

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2017./2018.

Iva Družin

**ZAŠTITA OSOBNIH PODATAKA
U INFORMACIJSKOM DRUŠTVU**

Završni rad

Mentor: dr.sc. Kristina Kocijan, doc.

Zagreb 2018.

Sadržaj

Sadržaj.....	2
Sažetak	3
1. Uvod.....	4
2. Osnovni pojmovi i važnost zaštite osobnih podataka	5
2.1. Podatci i informacije.....	5
2.2. Informacijsko društvo	5
2.3. Obrada podataka	6
2.4. Važnost zaštite podataka	7
3. Povijesni razvoj zapisivanja, obrade i zaštite podataka	9
3.1. Počeci zapisivanja i zaštite podataka	9
3.2. Obrada i zaštita podataka informacijsko-komunikacijskim tehnologijama	11
3.3. Veliki podatci	14
4. Zakonska regulativa zaštite osobnih podataka.....	17
4.1. Zakonodavstvo Europske unije	17
4.1.1. Povijesni razvoj zakonodavne regulative zaštite osobnih podataka u EU	17
4.1.2. Opća uredba o zaštiti osobnih podataka (GDPR)	21
4.1.3. Zaštita osobnih podataka u zakonodavstvu Republike Hrvatske.....	23
4.2. Usporedba sa zakonodavstvom drugih zemalja.....	24
5. Istraživanje o razini zaštite osobnih podataka u visokoškolskoj knjižnici.....	27
5.1. Cilj istraživanja.....	27
5.2. Metoda istraživanja.....	27
5.3. Rezultati istraživanja	27
5.4. Usporedba s istraživanjem o anonimnosti u hrvatskim i nizozemskim knjižnicama	32
6. Zaključak.....	36
7. Literatura.....	37

Sažetak

U ovome radu analizirane su mjere zaštite osobnih podataka, čiju je potrebu prepoznala Europska unija te je izglasana *Opća uredba o zaštiti podataka* (GDPR), koja je stupila na snagu 25. svibnja 2018. Promjene koje GDPR donosi trebale bi omogućiti građanima Europske unije veću kontrolu nad vlastitim podacima koje organizacije prikupljaju i obrađuju kako bi im pružile određene usluge. U radu je također predstavljeno istraživanje o razini zaštite osobnih podataka u Knjižnici Filozofskog fakulteta Sveučilišta u Zagrebu, koje je zatim uspoređeno s rezultatima istraživanja iz 2007. godine o razini anonimnosti korisnika u hrvatskim i nizozemskim knjižnicama. U suvremenom informacijskom društvu, koje svoj razvoj temelji na obradi mnoštva podataka, potrebna je regulacija prikupljanja i obrade osobnih podataka kako bi se zaštitila prava pojedinaca te kako ne bi došlo do zloupotrebe njihovih podataka.

Ključne riječi: *zaštita osobnih podataka, GDPR, privatnost, obrada podataka, informacijsko društvo, zaštita osobnih podataka u knjižnicama*

Personal Data Protection in the Information Society

Abstract

This paper analyses personal data protection measures, which the European Union recognised as necessary and therefore adopted the *General Data Protection Regulation* (GDPR), which came into effect on May 25, 2018. GDPR enables citizens of the EU to exercise greater control over their personal data that organisations collect and process in order to provide them with services. This paper will present the results of a research on the level of personal data protection in the Library of the Faculty of Humanities and Social Sciences in Zagreb. The research will be compared with the results of a 2007 study on the level of user anonymity in Croatian and Dutch libraries. In modern-day information society, whose development depends on data processing, it is necessary to regulate the collection and processing of personal data so as to protect the individual's rights, and so that their data would not be abused.

Key words: *personal data protection, GDPR, privacy, data processing, information society, personal data protection in libraries*

1. Uvod

U suvremenom informacijskom društvu, koje vrednuje podatke kao temelj za svoj razvitak, nužno je omogućiti slobodan protok podataka. No, mnogi podatci kojima se trguje identificiraju pojedinca i njegove interese, te je gotovo nemoguće dobiti određenu uslugu bez odavanja osobnih podataka. Ti se podatci ponekad koriste i za svrhe drugačije od one radi koje su prikupljeni, te se u medijima navodi sve više primjera sudskih tužbi protiv tvrtki koje osobne podatke svojih korisnika prodaju ili daju na uvid trećoj strani. Štoviše, jedna je društvena mreža najavila suradnju s bankama, kako bi korisnici mreže mogli vidjeti financijsko stanje drugih korisnika. Osobni podatci s društvenih mreža i ostalih mjesta na webu sve su traženiji i u državnim institucijama - SAD je najavio da će turisti za ulazak u zemlju morati odati i podatke kao što su stare e-mail adrese te svi stari i postojeći računi na društvenim mrežama. Privatnost pojedinca sve je više narušena, zbog čega je važno provesti odgovarajuće mjere zaštite.

Cilj ovoga rada je prikazati prijašnju i istražiti postojeću razinu zaštite osobnih podataka koje organizacije prikupljaju i obrađuju, stoga će se prvo objasniti uloga osobnih podataka i informacija u informacijskom društvu. Uz prikaz procesa obrade podataka, opisat će se i zašto je zaštita osobnih podataka danas posebno važna. U povijesnom kontekstu naznačit će se i kako je tekao razvoj zapisivanja, obrade i zaštite podataka, te kako je razvitak informacijsko-komunikacijske tehnologije doveo do nastanka fenomena velikih podataka, a posljedično i do novih izazova u zaštiti osobnih podataka.

Kako na zaštitu podataka uvelike utječe zakonodavstvo, prikazat će se kako su pojedine zakonske regulative imale utjecaja na protok podataka tržištem i na njihovu zaštitu. Zaštita osobnih podataka u raznim zemljama svijeta usporedit će se s razinom zaštite u Hrvatskoj i EU, s obzirom da se Europska unija najviše bavila pitanjem protoka, zaštite i automatske obrade osobnih podataka. U radu će se posebno naglasiti *Opća uredba o zaštiti podataka* (GDPR) koja je dovela do brojnih promjena u zaštiti podataka, te je aktualizirala problematiku zaštite osobnih podataka i potaknula javnu raspravu o toj temi na globalnoj razini.

Kako je cilj ovoga rada je istražiti trenutnu razinu zaštite osobnih podataka koje organizacije prikupljaju i obrađuju, provedeno je istraživanje u visokoškolskoj knjižnici kako bi se ustanovilo je li GDPR utjecao na odnos knjižnice prema podacima svojih korisnika. Naposljetku će se napraviti usporedba s istraživanjem o anonimnosti u hrvatskim i nizozemskim knjižnicama, koje su 2007. godine proveli Schepman, Koren, Horvat, Kurtović i Hebrang Grgić.

2. Osnovni pojmovi i važnost zaštite osobnih podataka

U ovome poglavlju definirat će se značenje i razlika između pojmova *podatak* i *informacija*, te će se pojasniti kontekst nastanka informacijskoga društva, što je također relevantno za temu rada. Opisat će se i proces obrade podataka te zašto je zaštita osobnih podataka posebno važna za suvremeno informacijsko doba.

2.1. Podatci i informacije

Kako bi se naznačila važnost zaštite osobnih podataka, potrebno je razlikovati pojmove podatak i informacija. Prema definiciji Hrvatske enciklopedije, podatkom se smatra svaka „poznata ili pretpostavljena činjenica na osnovi koje se oblikuje informacija“ („Podatak“, n.d.). Podatci sami po sebi nemaju značenje, već čine osnovu za stvaranje informacije. Iz definicije podataka slijedi da je informacija „skup podataka s pripisanim značenjem“ („Informacija“, n.d.). Zaštita osobnih podataka stoga je važna kako ne bi došlo do njihove zloupotrebe, jer pristup podacima, uz određeno znanje, omogućuje identifikaciju pojedinaca: „Ključnu ulogu u pretvorbi podataka u informaciju ima znanje kojim čovjek raspolaže. Ono mu omogućuje razumijevanje informacije, odn. prepoznavanje podataka, jezika kojim su ti podatci povezani u informaciju i konteksta na koji se odnose“ („Informacija“, n.d.).

2.2. Informacijsko društvo

Uloga zaštite osobnih podataka veća je nego ikada prije u današnjem tehnološki razvijenom informacijskom društvu, koje se definira kao društvo „koje svoj gospodarski, znanstv. i kult. razvoj zasniva na uvođenju i širenju računalne i telekomunikacijske tehnologije te stvaranju, obradbi i prijenosu informacija kao temelju za rast produktivnosti društva“ („Informacijsko društvo“, n.d.). Pojam informacijskog društva počeo se upotrebljavati ranih 1990-ih u dokumentima Europske unije u kojima je predložen strateški plan razvoja Europske unije u informacijskom društvu.

Kocijan (2014:9) navodi da su podatci „gorivo za informacijsko društvo bez kojega ne bi bile moguće inovacije o kojima današnji čovjek ovisi.“ U društvu koje vrednuje podatke i

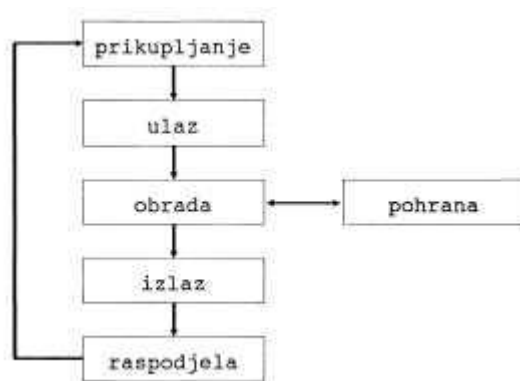
informacije kao važan segment za svoj napredak, postavlja se pitanje kako poštovati pravo na privatnost pojedinca, a istovremeno omogućiti slobodan protok podataka koji su potrebni za napredak društva. Europska unija je stoga usvojila niz dokumenata posvećenih zaštiti osobnih podataka, koji će se detaljnije obraditi u poglavlju o zakonskoj regulativi zaštite osobnih podataka.

2.3. Obrada podataka

U današnje postindustrijsko doba, ulogu proizvoda koji se stvaraju radi profita preuzeli su podatci. Razni podatci se kupuju te zatim obrađuju kako bi se unaprijedile određene usluge, a obrada podataka danas je gotovo nezamisliva bez upotrebe informacijsko-komunikacijskih tehnologija.

Tuđman et al. (1993) definiraju obradu podataka kao manipuliranje podacima kako bi se iskoristili za određenu svrhu, a podatke opisuju kao skup činjenica koje mogu biti brojčane, nebrojčane ili pak kombinacija brojčanih i nebrojčanih činjenica. Obrada može biti ručna ili automatska, a upravo je prodor računala doveo do veće mogućnosti obrade podataka, čineći informacijske sustave za obradu podataka bržim i točnijima, a samim time i efikasnijima. Kao temeljne operacije obrade podataka navode se zapisivanje, kopiranje, provjera, klasificiranje, uređivanje (sortiranje), spajanje, izračunavanje, pretraživanje, sažimanje te prikaz rezultata. Tuđman et al. (1993) navode i ciklus obrade podataka, koji se sastoji od tri temeljna koraka - ulaza, obrade i izlaza. Pod ulazom se podrazumijeva priprema ulaznih podataka za obradu, a oblik tih podataka ovisi o stroju kojim se vrši obrada. Procesom obrade ulazni se podatci mijenjaju ili kombiniraju s drugim informacijama kako bi se dobili podatci u prikladnom obliku, a rezultat obrade tih podataka skupljen je na izlazu.

