Dragan, Andonović Stefan, „Naknada štete kod povrede ličnih podataka", u *Odgovornost za štetu, naknada štete i osiguranje* (ur. V. Čolović, Z. Petrović), Valjevo-Beograd 2019.

Prlja Dragan, Diligenski Andrej, "Pravni aspekti neutralnosti internet mreže", *Strani pravni život*, br. 3, 2011.

Prlja Dragan, Ivanović Zvonimir, Reljanović Mario, *Krivična dela visokotehnološkog kriminala*, Institut za uporedno pravo, Beograd, 2011.

Prlja Dragan, Reljanović Mario, *Pravna informatika*, Beograd, Službeni glasnik, 2010.

Prlja Dragan, Reljanović Mario, „Visokotehnološki kriminal – uporedna iskustva“, *Strani pravni život* 3/2009.

Prlja Sanja, “Pravo na zaštitu ličnih podataka u EU”, *Strani pravni život* 1/2018, Beograd 2018.

Purtova Nadezhda, „Illusion of Personal Data as No Ones' Property“, *Law, Innovation and Techonology*, vol. 7, is. 1, Taylor and Francis 2015.

Radna grupa člana 29, Smernice o automatizovanom donošenju pojedinačnih odluka i izradi profila za potrebe Uredbe 2016/679 – Guidelines on automated decision-making and profile development for the purposes of the Regulation 17/HR, WP251REV.01, 2018.

Radna grupa člana 29, Smernice o pravu na prenosivost – Guidlines on the right to data portability, 16/EN WP 242 rev.01, online 2017.

Radna grupa člana 29, Smernice o principu transparentnosti po Uredbi 2016/679 - Guidelines on transparency under Regulation 2016/679, no. 17 WP260.

Radivojević Zoran, „Sud pravde Evropske Unije posle Lisabonskog ugovora“, *Zbornik radova Pravnog fakulteta u Nišu br. 73*, Niš 2016.

Radojković Miroljub, „Za slobodan pristup informacijama“, *Prizma,* br. 4/2002, Centar za liberalno-demokratske studije, Beograd 2002.

Radošević Ratko, “Upravni spor zbog ćutanja uprave”, *Zbornik radova Pravnog fakulteta u Novom Sadu*, br. 4/2015, Novi Sad 2015.

Reljanović Mario, “Odnos prava na privatnost i pojedinih aspekata visokotehnološkog kriminala”, u: Komlen-Nikolić Lidija et alia, *Suzbijanje visokotehnološkog kriminala*, Beograd, 2010.

Resanović Aleksandar, „Zaštita podataka o ličnosti u Srbiji i Crnoj Gori, odnosno u SR Jugoslaviji“, u *Zaštita podataka o ličnosti i poverljivi podaci – pravni aspekti*, Fond za otvoreno društvo, Beograd 2005.

Savet Evrope, *Konvencija o zaštiti ljudskih prava i osnovnih sloboda*, Rim, 1950, http:// www. echr. coe. int/ NR/rdonlyres/EA13181C-D74A-47F9-A4E5-8A3AF5092938/0/ Convention_BOS.pdf, 4.3.2013.

Schafer Artur, „Privacy – A Philosophical Overview“, Aspects of Privacy Law (ed. Dale Gibson), Butterworth, Toronto 1980.

Stamotoudi Irini, *Copyright Enforcement and the Internet*, Kluwer, 2010.

Stanković Obren, Vodinelić Vladimir, *Uvod u građansko pravo*, Nomos, Beograd 2007.

Stokes Simon, *Digital Copyright: Law and Practice*, 2005.

Share fondacija, *Vodič za zaštitu podataka o ličnosti za vreme pandemije*, Share fondacija, Beograd 2020, https://pandemija.mojipodaci.rs/.

Trkulja Jovica, "Deficiti medijskog zakonodavstva u Srbiji", *Zbornik radova Pravnog fakulteta u Nišu LXI* (ur. Milan Petrović), Niš 2012.