Tuđman et al. (1993) također spominju i prošireni ciklus obrade podataka ([Slika 1](#)), koji uključuje tri dodatna koraka u procesu obrade: prikupljanje izvornih podataka, raspodjela izlaznih podataka te pohranjivanje podataka. Pohranjeni podatci mogu poslužiti kao ulazni podaci za daljnju obradu, a skup pohranjenih podataka zajedno s njihovim relacijama čini bazu podataka.

**Slika 1:** Prošireni ciklus obrade podataka

(Izvor: Tuđman et al., 1993:98)

2.4. Važnost zaštite podataka

Razvoj novih tehnologija, a time i efikasnijeg, automatiziranog načina obrade podataka, omogućio je prikupljanje sve veće količine podataka, čime su osobni podatci postali dostupniji nego ikada prije. Schepman et al. (2008) navode da su korisnici zbog toga sve više zabrinuti za svoju privatnost te da nisu uvijek informirani o načinu na koji se njihovi osobni podatci obrađuju. Horvat (2002) napominje da je identifikacija osobnim podacima često neizbježna za dobivanje određene usluge ili obavljanja određenog posla. Također navodi i da su nove informacijske tehnologije omogućile i objedinjavanje osobnih podataka, te da se pojedinac „može s pravom bojati da bi mu neovlašteni uvid u njegove osobne podatke mogao onemogućiti dobivanje neke usluge, povlastice itd.” (Horvat, 2002:3).

Neupitno je da obrada podataka omogućuje brojne koristi koje prije nisu bile moguće, kao što su navigacijske upute u stvarnom vremenu te obrada zdravstvenih podataka u svrhu otkrivanja uzroka bolesti. No, podatci se mogu smatrati i „ispušnim plinom informacijskoga doba“¹ (Schneier, 2015:20) ako ih usporedimo s ekološkim zagađenjem: „podatci kao ispušni plin su nešto što svi proizvodimo baveći se poslovima informacijskoga doba...Podatci su zagađenje informacijskoga doba, a zaštita privatnosti je ekološki izazov.“² (Schneier, 2015:279). Nadalje, postavlja se pitanje „kako osmisliti sustave koji će koristiti naše podatke

¹ Ovo je slobodni prijevod autora ovog rada koji u izvorniku glasi: “the exhaust of the information age.”

² “data as exhaust: something we all produce as we go about our information-age business... Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.”

za dobrobit društva u cjelini, a istovremeno zaštititi svakog pojedinačno...to je temeljno pitanje informacijskoga doba“³ (Schneier, 2015:278).

Zaštita osobnih podataka stoga je važna radi očuvanja vlastite privatnosti koja je „neophodna za slobodu, neovisnost i ljudsko dostojanstvo...nešto što se treba očuvati i štititi kako bi uistinu bili sigurni“⁴ (Schneier, 2015:273).

³ “how do we design systems that make use of our data collectively to benefit society as a whole, while at the same time protecting people individually...this is the fundamental issue of the information age.”

⁴ “essential for liberty, autonomy, and human dignity...something to maintain and protect in order to have real security.”

3. Povijesni razvoj zapisivanja, obrade i zaštite podataka

Podatci su se tijekom stoljeća zapisivali i obrađivali na različite načine, a o tome je ovisio i način njihove zaštite. U ovome poglavlju opisan će se koji su se važni podatci zapisivali te kako je tekao razvoj njihove obrade i koje je podatke bilo važno sačuvati. Razvoj informacijsko-komunikacijskih tehnologija omogućio je prikupljanje i čuvanje sve veće količine podataka, što je naposljetku dovelo do fenomena velikih podataka, a samim time i novih izazova u zaštiti osobnih podataka.

3.1. Počeci zapisivanja i zaštite podataka

Ljudi su tijekom povijesti komunicirali na različite načine – pokretima, signalizacijom, govorom, a naposljetku i pisanjem. Povijest obrade podataka usko je povezana s poviješću pisanja, koje se razvilo sukladno s razvitkom civilizacije: „Civilizacija je nastala u Egiptu i Mezopotamiji, zemljama obogaćenim velikim rijekama. I upravo su tamo pronađeni najraniji primjeri ključnog obilježja civilizacije – pisanja“⁵ (Casson, 2001:1).

Način zaštite podataka uvelike ovisi o mediju na kojem su podatci zapisani, a prvi materijali na kojima se pisalo izrađivali su se od sirovina kojima je određeno područje obilovalo. Sumerani, koji su živjeli u Mezopotamiji prije 3000. p.n.e., iskoristili su područje bogato glinom, te su informacije vrijedne bilježenja zapisivali na *glinenim pločicama* ([Slika 2a](#)). Materijal na kojem su drevni narodi pisali odigrao je veliku ulogu i u njihovu očuvanju. Tako su glinene pločice Sumerana ostale očuvane sve do danas, dok su mnogi zapisi starih Egipćana, koji su pisani na papirusu ([Slika 2b](#)), nestali. Dok je vatra najveća prijetnja papirusu i sličnim materijalima za pisanje, glinene pločice vatrom pak očvrstnu i postaju još trajnije, čime su bile pogodne za zapisivanje važnih informacija koje su Sumerani htjeli sačuvati. Unatoč njihovoj glomaznosti, glinene pločice koristile su se više od 2 i pol tisućljeća.

Kako su obale rijeke Nil bile bogate biljkama papirusa, Egipćani su od njih izrađivali materijal za pisanje koji je bio kvalitetan, ali krhak. Opstanak zapisa na papirusu iz staroga Egipta omogućila je egipatska suha klima te su zbog niske prisutnosti vlage do danas ostali

⁵ “It was in Egypt and Mesopotamia, lands abundantly watered by great rivers, that civilization arose. And it is there that we find the earliest examples of that key feature of civilization, writing”

brojni zapisi na papirusu, a tome je pridonio i zaštitni sloj pijeska koji se tijekom stoljeća nakupljao na papirusu. S druge strane, velika prijetnja papirusu bila je vatra. U požaru je 48. godine p.n.e. izgorilo stotine tisuća svitaka koji su se nalazili u najvećoj knjižnici toga doba - Aleksandrijskoj knjižnici, čime je zauvijek uništeno znanje koje su tadašnji intelektualci zapisivali.



a. Glinena pločica



b. Papirus



c. Ostrakon



d. Kodeks

Slika 2: Materijali za pisanje

Stari Grci pisali su i na komadima razbijene keramike, tzv. *ostrakonima* ([Slika 2c](#)), koji su služili za glasanje o osobama koje će izgnati iz grada. Zapise s trajnom važnosti, kao što su bračni ugovori ili knjige, zapisivali su na papirusu. Sumerani su također uglavnom zapisivali podatke administrativne prirode – račune, isporuke, potvrde o primitku, inventare, zajmove, bračne ugovore, razvode, sudske odluke i sl. Administrativni dokumenti sadržavali su i osobne podatke pojedinaca, a čuvali su se u svrhu arhiviranja.

Arhivi su se obično nalazili unutar kraljevskih palača, gdje su bile i radne knjižnice kraljevskih pisara, a u prošlosti su arhivi imali i dualnu ulogu knjižnica. Casson (2001) navodi da su se knjižnice i arhivi pojavili na Bliskom istoku u 3. tisućljeću p.n.e., usporedno s pojavom pisma. Vladarima je bilo u interesu zaštititi svoje knjižnice s obzirom da su knjižnice bile kraljeve privatne zbirke.

Knjižnična građa nije se kupovala, već se prepisivala - vlasnici knjižnica ili zbirki poslali bi svoje pisare da kopiraju željene tekstove, a kopije su se pravile i u svrhu zaštite. No, prepisivanje tekstova bilo je podložno namjernom ili nenamjernom iskrivljavanju teksta, stoga je bilo upitno koliko je kopija vjerna originalu. Casson (2001) spominje da je isti problem prisutan i danas, kada se knjige mehanički proizvode. Aleksandrijska knjižnica, koja je imala najveću zbirku građe toga doba (više od 500 000 svitaka), posjedovala je više primjeraka istih tekstova iz različitih mjesta, što je omogućilo da se ustanovi koji je standardni tekst. Egipatski vladari Ptolomeji zapise su nabavljali šaljući agente u potragu za što starijim kopijama, što je rezultiralo nastankom nove industrije – falsifikacije kopija.

Zapisi se uglavnom nisu mogli posuđivati niti iznositi iz palačkih knjižnica i arhiva, a pristup toj građi bio je dostupan samo uz prisustvo ovlaštene osobe. Casson (2001) navodi da se to može smatrati jednom od prvih mjera zaštite podataka. Vlasnici privatnih zbirki koji su posuđivali svoje glinene pločice često bi na njih u svrhu zaštite zapisivali i kletve, vjerujući da oni koji štiju određeno božanstvo neće ukrasti ili oštetiti pločice. Knjižnice su obično bile smještene uz hramove posvećene raznim bogovima, također u svrhu svojevrsne zaštite građe.

U drugom stoljeću nove ere, svitke od pergamenta i papirusa zamijenili su *kodeksi* ([Slika 2d](#)), koji su nalikovali današnjim knjigama. Kodeksima je bilo lakše rukovati nego glinenim pločicama ili svitcima, što je i omogućilo prodavanje knjiga, koje se odvijalo na glavnom trgu grada. Time su posjetitelji iz raznih dijelova svijeta napokon imali slobodan i širi pristup znanju.

U Srednjem vijeku knjige su se uglavnom čuvale u knjižnicama, koje su postojale u sklopu fakulteta, kraljevskih palača te samostana, gdje su se vrijedne knjige držale zaključanima u niši. U tom je razdoblju došlo do masovne proizvodnje knjiga izumom tiska pokretnim slovima koje je, prema web enciklopediji („Komunikacija“, n.d.), nastalo 1450. godine u Kini, a 1454. i u Njemačkoj. Izum tiska značajno je utjecao na širenje znanja, ali i manju mogućnost manipulacije informacijama nego što je bio slučaj s ručnim prepisivanjem tekstova.