Tubić Bojan, "Lokalni pravni lekovi u praksi Evropskog suda za ljudska prava", *Zbornik radova Pravnog fakulteta u Novom Sadu*, 3/2006, Novi Sad 2006.

UK Information Commissioner's Office, *Principle (c): Data minimization*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/.

UK Information Commissioner's Office, *Principle (d): Accuracy*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.

UK Information Commissioner's Office, *Principle (e): Storage limitation*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/.

UK Information Commissioner's Office, *Right to access*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

Vasiljević Dragan, *Zakonitost uprave i diskreciona ocena*, Kriminalističko-policijska akademija, Beograd 2012.

Vaidhyanathan Siva, *Copyrights and copywrongs: the rise of intellectual property and how it threatens*, NYU Press, 2003.

Vodinelić Vladimir, „Sloboda medija kao granica zaštite podataka (medijska privilegija)", *Zaštita podataka o ličnosti i poverljivi podaci – pravni standardi*, Fond za otvoreno društvo, Beograd 2005.

Vodinelić Vladimir, „Pravo na slobodan pristup informacijama od javnog značaja kao ustavno pravo", u: *Slobodan pristup informacijama – ustavno jemstvo i zakonske garancije*, Fond za otvoreno društvo, Beograd 2004.

Voigt Paul, Dem Bussche Axel, *The EU General Data Protection Regulation (GDPR)- A Practical Guide*, Springer eBook, online 2017.

Von Solms Rossouw, „Information security management: why standards are important", *Information Management & Computer Security*, 7/1, MCB UP Ltd., UK 1999.

Vranješ Aleksandar, *Internet i razvoj ili ograničavanje slobode subjekata globalnog komuniciranja*, doktorska disertacija, Fakultet političkih nauka, Beograd 2017.

Vučković Jelena, "Ljudska prava i mediji", *Zbornik radova Pravnog fakulteta u Nišu*, LV, Niš 2010.

Vuković Mihajlo, *Interpretacija pravnih propisa*, Školska knjiga, Zagreb 1953.

Zirojević Mina, Ivanović Zvonimir, *Zaštita prava intelektualne svojine u sektoru informaciono-komunikacionih tehnologija*, Institut za uporedno pravo, Beograd 2016.

Zuković Slađana, Slijepčević Senka, „Roditeljska kontrola ponašanja dece na internetu i socijalnim mrežama“, u *Nastava i vaspitanje*, br. 64/2, Pedagoško društvo Srbije i Institut za pedagogiju i andragogiju Filozofskog fakulteta Univerziteta u Beograd, Beograd 2015.

Warren Samuel, Brandais Louis, *The Right to be Left Alone*, Harvard Law Review, Harvard 1890.

Wachter Sandra, Mittelstadt Brent, Floridi Luciano, „Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation“, *International Data Privacy Law,* No. 2/2017 (ed. Nora Ni Loideain), Oxford 2017.

Wilkens Andreas, *Facebook: "Likes" stehen unter dem Schutz der US-Verfassung*, heiseOnline, http:// www. heise. de/ newsticker/ meldung/ Facebook – Likes – stehen – unter – dem – Schutz – der – US -Verfassung-1662776.html.

8.2. Propisi i zakonski izvori

Direktiva o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnom kretanju takvih podataka – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995.

Direktiva 2002/58 Evropskog parlamenta i Saveta koja se odnosi na obradu ličnih podataka i zaštitu privatnosti u sektoru elektronskih komunikacija – Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 2002, 31/07/2002.*

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal L 105 , 13/04/2006.*

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal L 337 , 18/12/2009.

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, *Official Journal L 337,* 18/12/2009.

Direktiva 2016/80 Evropskog parlamenta i Veća o zaštiti pojedinaca u vezi sa obradom ličnih podataka od strane nadležnih organa u cilju sprečavanja, istrage, otkrivanja ili gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija i o slobodnom kretanju takvih podataka – Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data „Sl. list EU" L 119/89 od 04.05.2016. god

Konvencija Saveta Evrope o zaštiti lica u odnosu na automatsku obradu podataka (Konvencija 108), Savet Evrope, Strazbur, 1981., https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent ? documentId=0900001680078b37.

Konvencija Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda, Savet Evrope Rim, 1950.

Krivični zakonik Srbije, *Službeni glasnik* RS, br. 85/2005, 94/2016.

Međunarodni pakt o građanskim i političkim pravima, *Službeni list SFRJ*, (Međunarodni ugovori), br. 7/1971.

Opšta uredba o zaštiti podataka EU – Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95&46EC (General Data Protection

Regulation), of 27. April 2016, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.*

Povelja o ljudskim i manjinskim pravima i građanskim slobodama, *Službeni list* SCG, br. 6/2003.

Povelja o osnovnima pravima EU, „Sl. glasnik EU", br. 326/391, https://eur-lex.europa.eu/legal -content / EN / TXT / PDF / ? uri = CELEX : 12012P / TXT&from=EN.

Porodični zakon, „Sl. glasnik RS", br. 18/2005, 72/2011, 6/2015.

Poseban kolektivni ugovor za zaposlene u osnovnim i srednjim školama i domovima učenika, „Sl. glasnik RS", br. 21/2015.

Poseban kolektivni ugovor za javna preduzeća u komunalnoj delatnosti na teritoriji Republike Srbije, „Sl. glasnik RS", br. 27/2015.

Predlog Uredbe Evropskog parlamenta i Saveta o poštovanju privatnog života i zaštiti ličnih podataka u elektronskim komunikacijama – Uredba o privatnosti i elektronskim, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A52017PC0010.

Protokol 223 kojim se menja Konvencija o zaštiti lica u odnosu na automatsku obradu ličnih podataka**.** https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.

Smernice Evropskog odbora za zaštitu podataka 3/2018 o teritorijalnoj primeni Opšte uredbe EU, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Smernice za zaštitu privatnosti i prekogranični protok ličnih podataka, Aneks preporuke Saveta*,* OECD, od 23.09.1990., https://habeasdatacolombia. uniandes.edu.co/wp-content/uploads/ OECD_Privacy_ Guidelines_1980 .pdf.

Strategija zaštite podataka o ličnosti, „Sl. glasnik RS", br. 58/2010.

Univerzalna deklaracija Ujedinjenih nacija o ljudskim pravima, 217 (III), Organizacija Ujedinjenih Nacija, 10. decembar 1948 god., Pariz.

Uredba o obrascu za vođenje evidencije i načinu vođenja evidencije o oblasti podataka o ličnosti, „Sl. glasnik RS", br. 50/2009.

Ustav Republike Srbije, „Sl. glasnik RS", br. 1/90.

Ustav Republike Srbije, „Sl. glasnik RS", br. 98/2006.

Ustav Savezne Republike Jugoslavije, „Sl. list SRJ", br. 1/92

Ustav Socijalističke Federativne Republike Jugoslavije, "Sl. list SFRJ", br. 9/74.

Zakon o bezbednosti saobraćaja na putevima, „Sl. glasnik RS“, br. 41/2009, 53/2010, 101/2011, 55/2014, 96/2015, 9/2016, 24/2018, 41/2018, 87/2018, 23/2019.

Zakona o crkvama i verskim zajednicama, „Sl. glasnik RS“, br. 36/2006.

Zakon o državnim službenicima, „Sl. glasnik RS“, br. 79/2005, 81/2005, 83/2005, 64/2007, 67/2007, 116/2008, 104/2009, 99/2014, 94/2017, 95/2018.

Zakon o evidencijama i obradama podataka u oblasti unutrašnjih poslova, „Sl. glasnik RS“, br. 24/2018.

Zakon o informatici, evidencijama i slobodama Francuske - Loi n° 78-17, relative à l'informatique, aux fichiers et aux libertés, 1978.

Zakon o javnim nabavkama, „Sl. glasnik RS“, br. 124/2012, 14/2015, 68/2015.

Zakon o javnom informisanju i medijima, „Sl. glasnik RS“, br. 83/2014, 58/2015, 12/2016.

Zakon o jedinstvenom matičnom broju građana, „Sl. glasnik RS“, br. 24/2018.