3.2. Obrada i zaštita podataka informacijsko-komunikacijskim tehnologijama

U idućim stoljećima nije se puno promijenilo u zapisivanju, pohrani i zaštiti podataka, sve do kraja 18. stoljeća kada su uslijedile inovacije koje su omogućile lakše i brže prenošenje podataka i informacija. Na Hrvatskoj enciklopediji („Komunikacija“, n.d.) navodi se da su prvi

takvi izumi bili optički brzojav ([Slika 3a](#)), električni brzojav ([Slika 3b](#)) i fonograf ([Slika 3c](#)), a krajem 19. stoljeća došlo je i do obrata iz ručne u mehaničku obradu podataka.



a. Optički brzojav



b. Električni brzojav



c. Fonograf



d. Enigma

Slika 3: Izumi za prijenos informacija iz 19. i 20. stoljeća

Prema web enciklopediji („Računalo“, n.d.), za to je bilo zaslužan J.M. Jacquard koji je osmislio bušene kartice ([Slika 4a](#)) za pohranu informacija, a o rasporedu rupica na karticama ovisio je slijed operacija. Na temelju Jacquardova izuma, engleski matematičar Charles Babbage osmislio je analitički stroj ([Slika 4b](#)), čiji je program bio zapisan upravo na bušenim karticama.



a. Bušena kartica



b. Analitički stroj



c. Tabulator

Slika 4: Bušena kartica i strojevi za obradu podataka s bušenih kartica

Implementacijom struje razvila se i elektromehanička obrada podataka. Prve električne naprave za čitanje bušenih kartica – tabulatore ([Slika 4c](#)) – osmislio je američki statističar Herman Hollerith krajem 19. stoljeća. Freiburger, Hemmendinger, Pottenger i Swaine (2018) navode da je Hollerith izumio tabulator u svrhu mehanizacije popisivanja stanovništva. Prema enciklopediji Britannica („Census“, 2018), prvi popisi stanovništva vodili su se isključivo radi utvrđivanja koji ljudi moraju plaćati porez, koji će se unovačiti u vojsku te koji će biti prisiljeni na rad. Osobni podatci koji su se prikupljali bili su opskurni u usporedbi s modernim popisima koji su od 17. stoljeća uključivali sve više podataka. Kako su se ti podatci obrađivali ručno, popisivanje stanovništva u SAD-u bio je pravi pothvat s obzirom na veličinu zemlje i rastuću imigraciju. Takav način prikupljanja podataka bio je dugotrajan i nepotpun, a Kocijan (2014) navodi i da je većina podataka do kraja prebrojavanja već bila nevažeca. Mehanizacija popisivanja stanovništva stoga je bila prijeko potrebna, a Hollerithov izum prepoznale su i europske države te su također počele primjenjivati tabulatore za efikasniju obradu podataka o stanovništvu.

Istovremeno su izumljeni i uređaji za prijenos informacija i lakšu komunikaciju, od kojih Hrvatska enciklopedija („Komunikacija“) navodi telefon (1876), radio (1901) i televiziju (1925). Usporedno su se razvijali i strojevi za šifriranje podataka, od kojih je najpoznatiji njemačka Enigma ([Slika 3d](#)).

Daljnjem razvoju tehnologije za obradu podataka pridonio je izum računala s binarnim prikazom brojeva, a prema Hrvatskoj enciklopediji („Računalo“, n.d.) osmislio ga je Konrad Zuse 1938. Nekoliko godina kasnije osmišljen je i ENIAC (Electronic Numerical Integrator and Computer) - prvo cjelovito računalo s elektronskim cijevima, čime je započela elektronička obrada podataka.

Elektronske cijevi zamijenio je tranzistor kojega su prvi izradili J. Bardeen i Walter H. Brattain 1947. godine. Ubrzo su razvijeni i integrirani sklopovi te mikroprocesori, što je dovelo do prave revolucije na području računalne tehnologije. Rastu računalne snage svjedoči i Mooreov zakon o udvostručenju broja tranzistora svake dvije godine, za koji Schneier (2015) tvrdi da i dalje vrijedi.

Ubrzo je krenuo i razvoj računalnih mreža, a najvećom svjetskom računalnom mrežom postao je internet, poznat i kao „mreža svih mreža“. Preteča interneta bila je mreža ARPANET (*Advanced Research Projects Agency Network*) koja je nastala na inicijativu Ministarstva obrane SAD-a 1969. godine. Svrha ARPANET-a bila je povezati znanstveno-istraživačke

institucije, kako bi jednostavnijim dijeljenjem informacija između institucija unaprijedili vojnu tehnologiju. Nekoliko desetljeća kasnije, točnije početkom 1990-ih, na temelju ARPANET-a razvila se internetska mreža kakvu danas znamo i koristimo. Internet je omogućio pristup, objavljivanje i preuzimanje širokog spektra podataka, a komunikacija osobnih računala (klijenta) i servera (poslužitelja) preko interneta počela se odvijati putem protokola. Kako bi se podatci koji se razmjenjuju zaštitili, od 1994. godine se počinju koristiti sigurnosni protokoli poput HTTPS-a (*Hyper Text Transfer Protocol Secure*), koji kriptiraju podatke kao što su korisničko ime i lozinka za prijavu na određenu web stranicu.

Schneier (2015) spominje da se internetom prenose i biometrijski podatci s medicinskih uređaja, što može pomoći znanstvenicima u otkrivanju uzroka i ponašanja bolesti. No, takva istraživanja iziskuju veliku količinu podataka za obradu, te zahtijevaju i pomno osmišljene mjere zaštite osjetljivih podataka koje prenose.

3.3. Veliki podatci

Razvoj informacijsko-komunikacijske tehnologije i sve veća pristupačnost interneta omogućili su nagomilavanje svih mogućih podataka, odnosno stvaranje velikih podataka (eng. *big data*). Kocijan (2014) navodi da velike podatke karakteriziraju najmanje 3 V-a: volumen, odnosno velika količina podataka; varijantnost (raznolikost vrsta podataka); te velicitet (brzina prikupljanja novih podataka i njihove dostupnosti za analizu). Takvi podatci nadilaze mogućnost obrade u klasičnim relacijskim bazama podataka, a zahtijevaju i prilagodbu zaštitnih mjera podataka.

Veliki podatci u mnogočemu su korisni jer se iz njih mogu izvući relevantne informacije postupkom rudarenja podataka (eng. *data mining*). Bruce Schneier (2015) spominje brojne koristi rudarenja podataka, kao što su otkrivanje prijevara s kreditnim karticama i pojedinaca koji ne plaćaju porez. Podatci se rudare i u autoindustriji jer velika količina prikupljenih podataka o vožnji otkriva kako poboljšati sustave koji upravljaju automobilom, dok podatci o lokaciji sudionika u prometu otkrivaju stanje na cestama. No, za proces rudarenja u svrhu marketinga, političkih kampanja i sl., često se upotrebljavaju i osobni podatci pojedinca, poput njegove nacionalnosti i političke orijentacije te njegovih interesa, i to često bez njegova znanja i privole. Korisnici društvenih mreža često i nesvjesno otkrivaju svoje podatke, a tvrtke kao što su Google i Facebook rudare ih u svrhu oglašavanja ili ih prodaju trećoj strani. Prikupljeni

podatci koji se ne obrađuju također ostaju pohranjeni dok im se ne nađe svrha, odnosno kako bi se iskoristio njihov potencijal.

Pad cijena računalne memorije za pohranu podataka omogućio je organizacijama da trajno pohrane sve podatke o svojim korisnicima, čak i ako ta pohrana nema određenu svrhu, stoga se danas pohranjuje više podataka nego ikada prije: „Do 2010., mi kao vrsta smo dnevno stvarali više podataka, nego od početka vremena do 2003. godine“⁶ (Schneier, 2015:21). Fenomen velikih podataka rezultat je većeg stvaranja raznolikog sadržaja, čemu je uvelike pridonijela pojava interneta koja je omogućila pristupačniju objavu sadržaja. Primjer toga je i *lifelogging*, tj. bilježenje vlastitog života pisanjem bloga, snimanjem *vloga* (video bloga) i sl., čime se stvara velika količina podataka o pojedincu.

No, Schneier (2015:51) upozorava da veliki podatci ne osiguravaju anonimnost: „Možda naivno mislimo da nas je toliko puno da je jednostavno sakriti se u moru podataka. Ili da su većina naših podataka anonimni. No, to nije istina. Većina tehnika anonimizacije podataka ne funkcionira, a podatci se mogu deanonimizirati s iznenađujuće malo informacija.“⁷

Kako bi se spriječila identifikacija pojedinaca, pojedinci, ali i organizacije koje prikupljaju osobne podatke, trebali bi poduzeti određene mjere zaštite, a poseban naglasak je na enkripciji podataka: „Velika je matematička prednost u enkripciji naspram pokušaja probijanja enkripcije“⁸ (Schneier, 2015:168). Schneier (2015) navodi i da bi podizanje cijena nadzora i prikupljanja podataka moglo promijeniti politiku pružatelja usluga koji obrađuju osobne podatke. Također podržava i „*privacy by design*“ pristup, čijom se primjenom obrađuju samo oni podatci koji su nužni za pružanje određene usluge. Sve više web stranica primjenjuje ovaj pristup podacima: posjetitelji web stranice mogu odabrati hoće li web stranici dopustiti pristup svojoj lokaciji i prikupljanje kolačića za personalizaciju iskustva na stranici. Nedostatak ovakve primjene *privacy by design* pristupa je što neki posjetitelji web stranica smatraju da im odabir preferencija kolačića nepotrebno oduzima vrijeme te negativno utječe na njihovo iskustvo na web stranici.

⁶ “By 2010, we as a species were creating more data per day than we did from the beginning of time until 2003.”

⁷ “We might naively think that there are so many of us that it’s easy to hide in the sea of data. Or that most of our data is anonymous. That’s not true. Most techniques for anonymizing data don’t work, and the data can be de-anonymized with surprisingly little information.”

⁸ “There’s an enormous inherent mathematical advantage in encrypting versus trying to break encryption.”

Kocijan (2014) spominje da ulogu u zaštiti podatka imaju i algoritmičari, novonastali profesionalci koji bi obradu podataka trebali prilagoditi na način da se čuva tajnost osobnih podataka koji se analiziraju.

Naposljetku, važno je naglasiti i zakonodavni aspekt zaštite: „Tim Berners-Lee, osnivač World Wide Web-a, predlaže stvaranje nove Magna Carte, koja bi ograničila djelovanje vlada i korporacija te bi definirala ne samo prava, već i odgovornost korporacija informacijskoga doba“⁹ (Schneier, 2015:246). Više o tome bit će riječi u narednom poglavlju koje se bavi zakonskim regulativama zaštite osobnih podataka.

⁹ “Tim Berners-Lee, the inventor of the World Wide Web, has called for a new Magna Carta – one that restricts the actions of both governments and corporations, and that imposes responsibilities on information-age corporations rather than just rights.”

4. Zakonska regulativa zaštite osobnih podataka

Razvojem informacijskoga društva došlo je do potrebe za zakonskom regulacijom zaštite osobnih podataka, što će se u ovome poglavlju opisati prvenstveno kroz zakonodavstvo EU. Europska unija značajno je utjecala na protok podataka kojima se trguje, uključujući i osobne podatke, stoga će se prikazati kako je tekao razvoj zaštite podataka u EU. Poseban naglasak stavljen je na *Opću uredbu o zaštiti osobnih podataka*, koja je u svibnju 2018. godine stupila na snagu i donijela brojne promjene, kako za korisnike, tako i za pružatelje usluga. Opisat će se i kako se razvijalo zakonodavstvo o zaštiti osobnih podataka u Republici Hrvatskoj, a razina zaštite osobnih podataka u EU naposljetku će se usporediti i s drugim zemljama svijeta.

4.1. Zakonodavstvo Europske unije

4.1.1. Povijesni razvoj zakonodavne regulative zaštite osobnih podataka u EU

U *Priručniku o europskom zakonodavstvu o zaštiti podataka* navodi se da „prema članku 8. Europske konvencije o ljudskim pravima, pravo na zaštitu od prikupljanja i uporabe osobnih podataka dio je prava na poštovanje privatnog i obiteljskog života, doma i dopisivanja“ (2014:14) te da je „unutar prava Europske unije, zaštita podataka priznata kao temeljno pravo“ (2014:14). U Europskoj konvenciji o ljudskim pravima se time potvrđuje da EU već od svojega začetka pridaje vrijednost zaštiti osobnih podataka.

U *Priručniku* se također navodi da je pojavom informacijske tehnologije 1960-ih rasla „potreba za detaljnijim propisima kojima bi se zaštitili (osobni) podaci pojedinaca“ (2014:15) jer su, kako objašnjava Horvat (2002:3), „države vrlo brzo shvatile opasnost zlorabe mogućnosti koje pruža nova informacijska tehnologija.“ Slobodan protok informacija postao je bitna stavka europskoga tržišta, a kako se tehnologija za automatsku obradu i pohranu podataka razvijala istovremeno kada i Europska ekonomska zajednica (EEZ), ostvarena je i veća prekogranična razmjena podataka. Na temelju EEZ-a te Euratoma i Europske zajednice za ugljen i čelik nastala je Europska unija, koja je prepoznala potrebu za regulacijom protoka i obrade podataka te je doneseno više propisa s ciljem zaštite osobnih podataka. Najrecentniji među njima je *Opća uredba o zaštiti osobnih podataka*, čiji se razlog donošenja navodi i u preambuli: „Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti

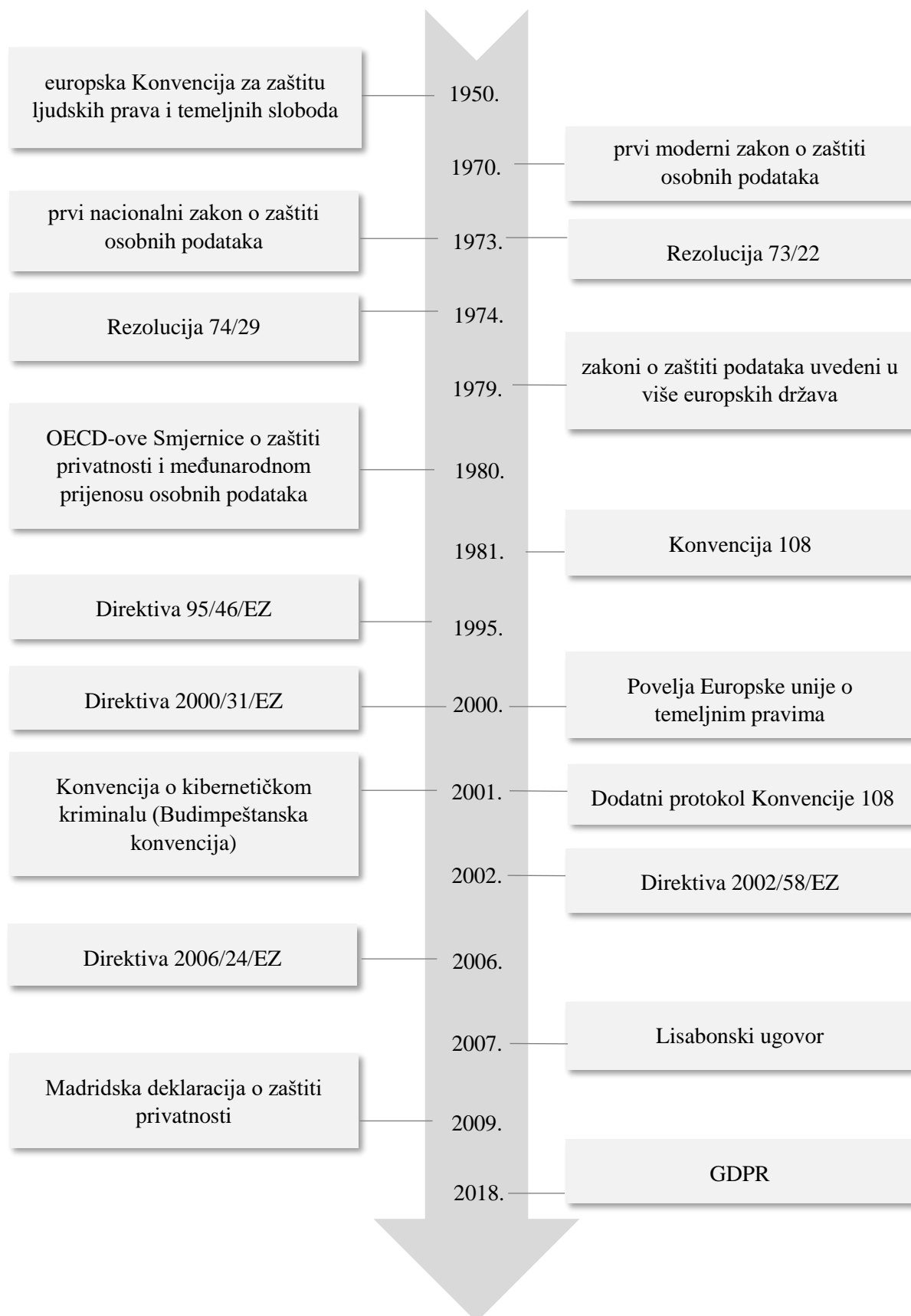
osobnih podataka...Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i gospodarstvo i društveni život te bi trebala dalje olakšavati slobodan protok osobnih podataka u Uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visoku razinu zaštite osobnih podataka.“ Sian Rudgard (2012) navodi detaljan povijesni pregled europskog zakonodavstva o zaštiti osobnih podataka, koji započinje sredinom 20. stoljeća, a vremenski je prikazan na [lenti 1](#).

U [tablici 1](#) navedeni su dokumenti značajni za zaštitu podataka, te su opisane promjene koje je svaki od njih donio. Iz tablice se vidi da je najviše regulativa o zaštiti podataka donijela Europska unija, što je označeno plavom bojom. Siva boja odnosi se na međunarodne dokumente, a narančasta predstavlja dokumente donesene na nacionalnoj razini. Također, zvjezdicom (*) su označeni dokumenti koji se primjenjuju i u Hrvatskoj.

europska Konvencija za zaštitu ljudskih prava i temeljnih sloboda *	<ul style="list-style-type: none"> države članice Vijeća Europa sastale su se u Rimu i potpisale konvenciju u kojoj se zaštita osobnih podataka navodi kao temeljno ljudsko pravo
1. moderni zakon o zaštiti osobnih podataka	<ul style="list-style-type: none"> uveden u njemačkoj saveznoj pokrajini Hessen
1. nacionalni zakon o zaštiti osobnih podataka	<ul style="list-style-type: none"> uveden u Švedskoj
Rezolucije 73/22 i 74/29	<ul style="list-style-type: none"> uspostavljena su načela zaštite podataka u automatiziranim bazama
nacionalni zakoni o zaštiti podataka	<ul style="list-style-type: none"> 7 država članica Europske unije uvele su nacionalne zakone o zaštiti podataka
Smjernice o zaštiti privatnosti i međunarodnom prijenosu osobnih podataka	<ul style="list-style-type: none"> Smjernice je objavila Organizacija za ekonomsku suradnju i razvoj (OECD)
Konvencija 108 *	<ul style="list-style-type: none"> prvi međunarodni obvezujući akt koji se izričito bavi zaštitom podataka

Direktiva 95/46/EZ	<ul style="list-style-type: none"> • zaštita podataka prvi put je regulirana unutar prava Europske unije
Direktiva 2000/31/EZ	<ul style="list-style-type: none"> • Direktiva o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini)
Povelja Europske unije o temeljnim pravima *	<ul style="list-style-type: none"> • posebnu pozornost pridaje zaštiti osobnih podataka
Dodatni protokol Konvencije 108 *	<ul style="list-style-type: none"> • koncept „primjerene“ razine zaštite osobnih podataka koji su preneseni u države izvan EU
Konvencija o kibernetičkom kriminalu (Budimpeštanska konvencija) *	<ul style="list-style-type: none"> • bavi se zločinima počinjenim protiv i putem elektroničkih mreža
Direktiva 2002/58/EZ (Direktiva o e-privatnosti) *	<ul style="list-style-type: none"> • bavi se regulacijom povjerljivosti informacija i postupanjem s podacima o prometu te spamom i kolačićima
Direktiva 2006/24/EZ	<ul style="list-style-type: none"> • obvezivala je pružatelja elektroničkih komunikacijskih usluga na zadržavanje određenih podataka, kako bi ti podatci bili dostupni u svrhu istrage, otkrivanja i progona teških kaznenih djela
Lisabonski ugovor *	<ul style="list-style-type: none"> • uvodi se Europski nadzornik za zaštitu podataka
Madridska deklaracija	<ul style="list-style-type: none"> • artikuliraju se prava na zaštitu privatnosti • potpisalo ju je više od 100 tvrtki
GDPR *	<ul style="list-style-type: none"> • zamijenio je Direktivu 95/46/EZ

Tablica 1: Pravni akti i promjene značajne za zaštitu osobnih podataka



Lenta 1: Povijesni pregled europskog zakonodavstva o zaštiti osobnih podataka

4.1.2. Opća uredba o zaštiti osobnih podataka (GDPR)

Uredba Europske unije o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, poznatija pod akronimom GDPR (eng. General Data Protection Regulation), donesena je 27. travnja 2016. u Bruxellesu od strane Europskog parlamenta i Vijeća Europske unije, a stupila je na snagu dvadesetog dana od dana objave u Službenom listu Europske unije. Sukladno članku 99., stavku 2., Uredba se primjenjuje od 25. svibnja 2018. u svim državama članicama Europske unije.

Prema web stranici Europskog nadzornika za zaštitu podataka („The History of the General Data Protection Regulation“, 2018), razvoj GDPR-a počinje 2012. godine kada je Europska komisija predložila reformu direktive o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka iz 1995. Cilj reforme bio je ojačati pravo na zaštitu podataka na internetu i unaprijediti digitalno gospodarstvo. Narednih se godina pripremala nova uredba kako bi se ispravili nedostaci direktive 95/46/EZ, što je značajno jer se definicija tih dvaju pojmova odnosi na način njihove primjene na nacionalno zakonodavstvo država članica EU: „sam pojam “Uredbe” znači da se izravno primjenjuje u zakonodavni okvir zemalja članica (izuzev u nekolicini pojmova koji se ostavljeni za razradu u nacionalnim zakonodavstvima) za razliku od do sada važeće “Direktive” koja je predstavljala “samo” Smjernice djelovanja“ (Boban, 2018:28).