Zakona o opštem upravnom postupku, „Sl. glasnik RS“, br. 18/2016, 95/2018.

Zakon o osnovama društvenog sistema informisanja i o informacionom sistemu Federacije, “Sl. list SFRJ”, br. 68/81.

Zakon o potvrđivanju Konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka, „Sl. list SRJ – Međunarodni ugovori“, br. 1/92.

Zakon o Povereniku za informacije Slovenije, „Uradni list RS“ št. 113/05.

Zakon o policiji, „Sl. glasnik RS“, br. 6/2016, 24/2018, 87/2018.

Zakon o poreskom postupku i poreskoj administraciji, „Sl. glasnik RS“, br. 80/2002 i drugi do 86/2019.

Zakon o pravima pacijenata, „Sl. glasnik RS“, br. 45/2013, 25/2019.

Zakon o privatnom obezbeđenju, „Sl. glasnik RS“, br. 104/2013, 42/2015, 87/2018.

Zakon o prebivalištu i boravištu građana, „Sl. glasnik RS“, br. 87/2011.

Zakon o prekršajima, *Službeni glasnik* RS, br. 65/2013, 13/2016 i 98/2016.

Zakon o primeni Opšte uredbe o zaštiti podataka Hrvatske, Narodne Novine 42/2018, https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka.

Zakon o radu, „Sl. glasnik RS“, br. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017, 113/2017, 95/2018.

Zakon o ratifikaciji Konvencije Ujedinjenih nacija o pravima deteta, „Sl. list SFRJ“ br. 15/90 i „Sl. list SRJ“, br. 4/96 i 2/97.

Zakon o slobodnom pristupu informacijama od javnog značaja, „Sl. glasnik RS“, br. 120/2004.

Zakon o slobodnom pristupu informacijama od javnog značaja, „Sl. glasnik RS“, br. 120/2004, 54/2007, 104/2009, 36/2010.

Zakon o sprečavanju pranja novca i finansiranja terorizma, „Sl. glasnik RS“, br. 113/2017, 91/2019.

Zakon o sportu, „Sl. glasnik RS“, br. 10/2016.

Zakon o zaštiti ličnih podataka BiH, „Sl. glasnik BiH“, be. 49/2006, 76/2011 i 89/2011.

Zakon o zaštiti podataka o ličnosti Crne Gore, „Sl. list CG“, br. 79/08, 70/09, 44/12, 22/17.

Zakon o zaštiti ličnih podataka Makedonije, „Sl. vesnik RSM“, br. 42/2020.

Zakon o zaštiti ličnih podataka Slovenije, „Uradni list RS“ ŠT. 94/07.

Zakon o zaštiti podataka o ličnosti, “Sl. list SRJ”, br. 24/98 i 26/98.

Zakon o zaštiti podataka o ličnosti „Sl. glasnik RS“, br. 97/2008, 104/2009, 68/2012, 107/2012.

Zakon o zaštiti podataka o ličnosti, „Sl. glasnik RS“, br. 87/2018.

Zakon o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva, „Sl. glasnik RS“, br. 123/2014, 106/2015, 105/2017, 25/2019.

Zakon o zdravstvenoj zaštiti, „Sl. glasnik RS“, br. 25/2019.

8.3. Odluke upravnih organa i sudova

Zaključak Poverenika br. 011-00-00156/2009-05 od 16.09.2010. god.

Krivična prijava Poverenika br. 07-00-01090/2010-05 od 12-07-2010. god.

Krivična prijava Poverenika br. 164-00-00010/2010-07 od 30.06.2010. god.

Mišljenje Evropskog supervizora za zaštitu podataka o predlogu Uredbe o e-privatnosti, https://eur-lex.europa.eu/legal-content/HR/TXT/? uri= CELEX%3A52017XX0720%2801%29.

Mišljenje Ministarstva prosvete i sporta, br. 120-01-230/2007-02 od 20.03.2007. god.

Mišljenje Poverenika br. 011-00-00607/2013-05, od 16.10.2013. god.

Mišljenje Poverenika br. 011-00-00272/2014-02 od 14.04.2014. god.