Europski je parlament glasovanjem na plenarnoj sjednici 12. ožujka 2014. dao potporu novoj Uredbi sa 621 glasom *za* te samo 10 glasova *protiv*. Dvije godine kasnije, 27. travnja 2016., GDPR službeno je donesen, a na snagu je stupio 20 dana nakon objave u Službenom listu Europske unije. Europska komisija također je predložila i donošenje dvije nove uredbe o privatnosti i elektroničkim komunikacijama (ePrivatnost) kako bi se uskladila postojeća pravila s odredbama GDPR-a. Značaj ove uredbe je „determinirati granice i maksimalno zaštititi protok podataka s naglaskom na obradu osobnih podataka i zaštitu privatnosti građana na području Europske unije u suvremenom informacijskom društvu“ (Boban, 2018:29).

Prema GDPR-u, osobni podatci definiraju se kao „svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni,

ekonomski, kulturni ili socijalni identitet tog pojedinca”. Boban (2018) spominje da se GDPR-om proširila definicija prvoga Zakona o zaštiti osobnih podataka jer se po prvi puta biometrijski podaci zakonski definiraju kao osobni podaci, a uvode se i pojmovi *mrežni identifikator* te *obrada lokacije*.

U Uredbi se, uz enkripciju, kao jedna od mogućih zaštitnih mjera spominje i pseudonimizacija, koja je prema članku 4., stavku 5. GDPR-a definirana kao „obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi“.

Za obradu podataka u skladu s GDPR-om, pružatelj usluge od korisnika mora dobiti privolu, odnosno „svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose“ (GDPR, čl. 4, st. 11.), a mora biti napisana jasnim i jednostavnim jezikom. Posebno je regulirana privola djeteta u odnosu na usluge informacijskog društva te je određeno da je obrada osobnih podataka djece dopuštena ako je dijete napunilo 16 ili više godina ili ako je privolu dao nositelj roditeljske odgovornosti. S druge strane, države članice imaju mogućnost sniziti tu dobnu granicu, no ona ne smije biti niža od 13 godina. Važna stavka je i da korisnik usluge može u svakom trenutku povući privolu, što mora biti jednako jednostavno kao i njezino davanje.

Prije obrade osobnih podataka, voditelji obrade dužni su napraviti procjenu učinka obrade. Boban (2018) navodi da je poglavlje o procjeni učinka izazvalo najviše interesa kod donošenja GDPR-a jer to do sada nije bila obveza voditelja zbirke podataka. Procjenu učinka na zaštitu osobnih podataka provodi voditelj obrade prije same obrade kako bi utvrdio razinu rizika obrade, to jest je li obrada visokorizična za prava i slobodu pojedinaca. Procjena učinka obvezna je prilikom obrade podataka velikog opsega, a posebno prilikom obrade osobnih podataka na regionalnoj, nacionalnoj ili nadnacionalnoj razini. Procjenu učinka također je potrebno provesti i za „opsežno praćenje javno dostupnih područja, posebno ako se upotrebljavaju optičko-elektronički uređaji“ (GDPR, preambula, 91).

Boban (2018) navodi i da su tvrtke u slučaju proboja sigurnosti osobnih podataka dužne o tome obavijestiti pojedinca, kao i o samoj prirodi povrede podataka. U GDPR-u navedeni su i uvjeti novčanog kažnjavanja te su propisane i kazne za kršenje Uredbe čiji iznos ovisi i o tijelu

koje krši odredbe te o odredbama koje nisu ispoštovane – kazne za voditelje i izvršitelje obrade te za certifikacijska tijela i tijela za praćenje mogu iznositi do 10 000 000 EUR, a ako se radi o poduzetniku do 2 % ukupnog godišnjeg prometa na svjetskoj razini, ovisno o tome što je veće, dok kazne za kršenje drugih važnih odredbi mogu iznositi čak 20 000 000 EUR, ili do 4 % ukupnog godišnjeg prometa. Boban (2018) napominje da se od donošenja GDPR kazne, za razliku od ranije, odnose na sve tvrtke koje posluju na području Europske unije.

Kako bi se osigurala primjena odredbi o zaštiti osobnih podataka, GDPR propisuje i obvezu uvođenja nadzornog tijela, čiju ulogu u Hrvatskoj ima Agencija za zaštitu osobnih podataka (AZOP). Nadzorno tijelo, osim što brine o provođenju GDPR-a, rješava i pritužbe o kršenju prava na zaštitu osobnih podataka, te promiče svijest o rizicima i mjerama zaštite podataka.

Agencija je također razvila i dvije edukativne mobilne aplikacije s ciljem podizanja svijesti o važnosti zaštite osobnih podataka te o odredbama GDPR-a. Aplikacija „AZOP“ primarno je namijenjena djeci, a na web stranici AZOP-a navedeno je da „sadrži korisne savjete za djecu o tome kako se ponašati i zaštititi na internetu i društvenim mrežama, kratki internetski pojmovnik, ali ujedno i savjete za roditelje, učitelje, nastavnike, školske pedagoge i psihologe.“ Također, ova aplikacija nudi i mogućnost slanja pitanja AZOP-u vezanih uz privatnost, edukaciju o privatnosti te o samoj Agenciji. Druga je aplikacija namijenjena široj javnosti kao vodič kroz GDPR, a trebala bi poslužiti kao informativni alat. Cilj ove aplikacije je približiti propise Uredbe pojedincima i poslovnim subjektima, a aplikacija također nudi i mogućnost slanja obavijesti o mogućim promjenama GDPR-a te o novim aktivnostima Agencije.

4.1.3. Zaštita osobnih podataka u zakonodavstvu Republike Hrvatske

Prema Ustavu Republike Hrvatske (2010), pod poglavljem o zaštiti ljudskih prava i temeljnih sloboda te potpoglavljem o osobnim i političkim slobodama i pravima, navodi se sljedeće:

„Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita osobnih podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja“ (Narodne novine, br. 85/2010, 2010).

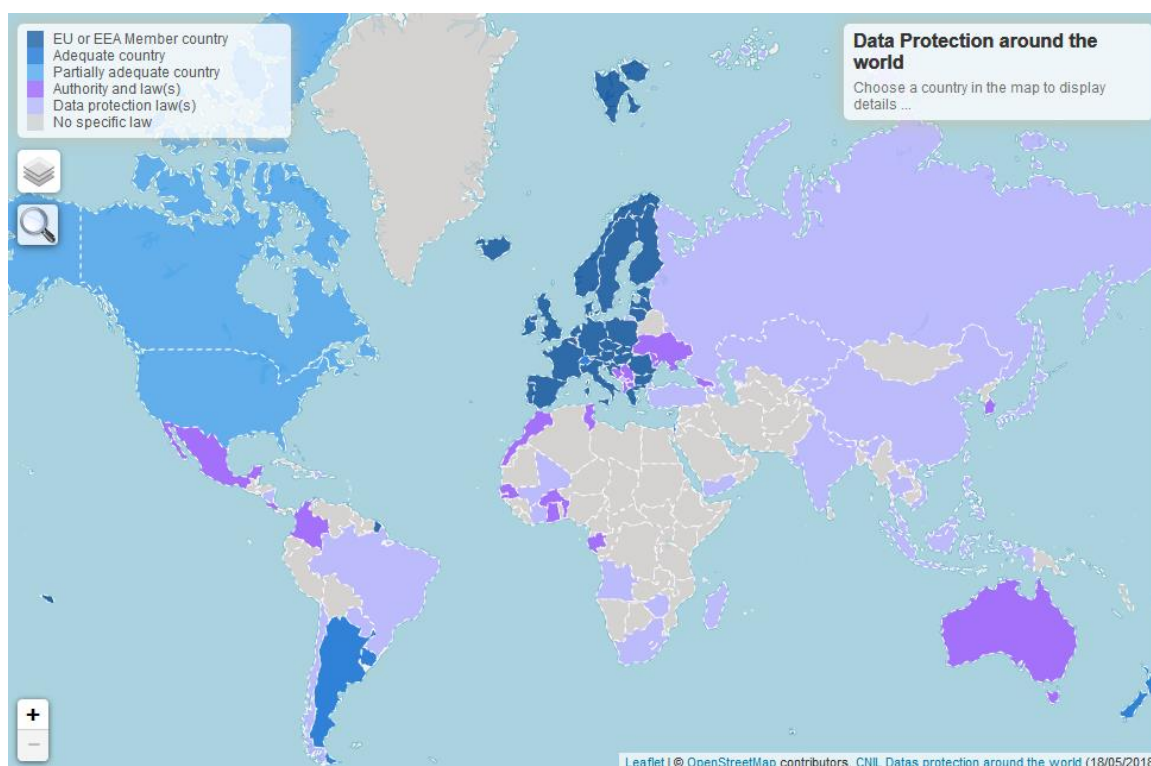
RH je kao članica Vijeća Europe potpisnica Konvencije o zaštiti osoba glede automatske obrade osobnih podataka (Konvencija 108) i Dodatnog protokola uz Konvenciju 108, a Zakon o potvrđivanju Konvencije i Dodatnog protokola uz Konvenciju 108 donesen je 2005. godine. Hrvatski sabor je 2003. godine donio i Zakon o zaštiti osobnih podataka, koji je vrijedio sve do 25. svibnja 2018. kada je na snagu stupio Zakon o provedbi Opće uredbe o zaštiti podataka, čime je GDPR implementiran i u nacionalno zakonodavstvo RH.

4.2. Usporedba sa zakonodavstvom drugih zemalja

Francuska agencija za zaštitu osobnih podataka CNIL (*Commission Nationale de l'Informatique et des Libertés*) objavila je na svojoj web stranici interaktivnu kartu ([Slika 5](#)) koja nudi kratki pregled razine zakonodavne zaštite osobnih podataka svih zemalja svijeta za koje imaju podatke.

Na karti su zemlje razvrstane po kategorijama ovisno o primjerenosti razine zaštite koja se u određenoj zemlji primjenjuje. Europska komisija može donijeti odluku o prenošenju podataka u drugo društvo u trećoj zemlji „a da pritom nema potrebe za izvoznikom podataka koji bi pružio dodatne zaštitne mjere ili bez podlijevanja dodatnim uvjetima. Drugim riječima, prijenosi u „primjerenu” treću zemlju bit će izjednačeni s prijenosom podataka unutar EU-a“ („Koja se pravila primjenjuju ako moja organizacija prenosi podatke izvan EU-a?”, 2018).

Prvu kategoriju na karti označenu tamnoplavom bojom čine zemlje Europske unije i Europskog gospodarskog prostora (EEA), a sljedeće kategorije čine zemlje koje prema procjeni EU imaju primjerenu razinu zaštite osobnih podataka (Švicarska, Argentina, Urugvaj, Izrael i Novi Zeland), djelomično primjerenu razinu zaštite (Kanada, SAD), te zemlje koje ne osiguravaju dovoljnu razinu zaštite prema procjeni EU-a (Srbija, BiH, Makedonija, Albanija, Meksiko, Australija, Južna Koreja, Kolumbija, Ukrajina, Tunis, i dr.), kao i države koje također imaju zakone o zaštiti osobnih podataka, no koji se smatraju nedovoljnima (Rusija, Turska, Kina, Brazil). Pregledom pojedine zemlje na karti prikazuje se i koja je organizacija zadužena za provedbu zakona o zaštiti podataka.