Mišljenje Poverenika br. 073-12-1090/2018-02.

Mišljenje Radne grupa člana 29, br. 3/2010 o principu odgovornosti, br. 00062/10/EN, WP 173, od 13. 07.2010.

Odluka Suda pravde Evropske unije u slučaju *Google v. Costeja* - Court of Justice of the European Union, *Google Spain SL, Google Inc. Vs. Agencia Espanola de Protecction de Datos (Google v. Costeja),* Case C-131/12, 2014.

Odluka Upravnog suda Stade br. Az. 1 B 1918/18, od 09.10.2018. god

Odluka Ustavnog suda Srbije, U. br. 41/10 od 30.05. 2012. god.

Odluka Ustavnog suda Srbije, U. br. 41/04 od 26.11. 2009. god.

Odluka Ustavnog suda br. Iuz – 1245/2010 od 08.07.2013. god.

Odluka Ustavnog suda br. Iuz-1218/2010 od 24.05.2012. god.

Presuda Evropskog suda za ljudska prava Halford, presuda od 25.06.1997. god., RJD, 1997 – III, br. 44.

Presuda Višeg suda u Beogradu br. K. Po3-10/13-SPK – 15/15 od 25.05.2015. god.

Presuda Vrhovnog kasacionog suda, KZZ. 184/19 od 26.02.2019. god.

Presuda Evropskog suda za ljudska prava Rotary od 04.05.2000. god., br. 46. Amman, presuda od 16.02.2000. god., br. 69.

Presuda Prekršajnog suda u Beogradu 89 pr. Br. 120316/12 od 29.01.2014. god.

Presuda Prekršajnog suda u Beogradu 56. Pr.br. 118324/12 od 11.12.2013. god

Presuda Prekršajnog suda u Šapcu, odeljenje u Bogatiću, br. I. 13 pr. 9690/17 od 10.05.2018. god.

Presuda Upravnog suda Odeljenje u Novom Sadu br. III-8 U.17892/17, od 10.01.2018. god.

Presuda Upravnog suda u Beogradu 17 U 12679/17 od 15.12.2017. god.

Presuda Višeg suda u Beogradu br. K. Po3-10/13-SPK – 15/15 od 25.05.2015. god.

Rešenje Višeg suda u Čačku KŽ 119/16 od 09.01.2017 god.

Rešenje Osnovnog suda u Čačku K 398/16 od 16.11.2016. god.

Rešenje Upravnog suda u Beogradu br. 10 U 4205/19 od 22.03.2019. god.

Rešenje Upravnog suda u Beogradu br. 14 U 13873/18 od 09.11.2018. god.

Rešenje Poverenika br. 07-00-01090/2010-05 od 27.07.2010. god.

Rešenje Poverenika br. 07-00-02308/2010-06 od 21.12.2010. god.

Rešenje Poverenika br. 011-00-00102/2009-05 od 08.03.2011. god.

Upozorenje Poverenika br. 164-00-00030/2011-07 od 31.03.2011. god.

Upozorenje Poverenika br. 164/01-00003/2010/06 od 11.05.2010. god.

Upozorenje Poverenika br. 164-01-00015/2010-07 od 31.03.2011. god.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

342.738(497.11)

АНДОНОВИЋ, Стефан, 1991-
Osnovi prava zaštite podataka o ličnosti / Stefan Andonović, Dragan Prlja. - Beograd : Institut za uporedno pravo, 2020 (Beograd : Službeni glasnik). - 226 str. ; 25 cm

Tiraž 200. - Napomene i bibliografske reference uz tekst. - Bibliografija: str. 211-224.

ISBN 978-86-80186-57-3

1. Прља, Драган, 1959- [аутор]
а) Право на заштиту података о личности

COBISS.SR-ID 17830921

’’Naše se okuženje ubrzano približava nečemu što se naziva ’’onlife’’ svet. Svet u kome dnevnom egzistencijom upravlja pametna tehnologija, a odluke se donose u hiperpovezanom okruženju na bazi obrade podataka o ličnosti pametnom tehnologijom’’