Slika 5: Karta s prikazom razine zakonodavne zaštite osobnih podataka prema procjeni EU (Izvor: Data protection around the world, CNIL)

Razliku u razini zaštite osobnih podataka Schneier (2015) pripisuje različitim kulturološkim i vremenskim definicijama privatnosti: „Naše osobne definicije privatnosti su i kulturalne i situacijske. Definicije koje su vrijedile prije 100 godina razlikuju se od današnjih, a razlikovat će se i za 100 godina. Različite su i u SAD-u, Europi, Japanu i drugdje. Razlikuju se i generacijski. Danas smo zbog utjecaja interneta prisiljeni promijeniti naše stavove o privatnosti kao nikada do sada.“¹⁰ (270)

Dok su sve države članice Europske unije morale implementirati Opću uredbu o zaštiti podataka u svoje zakonodavstvo, u Sjedinjenim Američkim Državama svaka federalna jedinica u svojem zakonodavstvu ima različite odredbe o zaštiti podataka. Schneier (2015) navodi da je SAD jedina zemlja Zapada koja nema temeljne zakone o zaštiti osobnih podataka, te da „za razliku od EU, u SAD-u danas vaše osobne informacije nisu vaše vlasništvo, već od onoga koji ih prikuplja. Zakoni štite određene kategorije osobnih podataka – financijske podatke,

¹⁰ “Our personal definitions of privacy are both cultural and situational. They were different 100 years ago than they are today, and they’ll be different 100 years from now. They’re different in the US than they are in Europe, Japan, and elsewhere. They’re different across generations. Right now, the Internet is forcing our attitudes about privacy to shift as never before.”

informacije o zdravstvenoj skrbi, podatci o studentima, o posudbi videovrpce – no to nije ni približno opsežnim zakonima o zaštiti osobnih podataka u europskim zemljama¹¹ (Schneier, 2015:229). Schneier (2015) također spominje i prijedlog zakona iz 2012. godine *US Consumer Privacy Bill of Rights* koji je trebao osigurati transparentnost o obradi osobnih podataka te omogućiti pojedincima veću kontrolu nad svojim podacima, ali ovaj prijedlog zakona nije prihvaćen. No, prema članku Alyson Sandler (2018) na web stranici *Inside Privacy*, nekoliko američkih senatora predložili su 2017. dva zakona o zaštiti osobnih podataka - *Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act* te *Secure and Protect Americans' Data Act*, no odluka o njihovom prihvaćanju još nije donesena. U travnju 2018. predložen je i zakon pod nazivom *Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act*, kojim bi se korisnike moralo obavijestiti o tome koje vrste osjetljivih podataka od njih prikupljaju pružatelji, te kako će ih oni koristiti i s kime će ih dijeliti.

No, Schneier (2015) smatra da je pravo na privatnost, odnosno zaštitu osobnih podataka, implicitno zajamčena četvrtim, petim i devetim amandmanima u Povelji o pravima Ustava Sjedinjenih Američkih Država, kojima se građani štite od neopravdane pretrage i svjedočenja protiv samih sebe, te im se jamče druga prava koja nisu eksplicitno navedena u zakonodavstvu SAD-a, ali se podrazumijevaju.

¹¹ “Unlike in the EU, in the US today personal information about you is not your property; it’s owned by the collector. Laws protect specific categories of personal data – financial data, healthcare information, student data, videotape rental records – but we have nothing like the broad privacy protection laws you find in European countries.”

5. Istraživanje o razini zaštite osobnih podataka u visokoškolskoj knjižnici

5.1. Cilj istraživanja

Cilj istraživanja razine zaštite osobnih podataka na primjeru visokoškolske knjižnice bio je ustanoviti koji se podatci prikupljaju o korisnicima knjižnice, na koji način se prikupljaju, obrađuju, pohranjuju i čuvaju ti podatci, te je li stupanje na snagu Opće uredbe o zaštiti osobnih podataka utjecalo na knjižnicu i uzrokovalo promjene.

5.2. Metoda istraživanja

Ovo je istraživanje provedeno intervjuiranjem sistemske knjižničarke Knjižnice Filozofskog fakulteta u Zagrebu, a rezultati istraživanja naposljetku su uspoređeni s radom stručnjaka iz Nizozemske i Hrvatske koji su 2007. godine istraživali anonimnost u javnim knjižnicama tih dviju zemalja.

5.3. Rezultati istraživanja

Prema novom *Pravilniku o uvjetima i načinu korištenja građe i usluga Knjižnice Filozofskog fakulteta Sveučilišta u Zagrebu*, koji je donesen 18. travnja 2018., a stupio je na snagu 23. travnja 2018., knjižnica FFZG-a s osobnim podacima svojih članova postupa sukladno zakonskim odredbama o zaštiti osobnih podataka, kao što je navedeno i u *Pravilniku (2018)*: „Podaci o članovima su povjerljivi i tretiraju se sukladno odredbama Zakona o zaštiti osobnih podataka te Uredbi EU o zaštiti osobnih podataka (GDPR).” (čl. 4, st. 1.) Knjižnica prikuplja samo one osobne podatke korisnika koji su nužni kako bi osigurala vlastitu imovinu, odnosno svoj knjižnični fond. Osobni podatci članova stoga su važni u slučaju da korisnik koji posudi određenu knjižničnu građu ne vrati ili uništi istu. Knjižnica, dakle, ne prikuplja podatke o svojim članovima radi njihove identifikacije, već radi praćenja koja je knjižnična građa posuđena i vraćena.

Učlanjivanje studenata Filozofskog fakulteta u Knjižnicu vrši se preuzimanjem određenih osobnih podataka iz ISVU sustava (Informacijski sustav visokih učilišta RH) koje

studenti daju prilikom upisa na sam Fakultet. Ti se podatci upisuju u elektronički imenik te se studentima pritom dodjeljuje elektronički identitet u AAI@EduHr sustavu (Autentifikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj). U Pravilniku (2018) se navodi i značaj elektroničkog identiteta za članove Knjižnice: „Elektronički identitet iz sustava AAI@EduHr je važna imovina svakog člana akademske i istraživačke zajednice koji omogućava pristup velikom broju različitih usluga, pristupanje svojim osobnim podacima i ostvarivanje različitih materijalnih prava. Zbog svega navedenog elektronički identitet treba koristiti isključivo osobno, ne ga davati drugim osobama i pažljivo ga čuvati od svake neovlaštene uporabe” (čl. 24., st. 3.).

Obvezni podatci koje Knjižnica preuzima su ime, prezime, adresa prebivališta, adresa elektroničke pošte, telefonski brojevi, jedinstveni matični broj akademskog građanina (JMBAG) i OIB, a za strane državljane i broj putovnice. Studentima i zaposlenicima FFZG-a bilježi se i podatak o elektroničkom identitetu iz sustava AAI@EduHr, a Knjižnica ne preuzima podatke iz ISVU sustava koji nisu potrebni radi sigurnosti, kao što je podatak o studijskoj grupi.

Članovi Knjižnice prema Pravilniku (2018) mogu biti studenti, zaposlenici i vanjski suradnici Filozofskog fakulteta te počasni članovi Knjižnice, dok se ostali građani mogu koristiti građom i uslugama samo unutar Knjižnice. Članovi Knjižnice mogu se prijaviti na web katalog Knjižnice putem svojeg AAI@EduHr elektroničkog identiteta, što im omogućava samostalno produživanje roka posudbe građe, kao i uvid u podatke koje knjižnica ima o članu te mogućnost izmjene istih. Članovi Knjižnice dužni su prijaviti svaku promjenu osobnih podataka, što mogu napraviti obavještanjem zaposlenika Knjižnice, koji će zatim ažurirati te podatke, ili samostalno putem prijave na web stranici Knjižnice. No, vlastitu izmjenu osobnih podataka mora potvrditi zaposlenik Knjižnice prije spremanja promjena, kako ne bi došlo do upisivanja krivih podataka ili pak gubitka potrebnih podataka korisnikovim brisanjem. Nakon izmjene, stari osobni podatci se ne čuvaju. Osobni podatci koji se mogu promijeniti prijavom na web stranicu Knjižnice su ime i prezime, datum rođenja, spol, adresa i mjesto stanovanja, broj telefona i e-mail adresa. Podatci koje korisnici pak ne mogu mijenjati su jedinstveni matični broj građana (JMBG), jedinstveni matični broj akademskog građana (JMBAG) te porezni broj (OIB). Na web profilu mogu se vidjeti i podatci o članstvu, kao što su broj članske iskaznice, datum isteka članstva te kategorija pod koju se član svrstava (student, zaposlenik i sl.). U web katalogu se bilježi i zapis povijesti posudbe, a članovi ne mogu isključiti tu opciju. Također se bilježe i oznake (*tagovi*) koje članovi mogu dodijeliti građi u web katalogu, te liste

djela koje mogu slagati. Prilikom plaćanja usluge međuknjižnične posudbe u sustavu se bilježe i podatci o plaćanju, odnosno koliko je korisnik dužan platiti Knjižnici za usluge.

Osobni podatci članova Knjižnice vode se i obrađuju u integriranom knjižničnom sustavu otvorenog koda *Koha*, kojega kontinuirano razvija zajednica programera Kohe i knjižnica. Djelatnici Knjižnice FFZG-a prijavljuju se u sustav putem svog AAI@EduHr elektroničkog identiteta, a njihove mogućnosti korištenja sustava ovise o ovlastima koje su im dodijeljene. Studenti koji odrađuju praksu u Knjižnici također se mogu prijaviti u sustav, no oni, za razliku od djelatnika Knjižnice, nemaju ovlasti mijenjati osobne podatke članova Knjižnice. Djelatnici pak ne mogu samostalno promijeniti korisničko ime i lozinku članova jer je korisničko ime u nadležnosti AAI@EduHr sustava, dok zaporku korisnik može promijeniti sam.

U slučaju neovlaštenog pristupa nečijem osobnom korisničkom računu djelatnici Knjižnice mogu blokirati korisnički račun, a korisnik može i dalje posuđivati građu nekim drugim oblikom identifikacije (npr. osobnom iskaznicom).

Osobni podatci djelatnika Knjižnice jednako su zaštićeni kao i podatci drugih članova Knjižnice – svi djelatnici Knjižnice imaju službenu e-mail adresu i broj telefona koji su javno dostupni, a mogu se koristiti i privatnim e-mail adresama i brojevima telefona.

Prema Pravilniku (2018), članstvo zaposlenika prestaje s prekidom radnog odnosa, dok studenti FFZG-a ostaju članovi dokle god imaju studentska prava. Prestankom članstva osobni podatci korisnika knjižničnih usluga za sada se ne brišu, već ostaju pohranjeni u bazi podataka. Brisanje osobnih podataka već je omogućeno u sustavu *Koha* alatom za brisanje, odnosno anonimizaciju, a u planu je da se nepotrebni podatci počnu brisati nakon što se ustanove kriteriji po kojima će se brisati.

Osobni podatci korisnika knjižničnih usluga ne prikupljaju se u svrhu statističke analize, no Knjižnica je dužna dostaviti određene podatke za statističku analizu svojoj matičnoj knjižnici, a to je Nacionalna i sveučilišna knjižnica u Zagrebu (NSK). U tu svrhu Knjižnica FFZG-a prikuplja agregirane podatke, što je i javno dostupno na web stranici Sustava statističkih podataka o knjižnicama, kojega vodi NSK. Na stranici impresuma Sustava (2018) navedeno je da su trenutačno dostupni podatci sustavu samo testni podaci, koji se koriste za ispitivanje samog sustava. Navedeno je da su statistički podatci važni za analizu poslovanja knjižnica, a sadrže podatke za 2017. godinu o uslugama i korištenju usluga, kao što su ukupan broj posudbi u i izvan knjižnica te ukupan broj aktivnih korisnika po kategorijama članstva.

Također sadrži i podatke o fondu knjižnice, opremi i troškovima te o osoblju knjižnice, a osobni podatci korisnika i zaposlenika knjižnice nisu evidentirani.

Upotreba i kretanje web stranicom Knjižnice također se ne prati u svrhu analize, bilo da su posjetitelji prijavljeni na stranicu ili ne. Vidljiva je samo IP adresa posjetitelja, a komunikacija posjetitelja web stranice i servera osigurana je HTTPS protokolom, čijom je enkripcijom zaštićen prijenos podataka između posjetitelja web stranice i servera.

Knjižnica ne prati ni preuzimanja pojedinačnih korisnika iz baze elektroničkih časopisa na koje je Knjižnica pretplaćena, a kojoj korisnici pristupaju prijavom s vlastitim elektroničkim identitetom preko web stranice Knjižnice, već se samo bilježi ukupan broj preuzimanja s određene baze radi statistike koju je Knjižnica FFZG-a dužna dostaviti matičnoj knjižnici. Ovi se podatci koriste kako bi se ustanovilo koliko se koja baza elektroničkih časopisa koristi, na temelju čega se procjenjuje daljnja pretplata na bazu, a ne radi praćenja interesa korisnika.

Aktivnosti korisnika Knjižnice ne prate se ni unutar prostorija same Knjižnice, a jedino se ulaz u knjižnicu nadzire sigurnosnim kamerama jer se tamo nalaze i RDIF čitači. Ulazni prostor nadzire se samo radi sigurnosti fonda, a kamera je u nadležnosti Fakulteta.

Prema odredbama GDPR-a, organizacijama s manje od 250 zaposlenika dopuštena su određena odstupanja od odredbi, što uključuje i zapošljavanje službenika za zaštitu osobnih podataka. S obzirom da je u Knjižnici Filozofskog fakulteta zaposleno pedesetak djelatnika te da Knjižnica radi u sklopu Filozofskog fakulteta Sveučilišta u Zagrebu, Knjižnica nije odredila vlastitog službenika, već je za tu dužnost odgovoran službenik za zaštitu podataka Filozofskog fakulteta. Službenik prema GDPR-u mora imati određene kvalifikacije, odnosno stručno znanje o pravu i praksama u području zaštite podataka, te je obavezan obavljati svoju dužnost pazeći na tajnost i povjerljivost osobnih podataka.

Na web stranici Filozofskog fakulteta navedeno je da se osobni podatci pojedinaca čuvaju u skladu s Uredbom, tj. da se podatci „u obliku koji omogućuje identifikaciju čuvaju se samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju“ („Zaštita osobnih podataka“, 2018). Ispunjavanjem obrazaca koji se nalaze na stranici Fakulteta pojedinac može zatražiti pristup, izmjenu te brisanje osobnih podataka, kao i davanje privole za obradu osobnih podataka. Navedeno je da pojedinci imaju i pravo na prigovor vezan uz obradu njihovih podataka, te pravo na prenosivost podataka.

Na temelju navedenog, GDPR nije utjecao na način prikupljanja, korištenja, pohrane i zaštite osobnih podataka korisnika Knjižnice Filozofskog fakulteta jer je Knjižnica isti odnos

prema osobnim podacima svojih korisnika imala i prije donošenja GDPR-a. Jedina promjena do koje je došlo odnosi se na zaposlenike Knjižnice koji su morali potpisati izjavu o čuvanju povjerljivosti i tajnosti podataka. Stoga je prije stupanja GDPR-a na snagu, održana prezentacija za djelatnike Knjižnice kako bi se upoznali s odredbama GDPR-a. Potpisivanjem izjave, djelatnici su dužni čuvati povjerljivost i tajnost osobnih podataka kojima imaju pristup prilikom rada s korisnicima, a mogu ih koristiti isključivo za propisanu svrhu te ih ne smiju odavati trećim osobama. Čuvanje osobnih podataka korisnika na ovaj način je i prije bila praksa djelatnika Knjižnice, na što ih je obvezivao i Pravilnik.

Horvat (2002) napominje da se čuvanje tajnosti podataka u knjižnicama može činiti oprečnim, s obzirom da je knjižnična djelatnost prema Zakonu o knjižnicama definirana kao javna služba. Knjižničari stoga moraju osigurati korisnicima slobodan pristup informacijama, no Horvat (2002) također navodi da, sukladno IFLA-inoj izjavi Knjižnice i intelektualna sloboda, korisnici knjižnica imaju pravo na privatnost i anonimnost, što znači da knjižničari nikako ne smiju otkriti identitet korisnika knjižnice trećoj osobi.

5.4. Usporedba s istraživanjem o anonimnosti u hrvatskim i nizozemskim knjižnicama

U istraživanju koje su 2007. godine proveli Schepman, Koren, Horvat, Kurtović i Hebrang Grgić, te objavili u članku *Access With(out) Anonymity* (2008), analizirala se razina anonimnosti korisnika u hrvatskim i nizozemskim javnim knjižnicama. Istraživanje je provedeno u suradnji Sveučilišta u Zagrebu te Nizozemskog udruženja narodnih knjižnica putem upitnika kojega su prvo ispunjavali knjižničari iz Nizozemske, nakon čega je preveden na hrvatski jezik te je poslan hrvatskim knjižnicama putem elektroničke pošte. U istraživanju je ukupno sudjelovalo 78 knjižnica, a upitnik je ispunilo 25 hrvatskih knjižnica, od čega 48% visokoškolskih knjižnica, 44% narodnih, 4% stručnih te 4% ostalih. Od 53 nizozemskih knjižnica koje su sudjelovale u istraživanju, 75% ispitanih bile su narodne knjižnice, 13% stručne, a 4% visokoučilišne i ostale knjižnice. Upitnik su većinom ispunjavali ravnatelji i voditelji knjižnica.

U članku se navodi da, iako su „Hrvatska i Nizozemska različita društva...obje su zemlje dio Europe te su kao takve pod utjecajem regulacija Europske unije, što se vidi i po sličnom zakonodavstvu o zaštiti osobnih podataka“¹² (Schepman et al., 2008:18). Obje zemlje su u vrijeme provođenja istraživanja imale poseban zakon o zaštiti osobnih podataka u svojem nacionalnom zakonodavstvu, koji je u Nizozemskoj usvojen 2001., a u Hrvatskoj 2003. godine, te je implementirao europsku Direktivu 95/46/EZ iz 1995. Knjižnice su bile dužne uskladiti svoje poslovanje sukladno tim zakonima kako bi se osigurala privatnost njihovih korisnika, no u istraživanju se pokazalo da nisu sve knjižnice tako i postupile.

Organizacija knjižnica Nizozemske FOBID objavila je i smjernice o zaštiti osobnih podataka, no istraživanje je pokazalo da neki knjižničari ne znaju da one postoje, dok ih drugi nisu implementirali. Objavljeno je više međunarodnih dokumenata koji reguliraju zaštitu podataka članova knjižnica, kao što su UNESCO-v Manifest za narodne knjižnice, te IFLA-ina izjava Knjižnice i intelektualna sloboda, a u Hrvatskoj je osmišljen Etički kodeks Hrvatskog knjižničarskog društva. No, Schepman et al. (2008) naglašavaju da navedeni dokumenti ne preciziraju dovoljno kako bi se to trebalo provesti.

¹² “Croatia and the Netherlands are different societies...But both countries are part of Europe and are closely influenced by regulations by the European Union. This is shown in the similar legislation on protection of personal data.”

Rezultati istraživanja, koji su prikazani u [tablici 2](#), pokazuju da ispitane knjižnice različito postupaju s podacima svojih korisnika. Zelenom bojom označene su nizozemske ili hrvatske knjižnice koje u određenim aspektima više vode brigu o zaštiti podataka svojih korisnika od drugih knjižnica. U tablici je također naznačeno koji od navedenih kriterija vrijede i za Knjižnicu FFZG-a, što je detaljnije navedeno u prethodnom poglavlju.

	ISTRAŽIVANJE 2007		ISTRAŽIVANJE 2018
	HRVATSKE KNJIŽNICE	NIZOZEMSKJE KNJIŽNICE	KNJIŽNICA FFZG-a
broj ispitanih knjižnica	25	53	1
pismena politika zaštite	8 %	23 %	+
autorizacija pristupa osobnim podacima	8 %	37 %	+
službenik za zaštitu osobnih podataka	4 %	-	+
osobni podatci vidljivi u web katalogu	< 50 %	83 %	+
mogućnost samostalne promjene osobnih podataka u web katalogu	8 %	30 %	+
bilježi povijest posudbe	48 %	80 %	+
podatci o plaćanju usluga	24 %	31 %	+
praćenje korisničke pretrage kataloga ili IP adrese	12 %	9 %	-
bilježi posjećene web stranice	32 %	15 %	-
obavještava korisnike o praćenju posjećenih web stranica	12 %	12 %	-
čuva sigurnosnu kopiju knjižničnog sustava na sigurnome mjestu	44 %	71 %	+
sigurnosni nadzor	28 %	21 %	+

Tablica 2: Rezultati istraživanja u Knjižnici FFZG-a te hrvatskim i nizozemskim knjižnicama

U istraživanju iz 2007., samo je nekoliko knjižnica navelo da ima politiku zaštite podataka u kojoj knjižnica izjavljuje kako postupa s osobnim podacima svojih korisnika. Neki od ispitanika odgovorili su da imaju ustanovljenu politiku privatnosti, iako ne i napismeno, a navodi se i da korisnici često niti ne znaju da politika zaštite podataka u knjižnici postoji. Kako Knjižnica FFZG-a obrađuje podatke svojih korisnika je pak navedeno u *Pravilniku o uvjetima i načinu korištenja građe i usluga Knjižnice*, o čemu su korisnici obavješteni putem web stranice Knjižnice.

U određenim knjižnicama samo pojedine osobe imaju autorizaciju pristupiti i promijeniti osobne podatke korisnika, dok korisnici u većini slučajeva prijavom u web katalog ne mogu samostalno promijeniti svoje podatke. Nekoliko hrvatskih knjižnica navelo je i da imaju djelatnika koji brine o zaštiti osobnih podataka članova.

S obzirom da su knjižnice „društvene organizacije koje prikupljaju podatke od svojih korisnika, o njima te za njih“¹³ (Schepman et al., 2008:2), one mogu iskoristiti te podatke kako bi korisnicima ponudili personalizirane usluge. Neke od usluga koje knjižnice mogu ponuditi svojim korisnicima obradom njihovih podataka su produživanje roka posudbe, uvid u detalje o plaćanju knjižničnih usluga te davanje prijedloga za čitanje ili slušanje. Prema istraživanju Schepman et al. (2008) mnogi djelatnici nisu znali odgovoriti mogu li ponuditi neku od personaliziranih usluga svojim korisnicima. Knjižnice koje bilježe povijest posudbe odgovorile su da je ta opcija omogućena uglavnom radi vođenja statistike, no neke pak navode da se ti podatci koriste kako bi se korisnicima ponudio prijedlog za čitanje, čak i onda kada su korisnici isključili opciju prikaza povijesti posudbe. Članovi Knjižnice Filozofskog fakulteta nemaju opciju isključenja povijesti posudbe, no ti se podatci ne koriste za personalizirane usluge, već samo radi statističke evidencije.

U određenim knjižnicama se prijavom na web katalog također mogu pregledati i podatci o plaćanju knjižničnih usluga. U pola ispitanih knjižnica iz Nizozemske ti se podatci čuvaju duže od 6 mjeseci, dok druga polovica nije znala odgovor na to pitanje.

Mnogi od ispitanika nisu znali bilježi li se pretraga web kataloga, dok je većina ispitanika koji prate pretragu web stranice ili IP adresu posjetitelja odgovorilo da o tome ne obavještavaju korisnike. Posjet web stranicama se u pojedinim knjižnicama čuva samo tijekom dana, a u drugima čak mjesec dana, nakon čega se ti podatci brišu. U 20% hrvatskih knjižnica posjećene web stranice mogu se i povezati s korisnikom koji ih posjećuje. Iako djelatnici

¹³ “Libraries are societal organizations which collect data from, about and for their users”

Knjižnice FFZG-a također mogu ustanoviti IP adresu posjetitelja web stranice Knjižnice, ti se podatci ne prate i ne bilježe.

Ispitane knjižnice koriste različite sustave za upravljanje knjižnicama, no većina ih čuva sigurnosnu kopiju sustava na sigurnome mjestu, iako samo pojedine knjižnice pravovremeno uništavaju stare verzije sustava.

Sigurnosni nadzor je prema istraživanju rijetkost u knjižnicama. Knjižnice koje imaju nadzorne kamere u većini slučajeva nadziru razne prostorije unutar knjižnice, a manji broj ih nadzire i ulaz. Sve ispitane hrvatske knjižnice navode da su obavijestile korisnike o nadzoru prostorija postavljanjem obavijesti blizu ulaza u knjižnicu.

Za sigurnost osobnih podataka u knjižnicama AZOP preporučuje i edukaciju djelatnika, što je na primjeru iz Nizozemske potaknulo knjižničare da se dodatno zauzmu za zaštitu podataka svojih korisnika: „Kada je predstavljena nova nizozemska regulativa koja bi olakšala policiji i pravosudnim tijelima da zatraže osobne podatke (uključujući podatke iz knjižnica), organiziran je seminar za knjižničare kako bi se dodatno podigla razina svijesti...to je rezultiralo protestom i pismima upozorenja ministru od strane krovne organizacije knjižnica FOBID“¹⁴ (Schepman et al., 2008:6).

Istraživanje iz 2007. godine pokazalo je da knjižnice u obje zemlje različito postupaju s osobnim podacima svojih korisnika te da uvođenje novih tehnologija u knjižnicama često ostaje neiskorišteno jer knjižničari nisu uvijek upoznati sa svim mogućnostima koje tehnologija nosi, kao ni koji se sve podatci o korisnicima prikupljaju njezinom implementacijom. Istraživanje je također pokazalo kako korisnici često nisu obaviješteni o načinu na koji knjižnica postupa s njihovim podacima.

¹⁴ “When new Dutch legislation was introduced to make it easier for police and legal authorities to request personal data (also from libraries), a library seminar was organised to raise further awareness...It resulted in protest and warning letters by the library umbrella organisation FOBID to the minister.”

6. Zaključak

U radu su opisani ključni pojmovi nužni za razumijevanje važnosti zaštite osobnih podataka, a to su podatak, informacija i informacijsko društvo, koje se temelji na proizvodnji, obradi i razmjeni podataka. Prema povijesnom kontekstu razaznaje se kako su se podatci zapisivali, obrađivali i čuvali tijekom stoljeća, te da je njihova zaštita oduvijek ovisila o mediju na kojem su pohranjeni. Razvojem informacijsko-komunikacijskih tehnologija došlo je do revolucije u obradi podataka, a nove tehnologije omogućile su i pohranu, odnosno iskoristivost sve veće količine podataka. No, to je dovelo i do novih izazova u zaštiti osobnih podataka.

Prema procjeni Europske unije, najviša razina zaštite osobnih podataka je upravo u državama EU i Europskog gospodarskog prostora, dok se razina zaštite u drugim zemljama svijeta smatra dovoljnom.

Istraživanje hrvatskih i nizozemskih stručnjaka iz 2007. godine pokazalo je da je tadašnja razina zaštite osobnih podataka u knjižnicama bila vrlo niska i razlikovala se od knjižnice do knjižnice. Stoga je postojala potreba za reformom zakonodavstva koje bi ujednačilo praksu u knjižnicama te povećalo razinu zaštite. Također, naglašena je i uloga edukacije djelatnika i članova knjižnice, koji često nisu informirani o načinu na koji knjižnica postupa s njihovim podacima te koji se podatci obrađuju i u koju svrhu.

Istraživanje o zaštiti osobnih podataka članova Knjižnice Filozofskog fakulteta u Zagrebu je pak pokazalo da je i prije donošenja GDPR-a Knjižnica primjereno postupala s podacima svojih korisnika, prikupljajući samo one podatke koji su Knjižnici potrebni radi sigurnosti vlastitoga fonda. Osim potpisivanja izjave o čuvanju povjerljivosti i tajnosti podataka, te imenovanja službenika za zaštitu podataka na razini fakulteta, stupanjem GDPR-a na snagu nije došlo do značajnih promjena u postupanju s podacima članova Knjižnice.

7. Literatura

1. AZOP. (bez dat.). Preuzeto 03. kolovoza 2018., od <http://azop.hr/info-servis/detaljnije/mobilne-aplikacije-azop-i-gdpr-na-dlanu>
2. Boban, M. (2018). Zaštita osobnih podataka i nova EU uredba o zaštiti podataka. *Bilten Hrvatskog društva za medicinsku informatiku*, 24 (1), 26–40. Preuzeto 14. srpnja 2018., od <https://hrcak.srce.hr/193680>
3. Casson, L. (2001). *Libraries in the Ancient World*. New Haven ; London: Yale University Press.
4. Census. (2018). Preuzeto 03. rujna 2018., od <https://www.britannica.com/science/census>
5. Data protection around the world | CNIL. (bez dat.). Preuzeto 12. kolovoza 2018., od <https://www.cnil.fr/en/data-protection-around-the-world>
6. European Union, Agency for Fundamental Rights, Council of Europe (Strasbourg), & European Court of Human Rights. (2014). *Priručnik o europskom zakonodavstvu o zaštiti podataka*. Luxembourg: Publications Office.
7. Freiburger, P.A., Hemmendinger, D., Pottenger, W.M., Swaine, M.R. (2018.) *Computer*. Preuzeto 03. rujna 2018., od <https://www.britannica.com/technology/computer/History-of-computing>
8. Horvat, A. (2002). Javno i tajno u knjižničarskoj struci. *Arhivi, knjižnice, muzeji: mogućnosti suradnje u okruženju globalne informacijske infrastrukture: zbornik radova*, 8–15. Preuzeto 14. srpnja 2018., od http://dzs.ffzg.unizg.hr/text/jit_u_%20knjiz.pdf
9. Informacija (bez dat.). U *Hrvatska enciklopedija*. Preuzeto 23. srpnja 2018., od <http://www.enciklopedija.hr/Natuknica.aspx?ID=27405>
10. Informacijsko društvo (bez dat.). Preuzeto 23. srpnja 2018., od <http://www.enciklopedija.hr/Natuknica.aspx?ID=27411>
11. Kocijan, K. (2014). Big Data: kako smo došli do Velikih podataka i kamo nas oni vode. U R. Vrana & Đ. Pečarić (Ur.), *Komunikacijski obrasci i informacijska znanost* (str. 37–62). Zagreb: Zavod za informacijske studije. Preuzeto od <http://darhiv.ffzg.unizg.hr/id/eprint/5064/>
12. Koja se pravila primjenjuju ako moja organizacija prenosi podatke izvan EU-a? (bez

- dat.). Preuzeto 02. kolovoza 2018., od https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_hr
13. Komunikacija (bez dat.). U *Hrvatska enciklopedija*. Preuzeto 16. kolovoza 2018., od <http://www.enciklopedija.hr/Natuknica.aspx?ID=32686>
14. Podatak (bez dat.). U *Hrvatska enciklopedija*. Preuzeto 23. srpnja 2018., od <http://www.enciklopedija.hr/natuknica.aspx?id=48887>
15. Pravilnik o uvjetima i načinu korištenja građe i usluga Knjižnice - Knjižnica Filozofskog fakulteta u Zagrebu. (2018). Preuzeto 17. srpnja 2018., od http://knjiznica.ffzg.unizg.hr/pravilnik_2018
16. Računalo (bez dat.). U *Hrvatska enciklopedija*. Preuzeto 16. kolovoza 2018., od <http://www.enciklopedija.hr/Natuknica.aspx?ID=51394>
17. Rudgard, S. (2012). Origins and Historical Context of Data Protection Law. U E. Ustaran (Ur.), *European Privacy: Law and Practice for Data Protection Professionals* (str. 3–17). Preuzeto od https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf
18. Sandler, A. (2018). Senate Democrats Propose CONSENT Act. Preuzeto 13. kolovoza 2018., od <https://www.insideprivacy.com/united-states/congress/senate-democrats-propose-consent-act/>
19. Schepman, T., Koren, M., Horvat, A., Kurtovic, D., Grgić, I. H. (2008). Access With(out) Anonymity. U *16th BOBCATSSS Symposium 2008* (str. 1–21). <http://dx.doi.org/10.18452/1279>
20. Schneier, B. (2015). *Data and Goliath* (1. izd.). New York ; London: W. W. Norton & Company.
21. Sustav statističkih podataka o knjižnicama. (2018). Preuzeto 17. srpnja 2018., od <http://hk.nsk.hr/>
22. The History of the General Data Protection Regulation. (2018). Preuzeto 19. srpnja 2018., od /data-protection/data-protection/legislation/history-general-data-protection-regulation_en
23. Tuđman, M., Boras, D., Dovedan, Z. (1993). *Uvod u informacijske znanosti* (2. izd.). Zagreb: Školska knjiga. Preuzeto od <http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/>

24. Opća uredba o zaštiti podataka. (2016). Preuzeto 14. srpnja 2018., od
<http://data.europa.eu/eli/reg/2016/679/oj/hrv>
25. Ustav Republike Hrvatske (Narodne novine, br. 85/2010). Preuzeto 14. srpnja 2018.,
od https://narodne-novine.nn.hr/clanci/sluzbeni/2010_07_85_2422.html
26. Zaštita osobnih podataka. (2018). Preuzeto 19. srpnja 2018., od
<http://dokumenti.ffzg.unizg.hr/javna-nabava/zastita-osobnih-podataka/>